# Contents

# What's new in Storage in Windows Server

12/16/2020 • 16 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

This topic explains the new and changed functionality in storage in Windows Server 2019, Windows Server 2016, and Windows Server Semi-Annual Channel releases.

## What's new in storage in Windows Server, version 1903

This release of Windows Server adds the following changes and technologies.

**Storage Migration Service now migrates local accounts, clusters, and Linux servers**

Storage Migration Service makes it easier to migrate servers to a newer version of Windows Server. It provides a graphical tool that inventories data on servers and then transfers the data and configuration to newer servers—all without apps or users having to change anything.

When using this version of Windows Server to orchestrate migrations, we've added the following abilities:

- Migrate local users and groups to the new server
- Migrate storage from failover clusters
- Migrate storage from a Linux server that uses Samba
- More easily sync migrated shares into Azure by using Azure File Sync
- Migrate to new networks such as Azure

For more info about Storage Migration Service, see Storage Migration Service overview.

**System Insights disk anomaly detection**

System Insights is a predictive analytics feature that locally analyzes Windows Server system data and provides insight into the functioning of the server. It comes with a number of built-in capabilities, but we've added the ability to install additional capabilities via Windows Admin Center, starting with disk anomaly detection.

Disk anomaly detection is a new capability that highlights when disks are behaving *differently* than usual. While different isn't necessarily a bad thing, seeing these anomalous moments can be helpful when troubleshooting issues on your systems.

This capability is also available for servers running Windows Server 2019.

**Windows Admin Center enhancements**

A new release of Windows Admin Center is out, adding new functionality to Windows Server. For info on the latest features, see Windows Admin Center.

## What's new in storage in Windows Server 2019 and Windows Server, version 1809

This release of Windows Server adds the following changes and technologies.

**Manage storage with Windows Admin Center**

Windows Admin Center is a new locally deployed, browser-based app for managing servers, clusters, hyper-converged infrastructure with Storage Spaces Direct, and Windows 10 PCs. It comes at no additional cost beyond Windows and is ready for production use.

To be fair, Windows Admin Center is a separate download that runs on Windows Server 2019 and other versions of Windows, but it's new and we didn't want you to miss it...

**Storage Migration Service**

Storage Migration Service is a new technology that makes it easier to migrate servers to a newer version of Windows Server. It provides a graphical tool that inventories data on servers, transfers the data and configuration to newer servers, and then optionally moves the identities of the old servers to the new servers so that apps and users don't have to change anything. For more info, see Storage Migration Service.

**Storage Spaces Direct (Windows Server 2019 only)**

There are a number of improvements to Storage Spaces Direct in Windows Server 2019 (Storage Spaces Direct isn't included in Windows Server, Semi-Annual Channel):

- Deduplication and compression for ReFS volumes

  Store up to ten times more data on the same volume with deduplication and compression for the ReFS filesystem. (It's just one click to turn on with Windows Admin Center.) The variable-size chunk store with optional compression maximizes savings rates, while the multi-threaded post-processing architecture keeps performance impact minimal. Supports volumes up to 64 TB and will deduplicate the first 4 TB of each file.

- Native support for persistent memory

  Unlock unprecedented performance with native Storage Spaces Direct support for persistent memory modules, including Intel® Optane™ DC PM and NVDIMM-N. Use persistent memory as cache to accelerate the active working set, or as capacity to guarantee consistent low latency on the order of microseconds. Manage persistent memory just as you would any other drive in PowerShell or Windows Admin Center.

- Nested resiliency for two-node hyper-converged infrastructure at the edge

  Survive two hardware failures at once with an all-new software resiliency option inspired by RAID 5+1. With nested resiliency, a two-node Storage Spaces Direct cluster can provide continuously accessible storage for apps and virtual machines even if one server node goes down and a drive fails in the other server node.

- Two-server clusters using a USB flash drive as a witness

  Use a low-cost USB flash drive plugged into your router to act as a witness in two-server clusters. If a server goes down and then back up, the USB drive cluster knows which server has the most up-to-date data. For more info, see the Storage at Microsoft blog and documentation on how to deploy a file share witness.

- Windows Admin Center

  Manage and monitor Storage Spaces Direct with the new purpose-built Dashboard and experience in Windows Admin Center. Create, open, expand, or delete volumes with just a few clicks. Monitor performance like IOPS and IO latency from the overall cluster down to the individual SSD or HDD. Available at no additional cost for Windows Server 2016 and Windows Server 2019.

- Performance history

  Get effortless visibility into resource utilization and performance with built-in history. Over 50 essential counters spanning compute, memory, network, and storage are automatically collected and stored on the cluster for up to one year. Best of all, there's nothing to install, configure, or start – it just works. Visualize in Windows Admin Center or query and process in PowerShell.

- Scale up to 4 PB per cluster

  Achieve multi-petabyte scale – great for media, backup, and archival use cases. In Windows Server 2019, Storage Spaces Direct supports up to 4 petabytes (PB) = 4,000 terabytes of raw capacity per storage pool. Related capacity guidelines are increased as well: for example, you can create twice as many volumes (64

instead of 32), each twice as large as before (64 TB instead of 32 TB). Stitch multiple clusters together into a cluster set for even greater scale within one storage namespace. For more info, see the Storage at Microsoft blog.

- **Mirror-accelerated parity is 2X faster**

  With mirror-accelerated parity you can create Storage Spaces Direct volumes that are part mirror and part parity, like mixing RAID-1 and RAID-5/6 to get the best of both. (It's easier than you think in Windows Admin Center.) In Windows Server 2019, the performance of mirror-accelerated parity is more than doubled relative to Windows Server 2016 thanks to optimizations.

- **Drive latency outlier detection**

  Easily identify drives with abnormal latency with proactive monitoring and built-in outlier detection, inspired by Microsoft Azure's long-standing and successful approach. Whether it's average latency or something more subtle like 99th percentile latency that stands out, slow drives are automatically labeled in PowerShell and Windows Admin Center with 'Abnormal Latency' status.

- **Manually delimit the allocation of volumes to increase fault tolerance**

  This enables admins to manually delimit the allocation of volumes in Storage Spaces Direct. Doing so can significantly increase fault tolerance under certain conditions, but imposes some added management considerations and complexity. For more info, see Delimit the allocation of volumes.

### Storage Replica

There are a number of improvements to Storage Replica in this release:

#### Storage Replica in Windows Server, Standard Edition

You can now use Storage Replica with Windows Server, Standard Edition in addition to Datacenter Edition. Storage Replica running on Windows Server, Standard Edition, has the following limitations:

- Storage Replica replicates a single volume instead of an unlimited number of volumes.
- Volumes can have a size of up to 2 TB instead of an unlimited size.

#### Storage Replica log performance improvements

We also made improvements to how the Storage Replica log tracks replication, improving replication throughput and latency, especially on all-flash storage as well as Storage Spaces Direct clusters that replicate between each other.

To gain the increased performance, all members of the replication group must run Windows Server 2019.

#### Test failover

You can now temporarily mount a snapshot of the replicated storage on a destination server for testing or backup purposes. For more information, see Frequently Asked Questions about Storage Replica.

#### Windows Admin Center support

Support for graphical management of replication is now available in Windows Admin Center via the Server Manager tool. This includes server-to-server replication, cluster-to-cluster, as well as stretch cluster replication.

#### Miscellaneous improvements

Storage Replica also contains the following improvements:

- Alters asynchronous stretch cluster behaviors so that automatic failovers now occur
- Multiple bug fixes

### SMB

- **SMB1 and guest authentication removal**: Windows Server no longer installs the SMB1 client and server by default. Additionally, the ability to authenticate as a guest in SMB2 and later is off by default. For more information, review SMBv1 is not installed by default in Windows 10, version 1709 and Windows

Server, version 1709.

- **SMB2/SMB3 security and compatibility**: Additional options for security and application compatibility were added, including the ability to disable oplocks in SMB2+ for legacy applications, as well as require signing or encryption on per-connection basis from a client. For more information, review the SMBShare PowerShell module help.

#### Data Deduplication

- **Data Deduplication now supports ReFS**: You no longer must choose between the advantages of a modern file system with ReFS and the Data Deduplication: now, you can enable Data Deduplication wherever you can enable ReFS. Increase storage efficiency by upwards of 95% with ReFS.
- **DataPort API for optimized ingress/egress to deduplicated volumes**: Developers can now take advantage of the knowledge Data Deduplication has about how to store data efficiently to move data between volumes, servers, and clusters efficiently.

#### File Server Resource Manager

Windows Server 2019 includes the ability to prevent the File Server Resource Manager service from creating a change journal (also known as a USN journal) on all volumes when the service starts. This can conserve space on each volume, but will disable real-time file classification. For more information, see File Server Resource Manager overview.

## What's new in storage in Windows Server, version 1803

#### File Server Resource Manager

Windows Server, version 1803 includes the ability to prevent the File Server Resource Manager service from creating a change journal (also known as a USN journal) on all volumes when the service starts. This can conserve space on each volume, but will disable real-time file classification. For more information, see File Server Resource Manager overview.

## What's new in storage in Windows Server, version 1709

Windows Server, version 1709 is the first Windows Server release in the Semi-Annual Channel. The Semi-Annual Channel is a Software Assurance benefit and is fully supported in production for 18 months, with a new version every six months.

For more information, see Windows Server Semi-annual Channel Overview.

#### Storage Replica

The disaster recovery protection added by Storage Replica is now expanded to include:

- **Test failover**: the option to mount the destination storage is now possible through the test failover feature. You can mount a snapshot of the replicated storage on destination nodes temporarily for testing or backup purposes. For more information, see Frequently Asked Questions about Storage Replica.
- **Windows Admin Center support**: Support for graphical management of replication is now available in Windows Admin Center via the Server Manager tool. This includes server-to-server replication, cluster-to-cluster, as well as stretch cluster replication.

Storage Replica also contains the following improvements:

- Alters asynchronous stretch cluster behaviors so that automatic failovers now occur
- Multiple bug fixes

#### SMB

- **SMB1 and guest authentication removal**: Windows Server, version 1709 no longer installs the SMB1 client and server by default. Additionally, the ability to authenticate as a guest in SMB2 and later is off by

default. For more information, review SMBv1 is not installed by default in Windows 10, version 1709 and Windows Server, version 1709.

- **SMB2/SMB3 security and compatibility**: Additional options for security and application compatibility were added, including the ability to disable oplocks in SMB2+ for legacy applications, as well as require signing or encryption on per-connection basis from a client. For more information, review the SMBShare PowerShell module help.

**Data Deduplication**

- **Data Deduplication now supports ReFS**: You no longer must choose between the advantages of a modern file system with ReFS and the Data Deduplication: now, you can enable Data Deduplication wherever you can enable ReFS. Increase storage efficiency by upwards of 95% with ReFS.
- **DataPort API for optimized ingress/egress to deduplicated volumes**: Developers can now take advantage of the knowledge Data Deduplication has about how to store data efficiently to move data between volumes, servers, and clusters efficiently.

## What's new in storage in Windows Server 2016

**Storage Spaces Direct**

Storage Spaces Direct enables building highly available and scalable storage using servers with local storage. It simplifies the deployment and management of software-defined storage systems and unlocks use of new classes of disk devices, such as SATA SSD and NVMe disk devices, that were previously not possible with clustered Storage Spaces with shared disks.

**What value does this change add?** Storage Spaces Direct enables service providers and enterprises to use industry standard servers with local storage to build highly available and scalable software defined storage. Using servers with local storage decreases complexity, increases scalability, and enables use of storage devices that were not previously possible, such as SATA solid state disks to lower cost of flash storage, or NVMe solid state disks for better performance.

Storage Spaces Direct removes the need for a shared SAS fabric, simplifying deployment and configuration. Instead it uses the network as a storage fabric, leveraging SMB3 and SMB Direct (RDMA) for high-speed, low-latency CPU efficient storage. To scale out, simply add more servers to increase storage capacity and I/O performance For more information, see the Storage Spaces Direct in Windows Server 2016.

**What works differently?** This capability is new in Windows Server 2016.

**Storage Replica**

Storage Replica enables storage-agnostic, block-level, synchronous replication between servers or clusters for disaster recovery, as well as stretching of a failover cluster between sites. Synchronous replication enables mirroring of data in physical sites with crash-consistent volumes to ensure zero data loss at the file-system level. Asynchronous replication allows site extension beyond metropolitan ranges with the possibility of data loss.

**What value does this change add?** Storage Replication enables you to do the following:

- Provide a single vendor disaster recovery solution for planned and unplanned outages of mission critical workloads.
- Use SMB3 transport with proven reliability, scalability, and performance.
- Stretch Windows failover clusters to metropolitan distances.
- Use Microsoft software end to end for storage and clustering, such as Hyper-V, Storage Replica, Storage Spaces, Cluster, Scale-Out File Server, SMB3, Deduplication, and ReFS/NTFS.
- Help reduce cost and complexity as follows:
  - Is hardware agnostic, with no requirement for a specific storage configuration like DAS or SAN.
  - Allows commodity storage and networking technologies.

    - Features ease of graphical management for individual nodes and clusters through Failover Cluster Manager.
    - Includes comprehensive, large-scale scripting options through Windows PowerShell.
- Help reduce downtime, and increase reliability and productivity intrinsic to Windows.
- Provide supportability, performance metrics, and diagnostic capabilities.

For more information, see the Storage Replica in Windows Server 2016.

**What works differently?** This capability is new in Windows Server 2016.

**Storage Quality of Service**

You can now use storage quality of service (QoS) to centrally monitor end-to-end storage performance and create management policies using Hyper-V and CSV clusters in Windows Server 2016.

**What value does this change add?** You can now create storage QoS policies on a CSV cluster and assign them to one or more virtual disks on Hyper-V virtual machines. Storage performance is automatically readjusted to meet policies as the workloads and storage loads fluctuate.

- Each policy can specify a reserve (minimum) and/or a limit (maximum) to be applied to a collection of data flows, such as a virtual hard disk, a single virtual machine or a group of virtual machines, a service, or a tenant.
- Using Windows PowerShell or WMI, you can perform the following tasks:
    - Create policies on a CSV cluster.
    - Enumerate policies available on a CSV cluster.
    - Assign a policy to a virtual hard disk of a Hyper-V virtual machine.
    - Monitor the performance of each flow and status within the policy.
- If multiple virtual hard disks share the same policy, performance is fairly distributed to meet demand within the policy's minimum and maximum settings. Therefore, a policy can be used to manage a virtual hard disk, a virtual machine, multiple virtual machines comprising a service, or all virtual machines owned by a tenant.

**What works differently?** This capability is new in Windows Server 2016. Managing minimum reserves, monitoring flows of all virtual disks across the cluster via a single command, and centralized policy based management were not possible in previous releases of Windows Server.

For more information, see Storage Quality of Service

**Data Deduplication**

| FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
| --- | --- | --- |
| Support for Large Volumes | Updated | Prior to Windows Server 2016, volumes had to specifically sized for the expected churn, with volume sizes above 10 TB not being good candidates for deduplication. In Windows Server 2016, Data Deduplication supports volume sizes **up to 64 TB**. |
| Support for Large Files | Updated | Prior to Windows Server 2016, files approaching 1 TB in size were not good candidates for deduplication. In Windows Server 2016, files **up to 1 TB** are fully supported. |
| Support for Nano Server | New | Data Deduplication is available and fully supported in the new Nano Server deployment option for Windows Server 2016. |

| FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
| --- | --- | --- |
| Simplified Backup Support | New | In Windows Server 2012 R2, Virtualized Backup Applications, such as Microsoft's Data Protection Manager, were supported through a series of manual configuration steps. In Windows Server 2016, a new default Usage Type "Backup", has been added for seamless deployment of Data Deduplication for Virtualized Backup Applications. |
| Support for Cluster OS Rolling Upgrades | New | Data Deduplication fully supports the new Cluster OS Rolling Upgrade feature of Windows Server 2016. |

### SMB hardening improvements for SYSVOL and NETLOGON connections

In Windows 10 and Windows Server 2016 client connections to the Active Directory Domain Services default SYSVOL and NETLOGON shares on domain controllers now require SMB signing and mutual authentication (such as Kerberos).

**What value does this change add?** This change reduces the likelihood of man-in-the-middle attacks.

**What works differently?** If SMB signing and mutual authentication are unavailable, a Windows 10 or Windows Server 2016 computer won't process domain-based Group Policy and scripts.

> **NOTE**
> The registry values for these settings aren't present by default, but the hardening rules still apply until overridden by Group Policy or other registry values.

For more information on these security improvements - also referred to as UNC hardening, see Microsoft Knowledge Base article 3000483 and MS15-011 & MS15-014: Hardening Group Policy.

### Work Folders

Improved change notification when the Work Folders server is running Windows Server 2016 and the Work Folders client is Windows 10.

#### What value does this change add?

For Windows Server 2012 R2, when file changes are synced to the Work Folders server, clients are not notified of the change and wait up to 10 minutes to get the update. When using Windows Server 2016, the Work Folders server immediately notifies Windows 10 clients and the file changes are synced immediately.

#### What works differently?

This capability is new in Windows Server 2016. This requires a Windows Server 2016 Work Folders server and the client must be Windows 10.

If you're using an older client or the Work Folders server is Windows Server 2012 R2, the client will continue to poll every 10 minutes for changes.

### ReFS

The next iteration of ReFS provides support for large-scale storage deployments with diverse workloads, delivering

reliability, resiliency, and scalability for your data.

**What value does this change add?**
ReFS introduces the following improvements:

- ReFS implements new storage tiers functionality, helping deliver faster performance and increased storage capacity. This new functionality enables:
  - Multiple resiliency types on the same virtual disk (using mirroring in the performance tier and parity in the capacity tier, for example).
  - Increased responsiveness to drifting working sets.
- The introduction of block cloning substantially improves the performance of VM operations, such as .vhdx checkpoint merge operations.
- The new ReFS scan tool enables the recovery of leaked storage and helps salvage data from critical corruptions.

**What works differently?**
These capabilities are new in Windows Server 2016.

## Additional References

- What's New in Windows Server 2016

# Data Deduplication Overview

12/16/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel),

## What is Data Deduplication?

Data Deduplication, often called Dedup for short, is a feature that can help reduce the impact of redundant data on storage costs. When enabled, Data Deduplication optimizes free space on a volume by examining the data on the volume by looking for duplicated portions on the volume. Duplicated portions of the volume's dataset are stored once and are (optionally) compressed for additional savings. Data Deduplication optimizes redundancies without compromising data fidelity or integrity. More information about how Data Deduplication works can be found in the 'How does Data Deduplication work?' section of the Understanding Data Deduplication page.

> **IMPORTANT**
>
> KB4025334 contains a roll up of fixes for Data Deduplication, including important reliability fixes, and we strongly recommend installing it when using Data Deduplication with Windows Server 2016 and Windows Server 2019.

## Why is Data Deduplication useful?

Data Deduplication helps storage administrators reduce costs that are associated with duplicated data. Large datasets often have **a lot** of duplication, which increases the costs of storing the data. For example:

- User file shares may have many copies of the same or similar files.
- Virtualization guests might be almost identical from VM-to-VM.
- Backup snapshots might have minor differences from day to day.

The space savings that you can gain from Data Deduplication depend on the dataset or workload on the volume. Datasets that have high duplication could see optimization rates of up to 95%, or a 20x reduction in storage utilization. The following table highlights typical deduplication savings for various content types:

| SCENARIO | CONTENT | TYPICAL SPACE SAVINGS |
|---|---|---|
| User documents | Office documents, photos, music, videos, etc. | 30-50% |
| Deployment shares | Software binaries, cab files, symbols, etc. | 70-80% |
| Virtualization libraries | ISOs, virtual hard disk files, etc. | 80-95% |
| General file share | All the above | 50-60% |

## When can Data Deduplication be used?

### General purpose file servers

General purpose file servers are general use file servers that might contain any of the following types of shares:

- Team shares
- User home folders
- Work Folders
- Software development shares

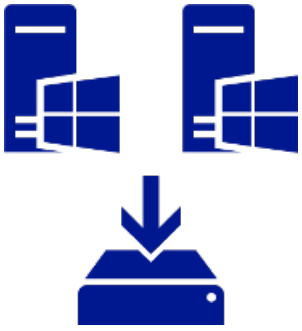
General purpose file servers are a good candidate for Data Deduplication because multiple users tend to have many copies or versions of the same file. Software development shares benefit from Data Deduplication because many binaries remain essentially unchanged from build to build.

### Virtualized Desktop Infrastructure (VDI) deployments

VDI servers, such as Remote Desktop Services, provide a lightweight option for organizations to provision desktops to users. There are many reasons for an organization to rely on such technology:

- **Application deployment**: You can quickly deploy applications across your enterprise. This is especially useful when you have applications that are frequently updated, infrequently used, or difficult to manage.
- **Application consolidation**: When you install and run applications from a set of centrally managed virtual machines, you eliminate the need to update applications on client computers. This option also reduces the amount of network bandwidth that is required to access applications.
- **Remote access**: Users can access enterprise applications from devices such as home computers, kiosks, low-powered hardware, and operating systems other than Windows.
- **Branch office access**: VDI deployments can provide better application performance for branch office workers who need access to centralized data stores. Data-intensive applications sometimes do not have client/server protocols that are optimized for low-speed connections.

VDI deployments are great candidates for Data Deduplication because the virtual hard disks that drive the remote desktops for users are essentially identical. Additionally, Data Deduplication can help with the so-called *VDI boot storm*, which is the drop in storage performance when many users simultaneously sign in to their desktops to start the day.



### Backup targets, such as virtualized backup applications

Backup applications, such as Microsoft Data Protection Manager (DPM), are excellent candidates for Data Deduplication because of the significant duplication between backup snapshots.

**Other workloads**

Other workloads may also be excellent candidates for Data Deduplication.

# What's New in Data Deduplication

12/16/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

Data Deduplication in Windows Server has been optimized to be highly performant, flexible, and manageable at private cloud scale. For more information about the software-defined storage stack in Windows Server, please see What's New in Storage in Windows Server.

Data Deduplication has the following enhancements in Windows Server 2019:

| FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
|---|---|---|
| ReFS support | New | Store up to 10X more data on the same volume with deduplication and compression for the ReFS filesystem. (It's just one click to turn on with Windows Admin Center.) The variable-size chunk store with optional compression maximizes savings rates, while the multi-threaded post-processing architecture keeps performance impact minimal. Supports volumes up to 64 TB and will deduplicate the first 4 TB of each file. |

Data Deduplication has the following enhancements starting in Windows Server 2016:

| FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
|---|---|---|
| Support for large volumes | Updated | Prior to Windows Server 2016, volumes had to be specifically sized for the expected churn, with volume sizes above 10 TB not being good candidates for deduplication. In Windows Server 2016, Data Deduplication supports volume sizes up to 64 TB. |
| Support for large files | Updated | Prior to Windows Server 2016, files approaching 1 TB in size were not good candidates for deduplication. In Windows Server 2016, files up to 1 TB are fully supported. |
| Support for Nano Server | New | Data Deduplication is available and fully supported in the new Nano Server deployment option for Windows Server 2016. |

| FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
| --- | --- | --- |
| Simplified backup support | New | Windows Server 2012 R2 supported Virtualized Backup Applications, such as Microsoft's Data Protection Manager, through a series of manual configuration steps. Windows Server 2016 has added a new default Usage Type (Backup) for seamless deployment of Data Deduplication for Virtualized Backup Applications. |
| Support for Cluster OS Rolling Upgrade | New | Data Deduplication fully supports the new Cluster OS Rolling Upgrade feature of Windows Server 2016. |

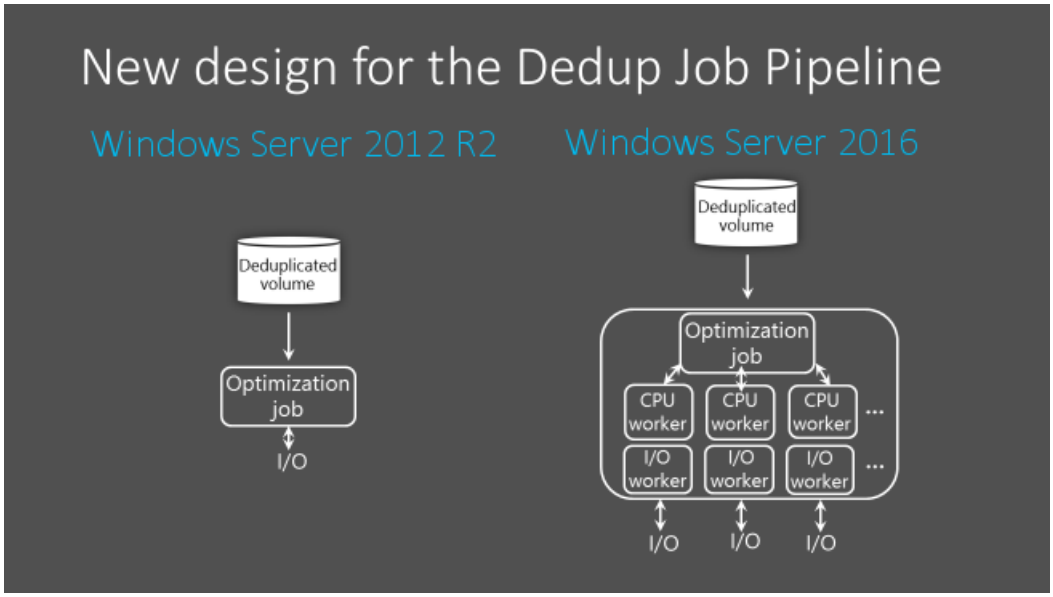
## Support for large volumes

**What value does this change add?** To get the best performance out of Data Deduplication in Windows Server 2012 R2, volumes must be sized properly to ensure that the Optimization job can keep up with the rate of data changes, or "churn." Typically, this means that Data Deduplication is only performant on volumes of 10 TB or less, depending on the workload's write patterns.

In Windows Server 2016, Data Deduplication is highly performant on volumes up to 64 TB.

**What works differently?** In Windows Server 2012 R2, the Data Deduplication Job Pipeline uses a single-thread and I/O queue for each volume. To ensure that the Optimization jobs do not fall behind, which would cause the overall savings rate for the volume to decrease, large datasets must be broken up into smaller volumes. The appropriate volume size depends on the expected churn for that volume. On average, the maximum is ~6-7 TB for high churn volumes and ~9-10 TB for low churn volumes.

In Windows Server 2016, the Data Deduplication Job pipeline has been redesigned to run multiple threads in parallel using multiple I/O queues for each volume. This results in performance that was previously only possible by dividing up data into multiple smaller volumes. This change is represented in the following image:




These optimizations apply to all Data Deduplication Jobs, not just the Optimization Job.

## Support for large files

**What value does this change add?** In Windows Server 2012 R2, very large files are not good candidates for

Data Deduplication due to decreased performance of the Deduplication Processing Pipeline. In Windows Server 2016, deduplication of files up to 1 TB is very performant, enabling administrators to apply deduplication savings to a larger range of workloads. For example, you can deduplicate very large files normally associated with backup workloads.

**What works differently?** In Windows Server 2016, Data Deduplication makes use of new stream map structures and other "under- the hood" improvements to increase optimization throughput and access performance. Additionally, the Deduplication Processing Pipeline can now resume optimization after a failover rather than restarting. These changes make deduplication on files up to 1 TB highly performant.

## Support for Nano Server

**What value does this change add?** Nano Server is a new headless deployment option in Windows Server 2016 that requires a far smaller system resource footprint, starts up significantly faster, and requires fewer updates and restarts than the Windows Server Core deployment option. Data Deduplication is fully supported on Nano Server. For more information about Nano Server, see Getting Started with Nano Server.

## Simplified configuration for Virtualized Backup Applications

**What value does this change add?** Data Deduplication for Virtualized Backup Applications is a supported scenario in Windows Server 2012 R2, but it requires manually tuning of the deduplication settings. In Windows Server 2016, the configuration of Deduplication for Virtualized Backup Applications is drastically simplified. It uses a predefined Usage Type option when enabling Deduplication for a volume, just like our options for General Purpose File Server and VDI.

## Support for Cluster OS Rolling Upgrade

**What value does this change add?** Windows Server Failover Clusters running Data Deduplication can have a mix of nodes running Windows Server 2012 R2 versions of Data Deduplication alongside nodes running Windows Server 2016 versions of Data Deduplication. This enhancement provides full data access to all deduplicated volumes during a cluster rolling upgrade, allowing for the gradual rollout of the new version of Data Deduplication on an existing Windows Server 2012 R2 cluster without incurring downtime to upgrade all nodes at once.

**What works differently?**
With previous versions of Windows Server, a Windows Server Failover Cluster required all nodes in the cluster to have the same Windows Server version. Starting with the Windows Server 2016, the cluster rolling upgrade functionality allows a cluster to run in a mixed-mode. Data Deduplication supports this new mixed-mode cluster configuration to enable full data access during a cluster rolling upgrade.

# Understanding Data Deduplication

12/16/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

This document describes how Data Deduplication works.

## How does Data Deduplication work?

Data Deduplication in Windows Server was created with the following two principles:

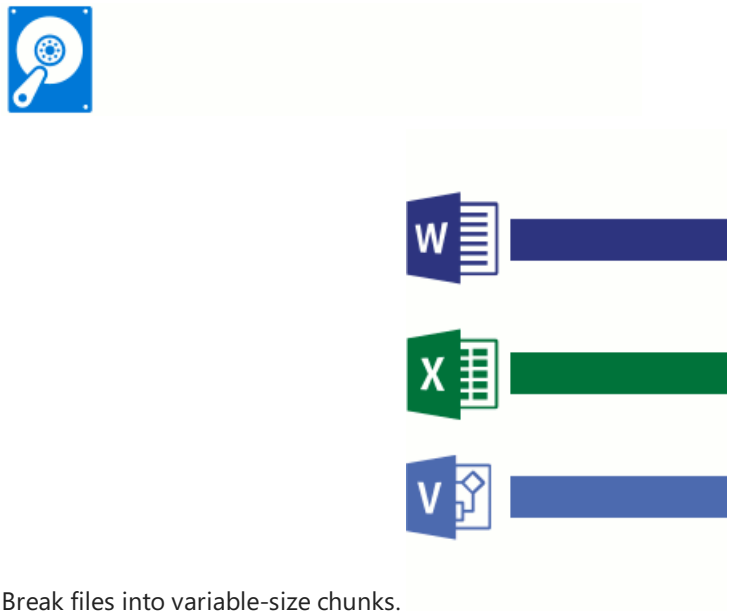
1. **Optimization should not get in the way of writes to the disk** Data Deduplication optimizes data by using a post-processing model. All data is written unoptimized to the disk and then optimized later by Data Deduplication.
2. **Optimization should not change access semantics** Users and applications that access data on an optimized volume are completely unaware that the files they are accessing have been deduplicated.

Once enabled for a volume, Data Deduplication runs in the background to:

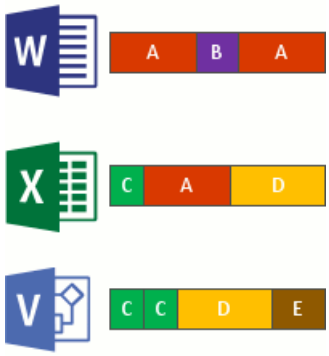
- Identify repeated patterns across files on that volume.
- Seamlessly move those portions, or chunks, with special pointers called reparse points that point to a unique copy of that chunk.

This occurs in the following four steps:

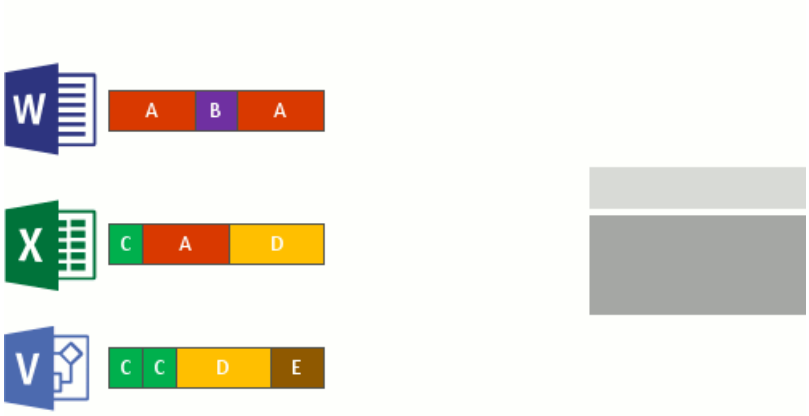
1. Scan the file system for files meeting the optimization policy.



2. Break files into variable-size chunks.




3. Identify unique chunks.
4. Place chunks in the chunk store and optionally compress.




5. Replace the original file stream of now optimized files with a reparse point to the chunk store.


When optimized files are read, the file system sends the files with a reparse point to the Data Deduplication file system filter (Dedup.sys). The filter redirects the read operation to the appropriate chunks that constitute the stream for that file in the chunk store. Modifications to ranges of a deduplicated files get written unoptimized to the disk and are optimized by the Optimization job the next time it runs.

## Usage Types

The following Usage Types provide reasonable Data Deduplication configuration for common workloads:

| USAGE TYPE | IDEAL WORKLOADS | WHAT'S DIFFERENT |
| --- | --- | --- |

| USAGE TYPE | IDEAL WORKLOADS | WHAT'S DIFFERENT |
| --- | --- | --- |
| Default | General purpose file server:<br>• Team shares<br>• Work Folders<br>• Folder redirection<br>• Software development shares | • Background optimization<br>• Default optimization policy:<br>  ◦ Minimum file age = 3 days<br>  ◦ Optimize in-use files = No<br>  ◦ Optimize partial files = No |
| Hyper-V | Virtualized Desktop Infrastructure (VDI) servers | • Background optimization<br>• Default optimization policy:<br>  ◦ Minimum file age = 3 days<br>  ◦ Optimize in-use files = Yes<br>  ◦ Optimize partial files = Yes<br>• "Under-the-hood" tweaks for Hyper-V interop |
| Backup | Virtualized backup applications, such as Microsoft Data Protection Manager (DPM) | • Priority optimization<br>• Default optimization policy:<br>  ◦ Minimum file age = 0 days<br>  ◦ Optimize in-use files = Yes<br>  ◦ Optimize partial files = No<br>• "Under-the-hood" tweaks for interop with DPM/DPM-like solutions |

## Jobs

Data Deduplication uses a post-processing strategy to optimize and maintain a volume's space efficiency.

| JOB NAME | JOB DESCRIPTIONS | DEFAULT SCHEDULE |
| --- | --- | --- |
| Optimization | The **Optimization** job deduplicates by chunking data on a volume per the volume policy settings, (optionally) compressing those chunks, and storing chunks uniquely in the chunk store. The optimization process that Data Deduplication uses is described in detail in How does Data Deduplication work?. | Once every hour |
| Garbage Collection | The **Garbage Collection** job reclaims disk space by removing unnecessary chunks that are no longer being referenced by files that have been recently modified or deleted. | Every Saturday at 2:35 AM |

| JOB NAME | JOB DESCRIPTIONS | DEFAULT SCHEDULE |
| --- | --- | --- |
| Integrity Scrubbing | The **Integrity Scrubbing** job identifies corruption in the chunk store due to disk failures or bad sectors. When possible, Data Deduplication can automatically use volume features (such as mirror or parity on a Storage Spaces volume) to reconstruct the corrupted data. Additionally, Data Deduplication keeps backup copies of popular chunks when they are referenced more than 100 times in an area called the hotspot. | Every Saturday at 3:35 AM |
| Unoptimization | The **Unoptimization** job, which is a special job that should only be run manually, undoes the optimization done by deduplication and disables Data Deduplication for that volume. | On-demand only |

## Data Deduplication terminology

| TERM | DEFINITION |
| --- | --- |
| Chunk | A chunk is a section of a file that has been selected by the Data Deduplication chunking algorithm as likely to occur in other, similar files. |
| Chunk store | The chunk store is an organized series of container files in the System Volume Information folder that Data Deduplication uses to uniquely store chunks. |
| Dedup | An abbreviation for Data Deduplication that's commonly used in PowerShell, Windows Server APIs and components, and the Windows Server community. |
| File metadata | Every file contains metadata that describes interesting properties about the file that are not related to the main content of the file. For instance, Date Created, Last Read Date, Author, etc. |
| File stream | The file stream is the main content of the file. This is the part of the file that Data Deduplication optimizes. |
| File system | The file system is the software and on-disk data structure that the operating system uses to store files on storage media. Data Deduplication is supported on NTFS formatted volumes. |
| File system filter | A file system filter is a plugin that modifies the default behavior of the file system. To preserve access semantics, Data Deduplication uses a file system filter (Dedup.sys) to redirect reads to optimized content completely transparently to the user or application that makes the read request. |
| Optimization | A file is considered optimized (or deduplicated) by Data Deduplication if it has been chunked, and its unique chunks have been stored in the chunk store. |

| TERM | DEFINITION |
| --- | --- |
| Optimization policy | The optimization policy specifies the files that should be considered for Data Deduplication. For example, files may be considered out-of-policy if they are brand new, open, in a certain path on the volume, or a certain file type. |
| Reparse point | A reparse point is a special tag that notifies the file system to pass off I/O to a specified file system filter. When a file's file stream has been optimized, Data Deduplication replaces the file stream with a reparse point, which enables Data Deduplication to preserve the access semantics for that file. |
| Volume | A volume is a Windows construct for a logical storage drive that may span multiple physical storage devices across a one or more servers. Deduplication is enabled on a volume-by-volume basis. |
| Workload | A workload is an application that runs on Windows Server. Example workloads include general purpose file server, Hyper-V, and SQL Server. |

**WARNING**

Unless instructed by authorized Microsoft Support Personnel, do not attempt to manually modify the chunk store. Doing so may result in data corruption or loss.

## Frequently asked questions

**How does Data Deduplication differ from other optimization products?** There are several important differences between Data Deduplication and other common storage optimization products:

- *How does Data Deduplication differ from Single Instance Store?* Single Instance Store, or SIS, is a technology that preceded Data Deduplication and was first introduced in Windows Storage Server 2008 R2. To optimize a volume, Single Instance Store identified files that were completely identical and replaced them with logical links to a single copy of a file that's stored in the SIS common store. Unlike Single Instance Store, Data Deduplication can get space savings from files that are not identical but share many common patterns and from files that themselves contain many repeated patterns. Single Instance Store was deprecated in Windows Server 2012 R2 and removed in Windows Server 2016 in favor of Data Deduplication.
- *How does Data Deduplication differ from NTFS compression?* NTFS compression is a feature of NTFS that you can optionally enable at the volume level. With NTFS compression, each file is optimized individually via compression at write-time. Unlike NTFS compression, Data Deduplication can get spacing savings across all the files on a volume. This is better than NTFS compression because files may have both internal duplication (which is addressed by NTFS compression) and have similarities with other files on the volume (which is not addressed by NTFS compression). Additionally, Data Deduplication has a post-processing model, which means that new or modified files will be written to disk unoptimized and will be optimized later by Data Deduplication.
- *How does Data Deduplication differ from archive file formats like zip, rar, 7z, cab, etc.?* Archive file formats, like zip, rar, 7z, cab, etc., perform compression over a specified set of files. Like Data Deduplication, duplicated patterns within files and duplicated patterns across files are optimized. However, you have to choose the files that you want to include in the archive. Access semantics are different, too. To access a specific file within the archive, you have to open the archive, select a specific file, and decompress that file for use. Data Deduplication operates transparently to users and administrators and requires no manual kick-

off. Additionally, Data Deduplication preserves access semantics: optimized files appear unchanged after optimization.

**Can I change the Data Deduplication settings for my selected Usage Type?** Yes. Although Data Deduplication provides reasonable defaults for **Recommended workloads**, you might still want to tweak Data Deduplication settings to get the most out of your storage. Additionally, other workloads will require some tweaking to ensure that Data Deduplication does not interfere with the workload.

**Can I manually run a Data Deduplication job?** Yes, all Data Deduplication jobs may be run manually. This may be desirable if scheduled jobs did not run due to insufficient system resources or because of an error. Additionally, the Unoptimization job can only be run manually.

**Can I monitor the historical outcomes of Data Deduplication jobs?** Yes, all Data Deduplication jobs make entries in the Windows Event Log.

**Can I change the default schedules for the Data Deduplication jobs on my system?** Yes, all schedules are configurable. Modifying the default Data Deduplication schedules is particularly desirable to ensure that the Data Deduplication jobs have time to finish and do not compete for resources with the workload.

# Install and enable Data Deduplication

11/2/2020 • 8 minutes to read • Edit Online

Applies to Windows Server (Semi-Annual Channel), Windows Server 2016

This topic explains how to install Data Deduplication, evaluate workloads for deduplication, and enable Data Deduplication on specific volumes.

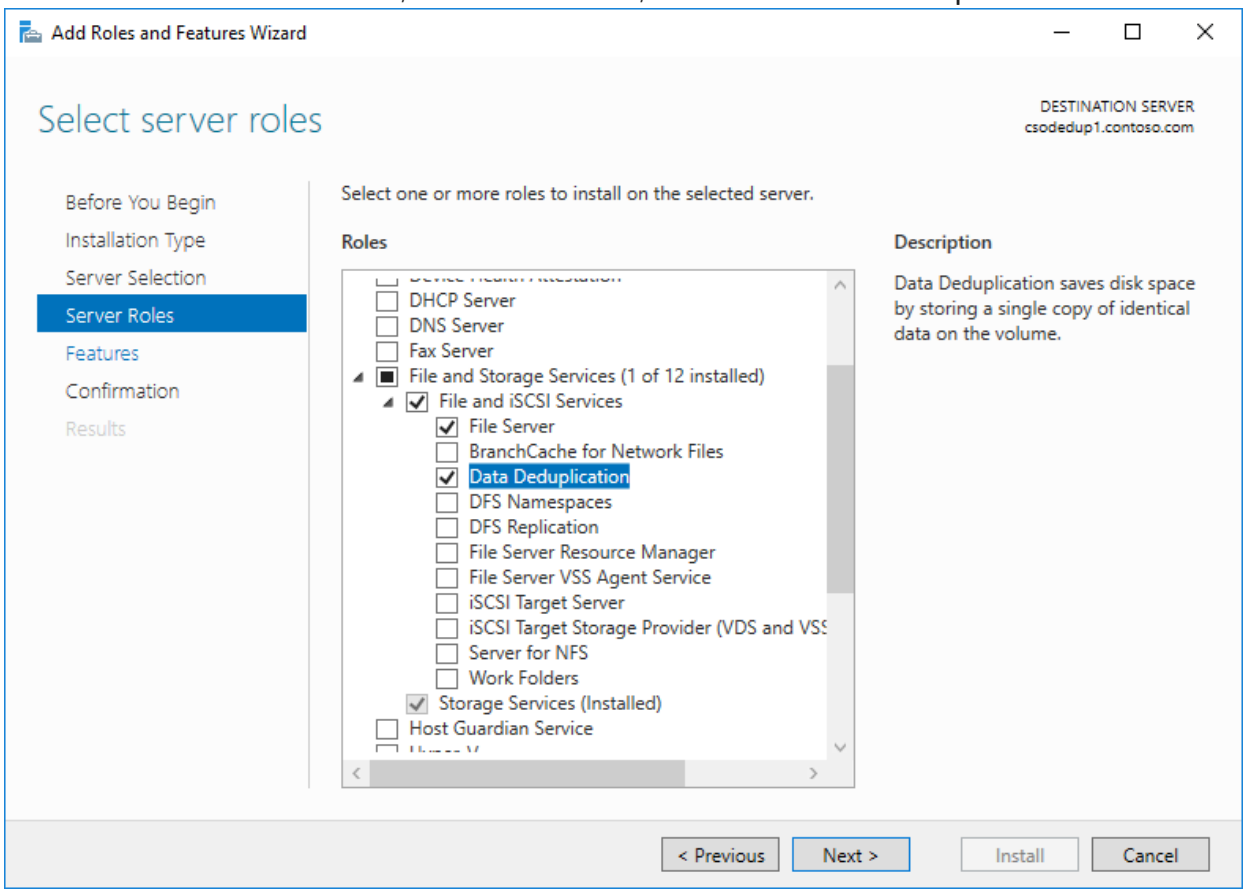
> **NOTE**
> If you're planning to run Data Deduplication in a Failover Cluster, every node in the cluster must have the Data Deduplication server role installed.

## Install Data Deduplication

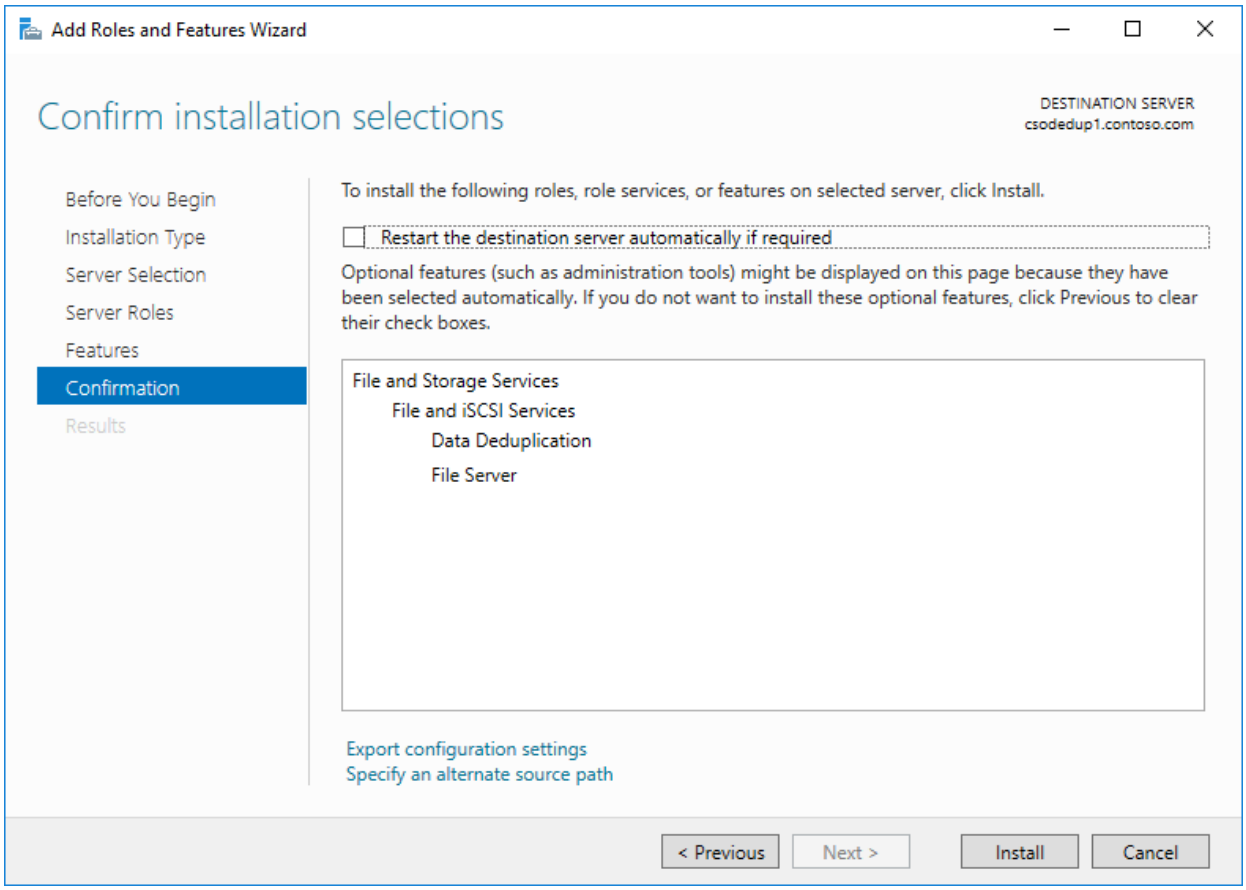
> **IMPORTANT**
> KB4025334 contains a roll up of fixes for Data Deduplication, including important reliability fixes, and we strongly recommend installing it when using Data Deduplication with Windows Server 2016.

### Install Data Deduplication by using Server Manager

1. In the Add Roles and Feature wizard, select **Server Roles**, and then select **Data Deduplication**.




2. Click **Next** until the **Install** button is active, and then click **Install**.




### Install Data Deduplication by using PowerShell

To install Data Deduplication, run the following PowerShell command as an administrator:

```
Install-WindowsFeature -Name FS-Data-Deduplication
```

To install Data Deduplication in a Nano Server installation:

1. Create a Nano Server installation with the Storage installed as described in Getting Started with Nano Server.
2. From a server running Windows Server 2016 in any mode other than Nano Server, or from a Windows PC with the Remote Server Administration Tools (RSAT) installed, install Data Deduplication with an explicit reference to the Nano Server instance (replace 'MyNanoServer' with the real name of the Nano Server instance):

   ```
   Install-WindowsFeature -ComputerName <MyNanoServer> -Name FS-Data-Deduplication
   ```

   -- OR --

   Connect remotely to the Nano Server instance with PowerShell remoting and install Data Deduplication by using DISM:

   ```
   Enter-PSSession -ComputerName MyNanoServer
   dism /online /enable-feature /featurename:dedup-core /all
   ```

## Enable Data Deduplication

### Determine which workloads are candidates for Data Deduplication

Data Deduplication can effectively minimize the costs of a server application's data consumption by reducing the amount of disk space consumed by redundant data. Before enabling deduplication, it is important that you

understand the characteristics of your workload to ensure that you get the maximum performance out of your storage. There are two classes of workloads to consider:

- *Recommended workloads* that have been proven to have both datasets that benefit highly from deduplication and have resource consumption patterns that are compatible with Data Deduplication's post-processing model. We recommend that you always enable Data Deduplication on these workloads:
  - General purpose file servers (GPFS) serving shares such as team shares, user home folders, work folders, and software development shares.
  - Virtualized desktop infrastructure (VDI) servers.
  - Virtualized backup applications, such as Microsoft Data Protection Manager (DPM).
- Workloads that might benefit from deduplication, but aren't always good candidates for deduplication. For example, the following workloads could work well with deduplication, but you should evaluate the benefits of deduplication first:
  - General purpose Hyper-V hosts
  - SQL servers
  - Line-of-business (LOB) servers

**Evaluate workloads for Data Deduplication**

> **IMPORTANT**
> If you are running a recommended workload, you can skip this section and go to Enable Data Deduplication for your workload.

To determine whether a workload works well with deduplication, answer the following questions. If you're unsure about a workload, consider doing a pilot deployment of Data Deduplication on a test dataset for your workload to see how it performs.

1. **Does my workload's dataset have enough duplication to benefit from enabling deduplication?** Before enabling Data Deduplication for a workload, investigate how much duplication your workload's dataset has by using the Data Deduplication Savings Evaluation tool, or DDPEval. After installing Data Deduplication, you can find this tool at `C:\Windows\System32\DDPEval.exe`. DDPEval can evaluate the potential for optimization against directly connected volumes (including local drives or Cluster Shared Volumes) and mapped or unmapped network shares. Running DDPEval.exe will return an output similar to the following:

   ```
   Data Deduplication Savings Evaluation Tool
   Copyright 2011-2012 Microsoft Corporation. All Rights Reserved.  Evaluated folder: E:\Test
   Processed files: 34  Processed files size: 12.03MB  Optimized files size: 4.02MB  Space savings: 8.01MB
   Space savings percent: 66  Optimized files size (no compression): 11.47MB
   Space savings (no compression): 571.53KB  Space savings percent (no compression): 4
   Files with duplication: 2  Files excluded by policy: 20  Files excluded by error: 0
   ```

2. **What do my workload's I/O patterns to its dataset look like? What performance do I have for my workload?** Data Deduplication optimizes files as a periodic job, rather than when the file is written to disk. As a result, it is important to examine is a workload's expected read patterns to the deduplicated volume. Because Data Deduplication moves file content into the Chunk Store and attempts to organize the Chunk Store by file as much as possible, read operations perform best when they are applied to sequential ranges of a file.

   Database-like workloads typically have more random read patterns than sequential read patterns because databases do not typically guarantee that the database layout will be optimal for all possible queries that may be run. Because the sections of the Chunk Store may exist all over the volume, accessing data ranges in the Chunk Store for database queries may introduce additional latency. High performance workloads are particularly sensitive to this extra latency, but other database-like workloads might not be.

> **NOTE**
>
> These concerns primarily apply to storage workloads on volumes made up of traditional rotational storage media (also known as Hard Disk drives, or HDDs). All-flash storage infrastructure (also known as Solid State Disk drives, or SSDs), is less affected by random I/O patterns because one of the properties of flash media is equal access time to all locations on the media. Therefore, deduplication will not introduce the same amount of latency for reads to a workload's datasets stored on all-flash media as it would on traditional rotational storage media.

3. **What are the resource requirements of my workload on the server?** Because Data Deduplication uses a post-processing model, Data Deduplication periodically needs to have sufficient system resources to complete its optimization and other jobs. This means that workloads that have idle time, such as in the evening or on weekends, are excellent candidates for deduplication, and workloads that run all day, every day may not be. Workloads that have no idle time may still be good candidates for deduplication if the workload does not have high resource requirements on the server.

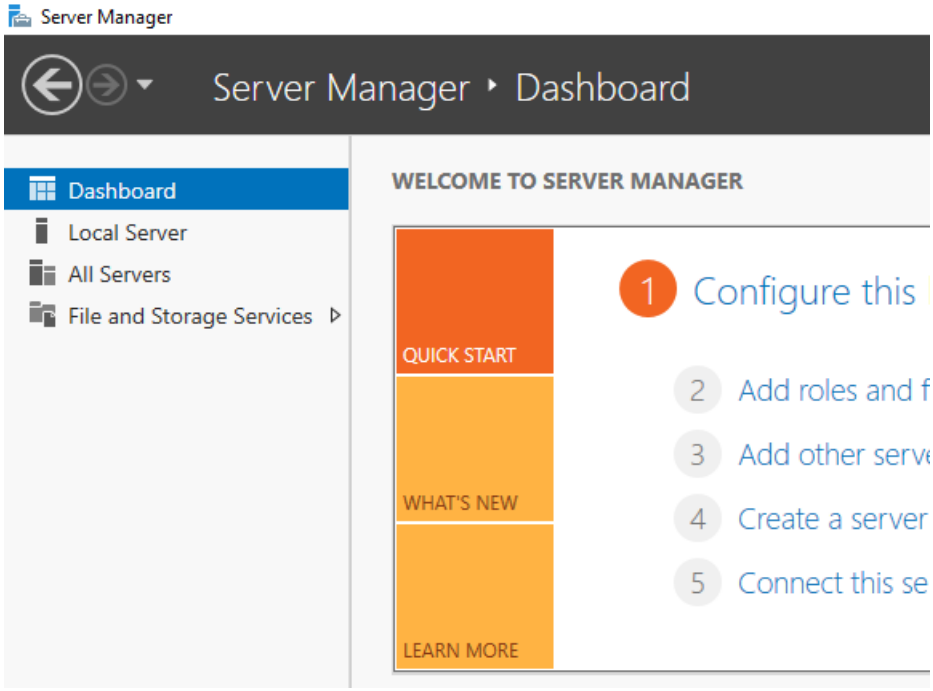
### Enable Data Deduplication

Before enabling Data Deduplication, you must choose the Usage Type that most closely resembles your workload. There are three Usage Types included with Data Deduplication.

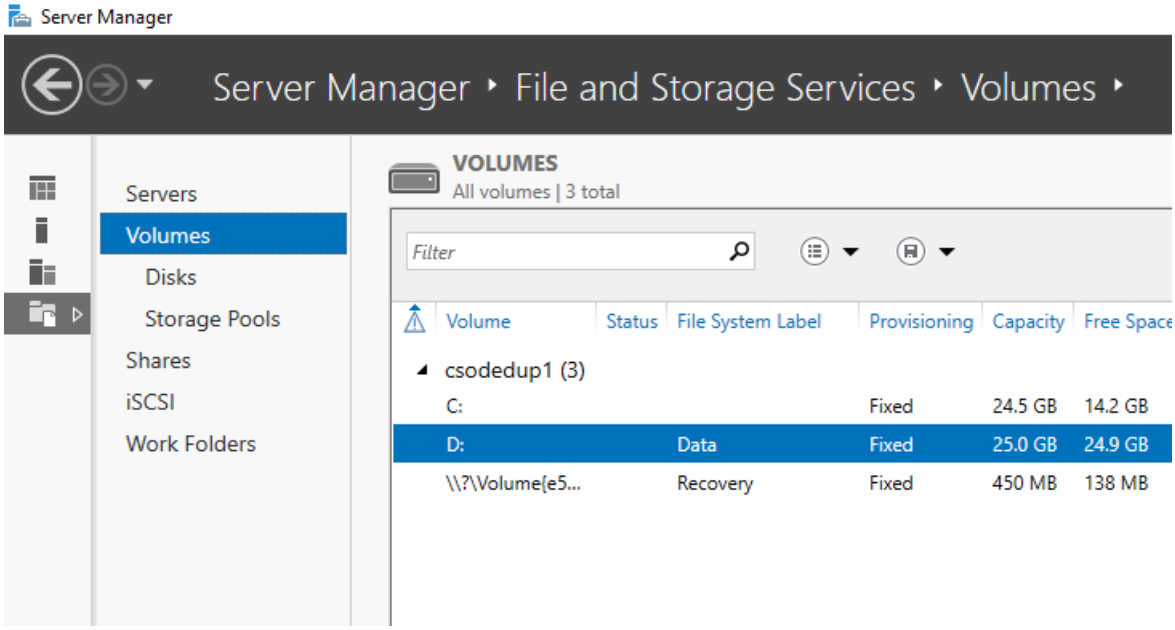
- Default - tuned specifically for general purpose file servers
- Hyper-V - tuned specifically for VDI servers
- Backup - tuned specifically for virtualized backup applications, such as Microsoft DPM

#### Enable Data Deduplication by using Server Manager

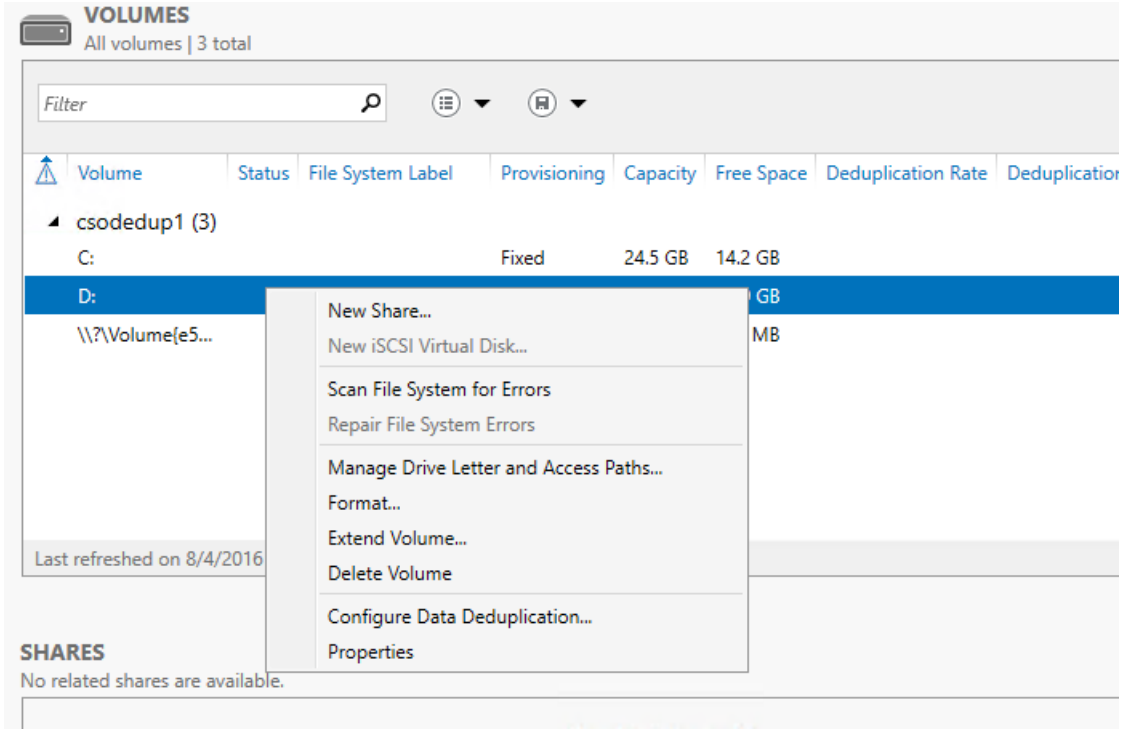
1. Select **File and Storage Services** in Server Manager.



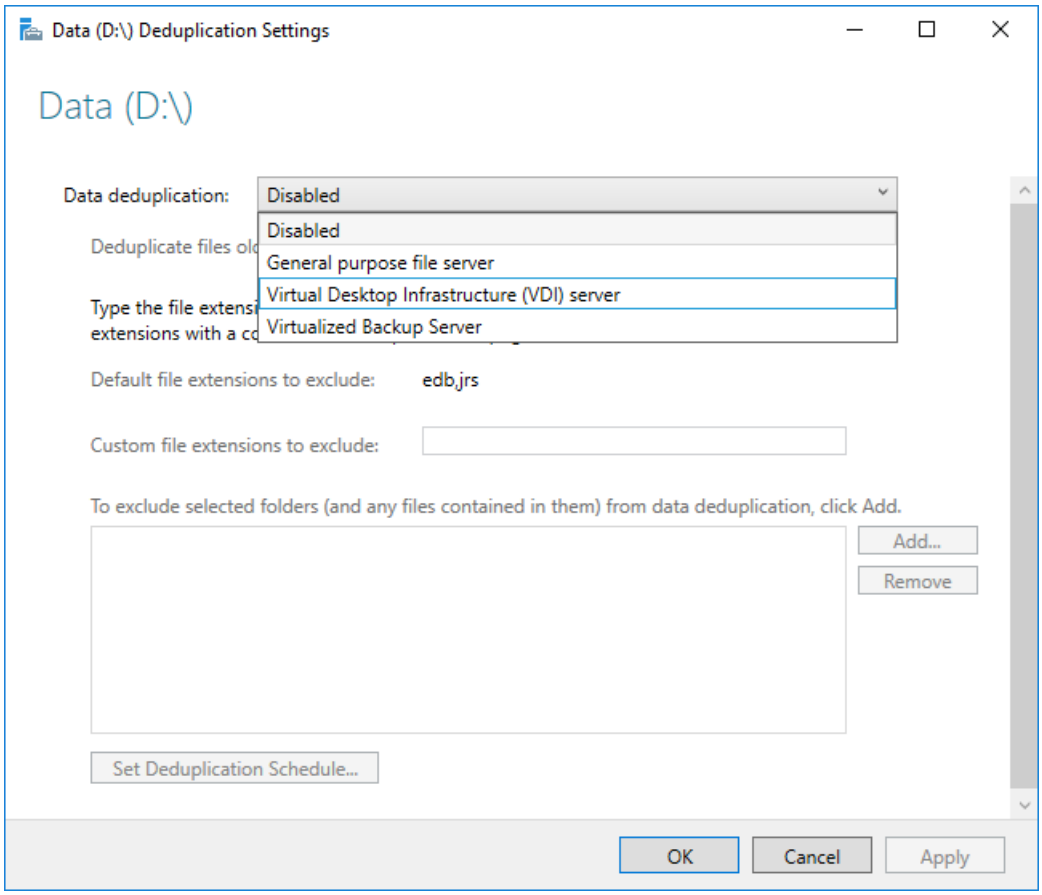

2. Select **Volumes** from **File and Storage Services**.




3. Right-click the desired volume and select **Configure Data Deduplication**.




4. Select the desired **Usage Type** from the drop-down box and select **OK**.




5. If you are running a recommended workload, you're done. For other workloads, see Other considerations.

> **NOTE**
> You can find more information on excluding file extensions or folders and selecting the deduplication schedule, including why you would want to do this, in Configuring Data Deduplication.

#### Enable Data Deduplication by using PowerShell

1. With an administrator context, run the following PowerShell command:

```
Enable-DedupVolume -Volume <Volume-Path> -UsageType <Selected-Usage-Type>
```

2. If you are running a recommended workload, you're done. For other workloads, see Other considerations.

> **NOTE**
> The Data Deduplication PowerShell cmdlets, including `Enable-DedupVolume`, can be run remotely by appending the `-CimSession` parameter with a CIM Session. This is particularly useful for running the Data Deduplication PowerShell cmdlets remotely against a Nano Server instance. To create a new CIM Session run `New-CimSession`.

#### Other considerations

> **IMPORTANT**
> If you are running a recommended workload, you can skip this section.

- Data Deduplication's Usage Types give sensible defaults for recommended workloads, but they also provide a good starting point for all workloads. For workloads other than the recommended workloads, it is possible to modify Data Deduplication's advanced settings to improve deduplication performance.

- If your workload has high resource requirements on your server, the Data Deduplication jobs should be scheduled to run during the expected idle times for that workload. This is particularly important when running deduplication on a hyper-converged host, because running Data Deduplication during expected working hours can starve VMs.
- If your workload does not have high resource requirements, or if it is more important that optimization jobs complete than workload requests be served, the memory, CPU, and priority of the Data Deduplication jobs can be adjusted.

## Frequently asked questions (FAQ)

**I want to run Data Deduplication on the dataset for X workload. Is this supported?** Aside from workloads that are known not to interoperate with Data Deduplication, we fully support the data integrity of Data Deduplication with any workload. Recommended workloads are supported by Microsoft for performance as well. The performance of other workloads depends greatly on what they are doing on your server. You must determine what performance impacts Data Deduplication has on your workload, and if this is acceptable for this workload.

**What are the volume sizing requirements for deduplicated volumes?** In Windows Server 2012 and Windows Server 2012 R2, volumes had to be carefully sized to ensure that Data Deduplication could keep up with the churn on the volume. This typically meant that the average maximum size of a deduplicated volume for a high-churn workload was 1-2 TB, and the absolute maximum recommended size was 10 TB. In Windows Server 2016, these limitations were removed. For more information, see What's new in Data Deduplication.

**Do I need to modify the schedule or other Data Deduplication settings for recommended workloads?** No, the provided Usage Types were created to provide reasonable defaults for recommended workloads.

**What are the memory requirements for Data Deduplication?** At a minimum, Data Deduplication should have 300 MB + 50 MB for each TB of logical data. For instance, if you are optimizing a 10 TB volume, you would need a minimum of 800 MB of memory allocated for deduplication ( `300 MB + 50 MB * 10 = 300 MB + 500 MB = 800 MB` ). While Data Deduplication can optimize a volume with this low amount of memory, having such constrained resources will slow down Data Deduplication's jobs.

Optimally, Data Deduplication should have 1 GB of memory for every 1 TB of logical data. For instance, if you are optimizing a 10 TB volume, you would optimally need 10 GB of memory allocated for Data Deduplication ( `1 GB * 10` ). This ratio will ensure the maximum performance for Data Deduplication jobs.

**What are the storage requirements for Data Deduplication?** In Windows Server 2016, Data Deduplication can support volume sizes up to 64 TB. For more information, view What's new in Data Deduplication.

# Running Data Deduplication

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

## Running Data Deduplication jobs manually

You can run every scheduled Data Deduplication job manually by using the following PowerShell cmdlets:

- `Start-DedupJob`: Starts a new Data Deduplication job
- `Stop-DedupJob`: Stops a Data Deduplication job already in progress (or removes it from the queue)
- `Get-DedupJob`: Shows all the active and queued Data Deduplication jobs

All settings that are available when you schedule a Data Deduplication job are also available when you start a job manually except for the scheduling-specific settings. For example, to start an Optimization job manually with high priority, maximum CPU usage, and maximum memory usage, execute the following PowerShell command with administrator privilege:

```
Start-DedupJob -Type Optimization -Volume <Your-Volume-Here> -Memory 100 -Cores 100 -Priority High
```

## Monitoring Data Deduplication

**Job successes**

Because Data Deduplication uses a post-processing model, it is important that Data Deduplication jobs succeed. An easy way to check the status of the most recent job is to use the `Get-DedupStatus` PowerShell cmdlet. Periodically check the following fields:

- For the Optimization job, look at `LastOptimizationResult` (0 = Success), `LastOptimizationResultMessage`, and `LastOptimizationTime` (should be recent).
- For the Garbage Collection job, look at `LastGarbageCollectionResult` (0 = Success), `LastGarbageCollectionResultMessage`, and `LastGarbageCollectionTime` (should be recent).
- For the Integrity Scrubbing job, look at `LastScrubbingResult` (0 = Success), `LastScrubbingResultMessage`, and `LastScrubbingTime` (should be recent).

> **NOTE**
> More detail on job successes and failures can be found in the Windows Event Viewer under `\Applications and Services Logs\Windows\Deduplication\Operational`.

**Optimization rates**

One indicator of Optimization job failure is a downward-trending optimization rate which might indicate that the Optimization jobs are not keeping up with the rate of changes, or churn. You can check the optimization rate by using the `Get-DedupStatus` PowerShell cmdlet.

**IMPORTANT**

`Get-DedupStatus` has two fields that are relevant to the optimization rate: `OptimizedFilesSavingsRate` and `SavingsRate`. These are both important values to track, but each has a unique meaning.

- `OptimizedFilesSavingsRate` applies only to the files that are 'in-policy' for optimization ( `space used by optimized files after optimization / logical size of optimized files` ).
- `SavingsRate` applies to the entire volume ( `space used by optimized files after optimization / total logical size of the optimization` ).

## Disabling Data Deduplication

To turn off Data Deduplication, run the Unoptimization job. To undo volume optimization, run the following command:

```
Start-DedupJob -Type Unoptimization -Volume <Desired-Volume>
```

**IMPORTANT**

The Unoptimization job will fail if the volume does not have sufficient space to hold the unoptimized data.

## Frequently Asked Questions

**Is there a System Center Operations Manager Management Pack available to monitor Data Deduplication?** Yes. Data Deduplication can be monitored through the System Center Management Pack for File Server. For more information, see the Guide for System Center Management Pack for File Server 2012 R2 document.

# Advanced Data Deduplication settings

12/16/2020 • 12 minutes to read • Edit Online

Applies to Windows Server (Semi-Annual Channel), Windows Server 2016

This document describes how to modify advanced Data Deduplication settings. For recommended workloads, the default settings should be sufficient. The main reason to modify these settings is to improve Data Deduplication's performance with other kinds of workloads.

## Modifying Data Deduplication job schedules

The default Data Deduplication job schedules are designed to work well for recommended workloads and be as non-intrusive as possible (excluding the *Priority Optimization* job that is enabled for the **Backup** usage type). When workloads have large resource requirements, it is possible to ensure that jobs run only during idle hours, or to reduce or increase the amount of system resources that a Data Deduplication job is allowed to consume.

### Changing a Data Deduplication schedule

Data Deduplication jobs are scheduled via Windows Task Scheduler and can be viewed and edited there under the path Microsoft\Windows\Deduplication. Data Deduplication includes several cmdlets that make scheduling easy.

- `Get-DedupSchedule` shows the current scheduled jobs.
- `New-DedupSchedule` creates a new scheduled job.
- `Set-DedupSchedule` modifies an existing scheduled job.
- `Remove-DedupSchedule` removes a scheduled job.

The most common reason for changing when Data Deduplication jobs run is to ensure that jobs run during off hours. The following step-by-step example shows how to modify the Data Deduplication schedule for a *sunny day* scenario: a hyper-converged Hyper-V host that is idle on weekends and after 7:00 PM on weeknights. To change the schedule, run the following PowerShell cmdlets in an Administrator context.

1. Disable the scheduled hourly Optimization jobs.

```
Set-DedupSchedule -Name BackgroundOptimization -Enabled $false
Set-DedupSchedule -Name PriorityOptimization -Enabled $false
```

2. Remove the currently scheduled Garbage Collection and Integrity Scrubbing jobs.

```
Get-DedupSchedule -Type GarbageCollection | ForEach-Object { Remove-DedupSchedule -InputObject $_ }
Get-DedupSchedule -Type Scrubbing | ForEach-Object { Remove-DedupSchedule -InputObject $_ }
```

3. Create a nightly Optimization job that runs at 7:00 PM with high priority and all the CPUs and memory available on the system.

```
New-DedupSchedule -Name "NightlyOptimization" -Type Optimization -DurationHours 11 -Memory 100 -Cores
100 -Priority High -Days @(1,2,3,4,5) -Start (Get-Date "2016-08-08 19:00:00")
```

> **NOTE**
> The *date* part of the `System.Datetime` provided to `-Start` is irrelevant (as long as it's in the past), but the *time* part specifies when the job should start.

4. Create a weekly Garbage Collection job that runs on Saturday starting at 7:00 AM with high priority and all the CPUs and memory available on the system.

```
New-DedupSchedule -Name "WeeklyGarbageCollection" -Type GarbageCollection -DurationHours 23 -Memory
100 -Cores 100 -Priority High -Days @(6) -Start (Get-Date "2016-08-13 07:00:00")
```

5. Create a weekly Integrity Scrubbing job that runs on Sunday starting at 7 AM with high priority and all the CPUs and memory available on the system.

```
New-DedupSchedule -Name "WeeklyIntegrityScrubbing" -Type Scrubbing -DurationHours 23 -Memory 100 -
Cores 100 -Priority High -Days @(0) -Start (Get-Date "2016-08-14 07:00:00")
```

### Available job-wide settings

You can toggle the following settings for new or scheduled Data Deduplication jobs:

| PARAMETER NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO SET THIS VALUE? |
|---|---|---|---|
| Type | The type of the job that should be scheduled | • Optimization<br>• GarbageCollection<br>• Scrubbing | This value is required because it is the type of job that you want to have be scheduled. This value cannot be changed after the task has been scheduled. |
| Priority | The system priority of the scheduled job | • High<br>• Medium<br>• Low | This value helps the system determine how to allocate CPU time. *High* will use more CPU time, *low* will use less. |
| Days | The days that the job is scheduled | An array of integers 0-6 representing the days of the week:<br>• 0 = Sunday<br>• 1 = Monday<br>• 2 = Tuesday<br>• 3 = Wednesday<br>• 4 = Thursday<br>• 5 = Friday<br>• 6 = Saturday | Scheduled tasks have to run on at least one day. |
| Cores | The percentage of cores on the system that a job should use | Integers 0-100 (indicates a percentage) | To control what level of impact a job will have on the compute resources on the system |

| PARAMETER NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO SET THIS VALUE? |
|---|---|---|---|
| DurationHours | The maximum number of hours a job should be allowed to run | Positive integers | To prevent a job for running into a workload's non-idle hours |
| Enabled | Whether the job will run | True/false | To disable a job without removing it |
| Full | For scheduling a full Garbage Collection job | Switch (true/false) | By default, every fourth job is a full Garbage Collection job. With this switch, you can schedule full Garbage Collection to run more frequently. |
| InputOutputThrottle | Specifies the amount of input/output throttling applied to the job | Integers 0-100 (indicates a percentage) | Throttling ensures that jobs don't interfere with other I/O-intensive processes. |
| Memory | The percentage of memory on the system that a job should use | Integers 0-100 (indicates a percentage) | To control what level of impact the job will have on the memory resources of the system |
| Name | The name of the scheduled job | String | A job must have a uniquely identifiable name. |
| ReadOnly | Indicates that the scrubbing job processes and reports on corruptions that it finds, but does not run any repair actions | Switch (true/false) | You want to manually restore files that sit on bad sections of the disk. |
| Start | Specifies the time a job should start | `System.DateTime` | The *date* part of the `System.Datetime` provided to *Start* is irrelevant (as long as it's in the past), but the *time* part specifies when the job should start. |
| StopWhenSystemBusy | Specifies whether Data Deduplication should stop if the system is busy | Switch (True/False) | This switch gives you the ability to control the behavior of Data Deduplication--this is especially important if you want to run Data Deduplication while your workload is not idle. |

# Modifying Data Deduplication volume-wide settings

### Toggling volume settings

You can set the volume-wide default settings for Data Deduplication via the usage type that you select when you enable a deduplication for a volume. Data Deduplication includes cmdlets that make editing volume-wide settings easy:

- `Get-DedupVolume`
- `Set-DedupVolume`

The main reasons to modify the volume settings from the selected usage type are to improve read performance for specific files (such as multimedia or other file types that are already compressed) or to fine-tune Data Deduplication for better optimization for your specific workload. The following example shows how to modify the Data Deduplication volume settings for a workload that most closely resembles a general purpose file server workload, but uses large files that change frequently.

1. See the current volume settings for Cluster Shared Volume 1.

   ```
   Get-DedupVolume -Volume C:\ClusterStorage\Volume1 | Select *
   ```

2. Enable OptimizePartialFiles on Cluster Shared Volume 1 so that the MinimumFileAge policy applies to sections of the file rather than the whole file. This ensures that the majority of the file gets optimized even though sections of the file change regularly.

   ```
   Set-DedupVolume -Volume C:\ClusterStorage\Volume1 -OptimizePartialFiles
   ```

**Available volume-wide settings**

| SETTING NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO MODIFY THIS VALUE? |
|---|---|---|---|
| ChunkRedundancyThreshold | The number of times that a chunk is referenced before a chunk is duplicated into the hotspot section of the Chunk Store. The value of the hotspot section is that so-called "hot" chunks that are referenced frequently have multiple access paths to improve access time. | Positive integers | The main reason to modify this number is to increase the savings rate for volumes with high duplication. In general, the default value (100) is the recommended setting, and you shouldn't need to modify this. |
| ExcludeFileType | File types that are excluded from optimization | Array of file extensions | Some file types, particularly multimedia or files that are already compressed, do not benefit very much from being optimized. This setting allows you to configure which types are excluded. |
| ExcludeFolder | Specifies folder paths that should not be considered for optimization | Array of folder paths | If you want to improve performance or keep content in particular paths from being optimized, you can exclude certain paths on the volume from consideration for optimization. |

| SETTING NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO MODIFY THIS VALUE? |
| --- | --- | --- | --- |
| InputOutputScale | Specifies the level of IO parallelization (IO queues) for Data Deduplication to use on a volume during a post-processing job | Positive integers ranging 1-36 | The main reason to modify this value is to decrease the impact on the performance of a high IO workload by restricting the number of IO queues that Data Deduplication is allowed to use on a volume. Note that modifying this setting from the default may cause Data Deduplication's post-processing jobs to run slowly. |
| MinimumFileAgeDays | Number of days after the file is created before the file is considered to be in-policy for optimization. | Positive integers (inclusive of zero) | The **Default** and **HyperV** usage types set this value to 3 to maximize performance on hot or recently created files. You may want to modify this if you want Data Deduplication to be more aggressive or if you do not care about the extra latency associated with deduplication. |
| MinimumFileSize | Minimum file size that a file must have to be considered in-policy for optimization | Positive integers (bytes) greater than 32 KB | The main reason to change this value is to exclude small files that may have limited optimization value to conserve compute time. |
| NoCompress | Whether the chunks should be compressed before being put into the Chunk Store | True/False | Some types of files, particularly multimedia files and already compressed file types, may not compress well. This setting allows you to turn off compression for all files on the volume. This would be ideal if you are optimizing a dataset that has a lot of files that are already compressed. |
| NoCompressionFileType | File types whose chunks should not be compressed before going into the Chunk Store | Array of file extensions | Some types of files, particularly multimedia files and already compressed file types, may not compress well. This setting allows compression to be turned off for those files, saving CPU resources. |

| SETTING NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO MODIFY THIS VALUE? |
|---|---|---|---|
| OptimizeInUseFiles | When enabled, files that have active handles against them will be considered as in-policy for optimization. | True/false | Enable this setting if your workload keeps files open for extended periods of time. If this setting is not enabled, a file would never get optimized if the workload has an open handle to it, even if it's only occasionally appending data at the end. |
| OptimizePartialFiles | When enabled, the MinimumFileAge value applies to segments of a file rather than to the whole file. | True/false | Enable this setting if your workload works with large, often edited files where most of the file content is untouched. If this setting is not enabled, these files would never get optimized because they keep getting changed, even though most of the file content is ready to be optimized. |
| Verify | When enabled, if the hash of a chunk matches a chunk we already have in our Chunk Store, the chunks are compared byte-by-byte to ensure they are identical. | True/false | This is an integrity feature that ensures that the hashing algorithm that compares chunks does not make a mistake by comparing two chunks of data that are actually different but have the same hash. In practice, it is extremely improbable that this would ever happen. Enabling the verification feature adds significant overhead to the optimization job. |

## Modifying Data Deduplication system-wide settings

Data Deduplication has additional system-wide settings that can be configured via the registry. These settings apply to all of the jobs and volumes that run on the system. Extra care must be given whenever editing the registry.

For example, you may want to disable full Garbage Collection. More information about why this may be useful for your scenario can be found in Frequently asked questions. To edit the registry with PowerShell:

- If Data Deduplication is running in a cluster:

```
  Set-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\ddpsvc\Settings -Name DeepGCInterval -
Type DWord -Value 0xFFFFFFFF
  Set-ItemProperty -Path HKLM:\CLUSTER\Dedup -Name DeepGCInterval -Type DWord -Value 0xFFFFFFFF
```

- If Data Deduplication is not running in a cluster:

```
  Set-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\ddpsvc\Settings -Name DeepGCInterval -
Type DWord -Value 0xFFFFFFFF
```

**Available system-wide settings**

| SETTING NAME | DEFINITION | ACCEPTED VALUES | WHY WOULD YOU WANT TO CHANGE THIS? |
|---|---|---|---|
| WlmMemoryOverPercentThreshold | This setting allows jobs to use more memory than Data Deduplication judges to actually be available. For example, a setting of 300 would mean that the job would have to use three times the assigned memory to get canceled. | Positive integers (a value of 300 means 300% or 3 times) | If you have another task that will stop if Data Deduplication takes more memory |
| DeepGCInterval | This setting configures the interval at which regular Garbage Collection jobs become full Garbage Collection jobs. A setting of n would mean that every $n^{th}$ job was a full Garbage Collection job. Note that full Garbage Collection is always disabled (regardless of the registry value) for volumes with the Backup Usage Type. `Start-DedupJob -Type GarbageCollection -Full` may be used if full Garbage Collection is desired on a Backup volume. | Integers (-1 indicates disabled) | See this frequently asked question |

# Frequently asked questions

**I changed a Data Deduplication setting, and now jobs are slow or don't finish, or my workload performance has decreased. Why?** These settings give you a lot of power to control how Data Deduplication runs. Use them responsibly, and monitor performance.

**I want to run a Data Deduplication job right now, but I don't want to create a new schedule--can I do this?** Yes, all jobs can be run manually.

**What is the difference between full and regular Garbage Collection?** There are two types of Garbage Collection:

- *Regular Garbage Collection* uses a statistical algorithm to find large unreferenced chunks that meet a certain criteria (low in memory and IOPs). Regular Garbage Collection compacts a chunk store container only if a minimum percentage of the chunks are unreferenced. This type of Garbage Collection runs much faster and uses fewer resources than full Garbage Collection. The default schedule of the regular Garbage Collection job is to run once a week.
- *Full Garbage Collection* does a much more thorough job of finding unreferenced chunks and freeing more disk space. Full Garbage Collection compacts every container even if just a single chunk in the container is unreferenced. Full Garbage Collection will also free space that may have been in use if there was a crash or power failure during an Optimization job. Full Garbage Collection jobs will recover 100 percent of the available space that can be recovered on a deduplicated volume at the cost of requiring more time and system resources

compared to a regular Garbage Collection job. The full Garbage Collection job will typically find and release up to 5 percent more of the unreferenced data than a regular Garbage Collection job. The default schedule of the full Garbage Collection job is to run every fourth time Garbage Collection is scheduled.

### Why would I want to disable full Garbage Collection?

- Garbage Collection could adversely affect the volume's lifetime shadow copies and the size of incremental backup. High churn or I/O-intensive workloads may see a degradation in performance by full Garbage Collection jobs.
- You can manually run a full Garbage Collection job from PowerShell to clean up leaks if you know your system crashed.

# Data Deduplication interoperability

12/16/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2019

## Supported

### ReFS

Data Deduplication is supported as of Windows Server 2019.

### Failover Clustering

Failover Clustering is fully supported, if every node in the cluster has the Data Deduplication feature installed. Other important notes:

- Manually started Data Deduplication jobs must be run on the Owner node for the Cluster Shared Volume.
- Scheduled Data Deduplication jobs are stored in the cluster task scheduled so that if a deduplicated volume is taken over by another node, the scheduled job will be applied on the next scheduled interval.
- Data Deduplication fully interoperates with the Cluster OS Rolling Upgrade feature.
- Data Deduplication is fully supported on Storage Spaces Direct NTFS-formatted volumes (mirror or parity). Deduplication is not supported on volumes with multiple tiers. See Data Deduplication on ReFS for more information.

### Storage Replica

Storage Replica is fully supported. Data Deduplication should be configured to not run on the secondary copy.

### BranchCache

You can optimize data access over the network by enabling BranchCache on servers and clients. When a BranchCache-enabled system communicates over a WAN with a remote file server that is running data deduplication, all of the deduplicated files are already indexed and hashed. Therefore, requests for data from a branch office are quickly computed. This is similar to preindexing or prehashing a BranchCache-enabled server.

### DFS Replication

Data Deduplication works with Distributed File System (DFS) Replication. Optimizing or unoptimizing a file will not trigger a replication because the file does not change. DFS Replication uses Remote Differential Compression (RDC), not the chunks in the chunk store, for over-the-wire savings. The files on the replica can also be optimized by using deduplication if the replica is using Data Deduplication.

### Quotas

Data Deduplication does not support creating a hard quota on a volume root folder that also has deduplication enabled. When a hard quota is present on a volume root, the actual free space on the volume and the quota-restricted space on the volume are not the same. This may cause deduplication optimization jobs to fail. It is possible however to creating a soft quota on a volume root that has deduplication enabled.

When quota is enabled on a deduplicated volume, quota uses the logical size of the file rather than the physical size of the file. Quota usage (including any quota thresholds) does not change when a file is processed by deduplication. All other quota functionality, including volume-root soft quotas and quotas on subfolders, works normally when using deduplication.

### Windows Server Backup

Windows Server Backup can back up an optimized volume as-is (that is, without removing deduplicated data). The

following steps show how to back up a volume and how to restore a volume or selected files from a volume.

1. Install Windows Server Backup.

```
Install-WindowsFeature -Name Windows-Server-Backup
```

2. Back up the E: volume to another volume by running the following command, substituting the correct volume names for your situation.

```
wbadmin start backup –include:E: -backuptarget:F: -quiet
```

3. Get the version ID of the backup you just created.

```
wbadmin get versions
```

   This output version ID will be a date and time string, for example: 08/18/2016-06:22.

4. Restore the entire volume.

```
wbadmin start recovery –version:02/16/2012-06:22 -itemtype:Volume  -items:E: -recoveryTarget:E:
```

   --OR--

   Restore a particular folder (in this case, the E:\Docs folder):

```
wbadmin start recovery –version:02/16/2012-06:22 -itemtype:File  -items:E:\Docs  -recursive
```

# Unsupported

**Windows 10 (client OS)**

Data Deduplication is not supported on Windows 10. There are several popular blog posts in the Windows community describing how to remove the binaries from Windows Server 2016 and install on Windows 10, but this scenario has not been validated as part of the development of Data Deduplication. Vote for this item for Windows 10 vNext on the Windows Server Storage UserVoice.

**Windows Search**

Windows Search doesn't support Data Deduplication. Data Deduplication uses reparse points, which Windows Search can't index, so Windows Search skips all deduplicated files, excluding them from the index. As a result, search results might be incomplete for deduplicated volumes. Vote for this item for Windows Server vNext on the Windows Server Storage UserVoice.

**Robocopy**

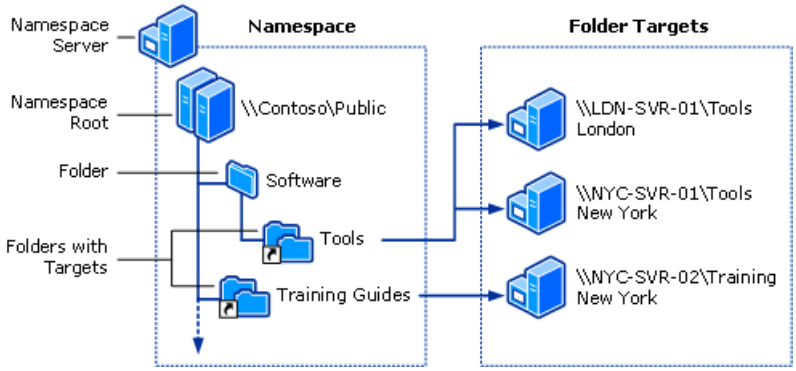
Running Robocopy with Data Deduplication is not recommended because certain Robocopy commands can corrupt the Chunk Store. The Chunk Store is stored in the System Volume Information folder for a volume. If the folder is deleted, the optimized files (reparse points) that are copied from the source volume become corrupted because the data chunks are not copied to the destination volume.

# DFS Namespaces overview

12/16/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server (Semi-Annual Channel)

DFS Namespaces is a role service in Windows Server that enables you to group shared folders located on different servers into one or more logically structured namespaces. This makes it possible to give users a virtual view of shared folders, where a single path leads to files located on multiple servers, as shown in the following figure:




Here's a description of the elements that make up a DFS namespace:

- **Namespace server** - A namespace server hosts a namespace. The namespace server can be a member server or a domain controller.
- **Namespace root** - The namespace root is the starting point of the namespace. In the previous figure, the name of the root is Public, and the namespace path is \\Contoso\Public. This type of namespace is a domain-based namespace because it begins with a domain name (for example, Contoso) and its metadata is stored in Active Directory Domain Services (AD DS). Although a single namespace server is shown in the previous figure, a domain-based namespace can be hosted on multiple namespace servers to increase the availability of the namespace.
- **Folder** - Folders without folder targets add structure and hierarchy to the namespace, and folders with folder targets provide users with actual content. When users browse a folder that has folder targets in the namespace, the client computer receives a referral that transparently redirects the client computer to one of the folder targets.
- **Folder targets** - A folder target is the UNC path of a shared folder or another namespace that is associated with a folder in a namespace. The folder target is where data and content is stored. In the previous figure, the folder named Tools has two folder targets, one in London and one in New York, and the folder named Training Guides has a single folder target in New York. A user who browses to \\Contoso\Public\Software\Tools is transparently redirected to the shared folder \\LDN-SVR-01\Tools or \\NYC-SVR-01\Tools, depending on which site the user is currently located in.

This topic discusses how to install DFS, what's new, and where to find evaluation and deployment information.

You can administer namespaces by using DFS Management, the DFS Namespace (DFSN) Cmdlets in Windows PowerShell, the **DfsUtil** command, or scripts that call WMI.

## Server requirements and limits

There are no additional hardware or software requirements for running DFS Management or using DFS Namespaces.

A namespace server is a domain controller or member server that hosts a namespace. The number of namespaces you can host on a server is determined by the operating system running on the namespace server.

Servers that are running the following operating systems can host multiple domain-based namespaces in addition to a single stand-alone namespace.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 Datacenter and Enterprise Editions
- Windows Server (Semi-Annual Channel)

Servers that are running the following operating systems can host a single stand-alone namespace:

- Windows Server 2008 R2 Standard

The following table describes additional factors to consider when choosing servers to host a namespace.

| SERVER HOSTING STAND-ALONE NAMESPACES | SERVER HOSTING DOMAIN-BASED NAMESPACES |
|---|---|
| Must contain an NTFS volume to host the namespace. | Must contain an NTFS volume to host the namespace. |
| Can be a member server or domain controller. | Must be a member server or domain controller in the domain in which the namespace is configured. (This requirement applies to every namespace server that hosts a given domain-based namespace.) |
| Can be hosted by a failover cluster to increase the availability of the namespace. | The namespace cannot be a clustered resource in a failover cluster. However, you can locate the namespace on a server that also functions as a node in a failover cluster if you configure the namespace to use only local resources on that server. |

## Installing DFS Namespaces

DFS Namespaces and DFS Replication are a part of the File and Storage Services role. The management tools for DFS (DFS Management, the DFS Namespaces module for Windows PowerShell, and command-line tools) are installed separately as part of the Remote Server Administration Tools.

Install DFS Namespaces by using Windows Admin Center, Server Manager, or PowerShell, as described in the next sections.

**To install DFS by using Server Manager**

1. Open Server Manager, click **Manage**, and then click **Add Roles and Features**. The Add Roles and Features Wizard appears.
2. On the **Server Selection** page, select the server or virtual hard disk (VHD) of an offline virtual machine on which you want to install DFS.
3. Select the role services and features that you want to install.
   - To install the DFS Namespaces service, on the **Server Roles** page, select **DFS Namespaces**.
   - To install only the DFS Management Tools, on the **Features** page, expand **Remote Server Administration Tools**, **Role Administration Tools**, expand **File Services Tools**, and then select **DFS Management Tools**.

**DFS Management Tools** installs the DFS Management snap-in, the DFS Namespaces module for Windows PowerShell, and command-line tools, but it does not install any DFS services on the server.

**To install DFS by using Windows PowerShell**

Open a Windows PowerShell session with elevated user rights, and then type the following command, where <name> is the role service or feature that you want to install (see the following table for a list of relevant role service or feature names):

```
Install-WindowsFeature <name>
```

| ROLE SERVICE OR FEATURE | NAME |
|---|---|
| DFS Namespaces | `FS-DFS-Namespace` |
| DFS Management Tools | `RSAT-DFS-Mgmt-Con` |

For example, to install the Distributed File System Tools portion of the Remote Server Administration Tools feature, type:

```
Install-WindowsFeature "RSAT-DFS-Mgmt-Con"
```

To install the DFS Namespaces, and the Distributed File System Tools portions of the Remote Server Administration Tools feature, type:

```
Install-WindowsFeature "FS-DFS-Namespace", "RSAT-DFS-Mgmt-Con"
```

## Interoperability with Azure virtual machines

Using DFS Namespaces on a virtual machine in Microsoft Azure has been tested; however, there are some limitations and requirements that you must follow.

- You can't cluster stand-alone namespaces in Azure virtual machines.
- You can host domain-based namespaces in Azure virtual machines, including environments with Azure Active Directory.

To learn about how to get started with Azure virtual machines, see Azure virtual machines documentation.

## Additional References

For additional related information, see the following resources.

| CONTENT TYPE | REFERENCES |
|---|---|
| **Product evaluation** | What's New in DFS Namespaces and DFS Replication in Windows Server |
| **Deployment** | DFS Namespace Scalability Considerations |
| **Operations** | DFS Namespaces: Frequently Asked Questions |
| **Community resources** | The File Services and Storage TechNet Forum |

| CONTENT TYPE | REFERENCES |
| --- | --- |
| **Protocols** | File Services Protocols in Windows Server (Deprecated) |
| **Related technologies** | Failover Clustering |
| **Support** | Windows IT Pro Support |

# Checklist: Deploy DFS Namespaces

11/2/2020 • 2 minutes to read • Edit Online

> Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Distributed File System (DFS) Namespaces and DFS Replication can be used to publish documents, software, and line-of-business data to users throughout an organization. Although DFS Replication alone is sufficient to distribute data, you can use DFS Namespaces to configure the namespace so that a folder is hosted by multiple servers, each of which holds an updated copy of the folder. This increases data availability and distributes the client load across servers.

When browsing a folder in the namespace, users are not aware that the folder is hosted by multiple servers. When a user opens the folder, the client computer is automatically referred to a server on its site. If no same-site servers are available, you can configure the namespace to refer the client to a server that has the lowest connection cost as defined in Active Directory Directory Services (AD DS).

To deploy DFS Namespaces, perform the following tasks:

- Review the concepts, and requirements of DFS Namespaces. Overview of DFS Namespaces
- Choose a namespace type
- Create a DFS namespace
- Migrate existing domain-based namespaces to Windows Server 2008 mode domain-based namespaces. Migrate a Domain-based Namespace to Windows Server 2008 mode
- Increase availability by adding namespace servers to a domain-based namespace. Add Namespace Servers to a Domain-based DFS Namespace
- Add folders to a namespace. Create a Folder in a DFS Namespace
- Add folder targets to folders in a namespace. Add Folder Targets
- Replicate content between folder targets using DFS Replication (optional). Replicate Folder Targets Using DFS Replication

## Additional References

- Namespaces
- Checklist: Tune a DFS Namespace
- Replication

# Checklist: Tune a DFS namespace

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

After creating a namespace and adding folders and targets, use the following checklist to tune or optimize the way the DFS namespace handles referrals and polls Active Directory Domain Services (AD DS) for updated namespace data.

- Prevent users from seeing folders in a namespace that they do not have permissions to access. Enable Access-Based Enumeration on a Namespace
- Enable or prevent users from being referred to a namespace or folder target when they access a folder in the namespace. Enable or Disable Referrals and Client Failback
- Adjust how long clients cache a referral before requesting a new one. Change the Amount of Time That Clients Cache Referrals
- Optimize how namespace servers poll AD DS to obtain the most current namespace data. Optimize Namespace Polling
- Use inherited permissions to control which users can view folders in a namespace for which access-based enumeration is enabled. Using Inherited Permissions with Access-Based Enumeration

In addition, by using a DFS Namespaces enhancement known as target priority, you can specify the priority of servers so that a specific server is always placed first or last in the list of servers (known as a referral) that the client receives when it accesses a folder with targets in the namespace.

- Specify in what order users should be referred to folder targets. Set the Ordering Method for Targets in Referrals
- Override referral ordering for a specific namespace server or folder target. Set Target Priority to Override Referral Ordering

## Additional References

- Namespaces
- Checklist: Deploy DFS Namespaces
- Tuning DFS Namespaces

# Deploying DFS Namespaces

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

To deploy DFS Namespaces, refer to the following topics:

- Choose a Namespaces Type
- Create a DFS Namespace
- Migrate a Domain-based Namespace to Windows Server 2008 Mode
- Add Namespace Servers to a Domain-based DFS Namespace
- Create a Folder in a DFS Namespace
- Add Folder Targets
- Replicate Folder Targets Using DFS Replication
- Delegate Management Permissions for DFS Namespaces

# Choose a namespace type

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

When creating a namespace, you must choose one of two namespace types: a stand-alone namespace or a domain-based namespace. In addition, if you choose a domain-based namespace, you must choose a namespace mode: Windows 2000 Server mode or Windows Server 2008 mode.

## Choosing a namespace type

Choose a stand-alone namespace if any of the following conditions apply to your environment:

- Your organization does not use Active Directory Domain Services (AD DS).
- You want to increase the availability of the namespace by using a failover cluster.
- You need to create a single namespace with more than 5,000 DFS folders in a domain that does not meet the requirements for a domain-based namespace (Windows Server 2008 mode) as described later in this topic.

> **NOTE**
>
> To check the size of a namespace, right-click the namespace in the DFS Management console tree, click **Properties**, and then view the namespace size in the **Namespace Properties** dialog box. For more information about DFS Namespace scalability, see the Microsoft website File Services.

Choose a domain-based namespace if any of the following conditions apply to your environment:

- You want to ensure the availability of the namespace by using multiple namespace servers.
- You want to hide the name of the namespace server from users. This makes it easier to replace the namespace server or migrate the namespace to another server.

## Choosing a domain-based namespace mode

If you choose a domain-based namespace, you must choose whether to use the Windows 2000 Server mode or the Windows Server 2008 mode. The Windows Server 2008 mode includes support for access-based enumeration and increased scalability. The domain-based namespace introduced in Windows 2000 Server is now referred to as "domain-based namespace (Windows 2000 Server mode)."

To use the Windows Server 2008 mode, the domain and namespace must meet the following minimum requirements:

- The forest uses the Windows Server 2003 or higher forest functional level.
- The domain uses the Windows Server 2008 or higher domain functional level.
- All namespace servers are running Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.

If your environment supports it, choose the Windows Server 2008 mode when you create new domain-based namespaces. This mode provides additional features and scalability, and also eliminates the possible need to migrate a namespace from the Windows 2000 Server mode.

For information about migrating a namespace to Windows Server 2008 mode, see Migrate a Domain-based Namespace to Windows Server 2008 Mode.

If your environment does not support domain-based namespaces in Windows Server 2008 mode, use the existing Windows 2000 Server mode for the namespace.

## Comparing namespace types and modes

The characteristics of each namespace type and mode are described in the following table.

| CHARACTERISTIC | STAND-ALONE NAMESPACE | DOMAIN-BASED NAMESPACE (WINDOWS 2000 SERVER MODE) | DOMAIN-BASED NAMESPACE (WINDOWS SERVER 2008 MODE) |
|---|---|---|---|
| Path to namespace | \\ *ServerName**RootName* | \\ *NetBIOSDomainName**RootName*<br>\\ *DNSDomainName**RootName* | \\ *NetBIOSDomainName**RootName*<br>\\ *DNSDomainName**RootName* |
| Namespace information storage location | In the registry and in a memory cache on the namespace server | In AD DS and in a memory cache on each namespace server | In AD DS and in a memory cache on each namespace server |
| Namespace size recommendations | The namespace can contain more than 5,000 folders with targets; the recommended limit is 50,000 folders with targets | The size of the namespace object in AD DS should be less than 5 megabytes (MB) to maintain compatibility with domain controllers that are not running Windows Server 2008. This means no more than approximately 5,000 folders with targets. | The namespace can contain more than 5,000 folders with targets; the recommended limit is 50,000 folders with targets |
| Minimum AD DS forest functional level | AD DS is not required | Windows 2000 | Windows Server 2003 |
| Minimum AD DS domain functional level | AD DS is not required | Windows 2000 mixed | Windows Server 2008 |
| Minimum supported namespace servers | Windows 2000 Server | Windows 2000 Server | Windows Server 2008 |
| Support for access-based enumeration (if enabled) | Yes, requires Windows Server 2008 namespace server | No | Yes |
| Supported methods to ensure namespace availability | Create a stand-alone namespace on a failover cluster. | Use multiple namespace servers to host the namespace. (The namespace servers must be in the same domain.) | Use multiple namespace servers to host the namespace. (The namespace servers must be in the same domain.) |
| Support for using DFS Replication to replicate folder targets | Supported when joined to an AD DS domain | Supported | Supported |

## Additional References

- Deploying DFS Namespaces
- Migrate a Domain-based Namespace to Windows Server 2008 Mode

# Create a DFS namespace

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

To create a new namespace, you can use Server Manager to create the namespace when you install the DFS Namespaces role service. You can also use the New-DfsnRoot cmdlet from a Windows PowerShell session.

The DFSN Windows PowerShell module was introduced in Windows Server 2012.

Alernatively, you can use the following procedure to create a namespace after installing the role service.

## To create a namespace

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, right-click the **Namespaces** node, and then click **New Namespace**.
3. Follow the instructions in the **New Namespace Wizard**.

   To create a stand-alone namespace on a failover cluster, specify the name of a clustered file server instance on the **Namespace Server** page of the **New Namespace Wizard** .

**IMPORTANT**

Do not attempt to create a domain-based namespace using the Windows Server 2008 mode unless the forest functional level is Windows Server 2003 or higher. Doing so can result in a namespace for which you cannot delete DFS folders, yielding the following error message: "The folder cannot be deleted. Cannot complete this function".

## Additional References

- Deploying DFS Namespaces
- Choose a Namespace Type
- Add Namespace Servers to a Domain-based DFS Namespace
- Delegate Management Permissions for DFS Namespaces.

# Migrate a domain-based namespace to Windows Server 2008 Mode

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

The Windows Server 2008 mode for domain-based namespaces includes support for access-based enumeration and increased scalability.

## To migrate a domain-based namespace to Windows Server 2008 mode

To migrate a domain-based namespace from Windows 2000 Server mode to Windows Server 2008 mode, you must export the namespace to a file, delete the namespace, re-create it in Windows Server 2008 mode, and then import the namespace settings. To do so, use the following procedure:

1. Open a Command Prompt window and type the following command to export the namespace to a file, where *domain**namespace* is the name of the appropriate domain, and namespace and *path**filename* is the path and file name of the file for export:

   ```
   Dfsutil root export \\domain\namespace path\filename.xml
   ```

2. Write down the path ( *server**share* ) for each namespace server. You must manually add namespace servers to the re-created namespace because Dfsutil cannot import namespace servers.

3. In DFS Management, right-click the namespace and then click **Delete**, or type the following command at a command prompt,
   where *domain**namespace* is the name of the appropriate domain and namespace:

   ```
   Dfsutil root remove \\domain\namespace
   ```

4. In DFS Management, re-create the namespace with the same name, but use the Windows Server 2008 mode, or type the following command at a command prompt, where
   *server**namespace* is the name of the appropriate server and share for the namespace root:

   ```
   Dfsutil root adddom \\server\namespace v2
   ```

5. To import the namespace from the export file, type the following command at a command prompt, where *domain**namespace* is the name of the appropriate domain and namespace and *path**filename* is the path and file name of the file to import:

   ```
   Dfsutil root import merge path\filename.xml \\domain\namespace
   ```

> **NOTE**
> To minimize the time required to import a large namespace, run the **Dfsutil** root import command locally on a namespace server.

6. Add any remaining namespace servers to the re-created namespace by right-clicking the namespace in DFS Management and then clicking **Add Namespace Server**, or by typing the following command at a command prompt, where *\\server\share* is the name of the appropriate server and share for the namespace root:

```
Dfsutil target add \\server\share
```

> **NOTE**
> You can add namespace servers before importing the namespace, but doing so causes the namespace servers to incrementally download the metadata for the namespace instead of immediately downloading the entire namespace after being added as a namespace server.

## Additional References

- Deploying DFS Namespaces
- Choose a Namespace Type

# Add namespace servers to a domain-based DFS namespace

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

You can increase the availability of a domain-based namespace by specifying additional namespace servers to host the namespace.

## To add a namespace server to a domain-based namespace

To add a namespace server to a domain-based namespace using DFS Management, use the following procedure:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a domain-based namespace, and then click **Add Namespace Server**.
3. Enter the path to another server, or click **Browse** to locate a server.

> **NOTE**
> This procedure is not applicable for stand-alone namespaces because they support only a single namespace server. To increase the availability of a stand-alone namespace, specify a failover cluster as the namespace server in the New Namespace Wizard.

> **TIP**
> To add a namespace server by using Windows PowerShell, use the New-DfsnRootTarget cmdlet. The DFSN Windows PowerShell module was introduced in Windows Server 2012.

## Additional References

- Deploying DFS Namespaces
- Review DFS Namespaces Server Requirements
- Create a DFS Namespace
- Delegate Management Permissions for DFS Namespaces

# Create a folder in a DFS namespace

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

You can use folders to create additional levels of hierarchy in a namespace. You can also create folders with folder targets to add shared folders to the namespace. DFS folders with folder targets cannot contain other DFS folders, so if you want to add a level of hierarchy to the namespace, do not add folder targets to the folder.

Use the following procedure to create a folder in a namespace using DFS Management:

## To create a folder in a DFS namespace

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a namespace or a folder within a namespace, and then click **New Folder**.
3. In the **Name** text box, type the name of the new folder.
4. To add one or more folder targets to the folder, click **Add** and specify the Universal Naming Convention (UNC) path of the folder target, and then click **OK** .

**TIP**

To create a folder in a namespace by using Windows PowerShell, use the New-DfsnFolder cmdlet. The DFSN Windows PowerShell module was introduced in Windows Server 2012.

## Additional References

- Deploying DFS Namespaces
- Delegate Management Permissions for DFS Namespaces

# Add folder targets

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

A folder target is the Universal Naming Convention (UNC) path of a shared folder or another namespace that is associated with a folder in a namespace. Adding multiple folder targets increases the availability of the folder in the namespace.

## To add a folder target

To add a folder target by using DFS Management, use the following procedure:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a folder, and then click **Add Folder Target**.
3. Type the path to the folder target, or click **Browse** to locate the folder target.
4. If the folder is replicated using DFS Replication, you can specify whether to add the new folder target to the replication group.

**TIP**

To add a folder target by using Windows PowerShell, use the New-DfsnFolderTarget cmdlet. The DFSN Windows PowerShell module was introduced in Windows Server 2012.

**NOTE**

Folders can contain folder targets or other DFS folders, but not both, at the same level in the folder hierarchy.

## Additional References

- Deploying DFS Namespaces
- Delegate Management Permissions for DFS Namespaces
- Replicate Folder Targets Using DFS Replication

# Replicate folder targets using DFS Replication

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008

You can use DFS Replication to keep the contents of folder targets in sync so that users see the same files regardless of which folder target the client computer is referred to.

## To replicate folder targets using DFS Replication

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a folder that has two or more folder targets, and then click **Replicate Folder**.
3. Follow the instructions in the Replicate Folder Wizard.

**NOTE**

Configuration changes are not applied immediately to all members except when using the Suspend-DfsReplicationGroup and Sync-DfsReplicationGroup cmdlets. The new configuration must be replicated to all domain controllers, and each member in the replication group must poll its closest domain controller to obtain the changes. The amount of time this takes depends on the Active Directory Directory Services (AD DS) replication latency and the long polling interval (60 minutes) on each member. To poll immediately for configuration changes, open a Command Prompt window and then type the following command once for each member of the replication group:
dfsrdiag.exe PollAD /Member:DOMAIN\Server1
To do so from a Windows PowerShell session, use the Update-DfsrConfigurationFromAD cmdlet, which was introduced in Windows Server 2012 R2.

## Additional References

- Deploying DFS Namespaces
- Delegate Management Permissions for DFS Namespaces
- DFS Replication

# Delegate management permissions for DFS Namespaces

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

The following table describes the groups that can perform basic namespace tasks by default, and the method for delegating the ability to perform these tasks:

| TASK | GROUPS THAT CAN PERFORM THIS TASK BY DEFAULT | DELEGATION METHOD |
|---|---|---|
| Create a domain-based namespace | Domain Admins group in the domain where the namespace is configured | Right-click the **Namespaces** node in the console tree, and then click **Delegate Management Permissions**. Or use the Set-DfsnRoot GrantAdminAccounts and Set-DfsnRoot RevokeAdminAccounts. Windows PowerShell cmdlets (introduced in Windows Server 2012). You must also add the user to the local Administrators group on the namespace server. |
| Add a namespace server to a domain-based namespace | Domain Admins group in the domain where the namespace is configured | Right-click the domain-based namespace in the console tree, and then click **Delegate Management Permissions**. Or use the Set-DfsnRoot GrantAdminAccounts and Set-DfsnRoot RevokeAdminAccounts. Windows PowerShell cmdlets (introduced in Windows Server 2012). You must also add the user to the local Administrators group on the namespace server to be added. |
| Manage a domain-based namespace | Local Administrators group on each namespace server | Right-click the domain-based namespace in the console tree, and then click **Delegate Management Permissions**. |
| Create a stand-alone namespace | Local Administrators group on the namespace server | Add the user to the local Administrators group on the namespace server. |
| Manage a stand-alone namespace* | Local Administrators group on the namespace server | Right-click the stand-alone namespace in the console tree, and then click **Delegate Management Permissions**. Or use the Set-DfsnRoot GrantAdminAccounts and Set-DfsnRoot RevokeAdminAccounts. Windows PowerShell cmdlets (introduced in Windows Server 2012). |

| TASK | GROUPS THAT CAN PERFORM THIS TASK BY DEFAULT | DELEGATION METHOD |
| --- | --- | --- |
| Create a replication group or enable DFS Replication on a folder | Domain Admins group in the domain where the namespace is configured | Right-click the Replication node in the console tree, and then click **Delegate Management Permissions**. |

*Delegating management permissions to manage a stand-alone namespace does not grant the user the ability to view and manage security by using the **Delegation** tab unless the user is a member of the local Administrators group on the namespace server. This issue occurs because the DFS Management snap-in cannot retrieve the discretionary access control lists (DACLs) for the stand-alone namespace from the registry. To enable the snap-in to display delegation information, you must follow the steps in the Microsoft® Knowledge Base article: KB314837: How to Manage Remote Access to the Registry

# Tuning DFS Namespaces

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

After creating a namespace and adding folders and targets, refer to the following sections to tune or optimize the way DFS Namespace handles referrals and polls Active Directory Domain Services (AD DS) for updated namespace data:

- Enable Access-Based Enumeration on a Namespace
- Enable or Disable Referrals and Client Failback
- Change the Amount of Time That Clients Cache Referrals
- Set the Ordering Method for Targets in Referrals
- Set Target Priority to Override Referral Ordering
- Optimize Namespace Polling
- Using Inherited Permissions with Access-Based Enumeration

**NOTE**

To search for folders or folder targets, select a namespace, click the **Search** tab, type your search string in the text box, and then click **Search**.

# Enable or Disable Referrals and Client Failback

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

A referral is an ordered list of servers that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or DFS folder with targets. After the computer receives the referral, the computer attempts to access the first server in the list. If the server is not available, the client computer attempts to access the next server. If a server becomes unavailable, you can configure clients to fail back to the preferred server after it becomes available.

The following sections provide information about how to enable or disable referrals or enable client failback:

## Enable or disable referrals

By disabling a namespace server's or folder target's referral, you can prevent users from being directed to that namespace server or folder target. This is useful if you need to temporarily take a server offline for maintenance.

- To enable or disable referrals to a folder target, use the following steps:
  1. In the DFS Management console tree, under the **Namespaces** node, click a folder containing targets, and then click the **Folder Targets** tab in the **Details** pane.
  2. Right-click the folder target, and then click either **Disable Folder Target** or **Enable Folder Target**.
- To enable or disable referrals to a namespace server, use the following steps:
  1. In the DFS Management console tree, select the appropriate namespace and then click the **Namespace Servers** tab.
  2. Right-click the appropriate namespace server and then click either **Disable Namespace Server** or **Enable Namespace Server**.

> **TIP**
> To enable or disable referrals by using Windows PowerShell, use the Set-DfsnRootTarget –State or Set-DfsnServerConfiguration cmdlets, which were introduced in Windows Server 2012.

## Enable client failback

If a target becomes unavailable, you can configure clients to fail back to the target after it is restored. For failback to work, client computers must meet the requirements listed in the following topic: Review DFS Namespaces Client Requirements.

> **NOTE**
> To enable client failback on a namespace root by using Windows PowerShell, use the Set-DfsnRoot cmdlet. To enable client failback on a DFS folder, use the Set-DfsnFolder cmdlet.

## To enable client failback for a namespace root

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a namespace, and then click **Properties**.
3. On the **Referrals** tab, select the **Clients fail back to preferred targets** check box.

Folders with targets inherit client failback settings from the namespace root. If client failback is disabled on the namespace root, you can use the following procedure to enable the client to fail back on a folder with targets.

## To enable client failback for a folder with targets

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a folder with targets, and then click **Properties**.
3. On the **Referrals** tab, click the **Clients fail back to preferred targets** check box.

## Additional References

- Tuning DFS Namespaces
- Review DFS Namespaces Client Requirements
- Delegate Management Permissions for DFS Namespaces

# Change the amount of time that clients cache referrals

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

A referral is an ordered list of targets that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or folder with targets in the namespace. You can adjust how long clients cache a referral before requesting a new one.

## To change the amount of time that clients cache namespace root referrals

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a namespace, and then click **Properties**.
3. On the **Referrals** tab, in the **Cache duration (in seconds)** text box, type the amount of time (in seconds) that clients cache namespace root referrals. The default setting is 300 seconds (five minutes).

> **TIP**
> To change the amount of time that clients cache namespace root referrals by using Windows PowerShell, use the Set-DfsnRoot TimeToLiveSec cmdlet. These cmdlets were introduced in Windows Server 2012.

## To change the amount of time that clients cache folder referrals

1. Click **Start** , point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a folder that has targets, and then click **Properties**.
3. On the **Referrals** tab, in the **Cache duration (in seconds)** text box, type the amount of time (in seconds) that clients cache folder referrals. The default setting is 1800 seconds (30 minutes).

## Additional References

- Tuning DFS Namespaces
- Delegate Management Permissions for DFS Namespaces

# Set the Ordering Method for Targets in Referrals

12/16/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

A referral is an ordered list of targets that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or folder with targets. After the client receives the referral, the client attempts to access the first target in the list. If the target is not available, the client attempts to access the next target. Targets on the client's site are always listed first in a referral. Targets outside of the client's site are listed according to the ordering method.

Use the following sections to specify in what order targets should be referred to clients and to understand the different methods of ordering target referrals:

## To set the ordering method for targets in namespace root referrals

Use the following procedure to set the ordering method on the namespace root:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a namespace, and then click **Properties**.
3. On the **Referrals** tab, select an ordering method.

> **NOTE**
>
> To use Windows PowerShell to set the ordering method for targets in namespace root referrals, use the Set-DfsnRoot cmdlet with one of the following parameters:
>
> - **EnableSiteCosting** specifies the **Lowest cost ordering** method
> - **EnableInsiteReferrals** specifies the **Exclude targets outside of the client's site** ordering method
> - Omitting either parameter specifies the **Random order** referral ordering method.

The DFSN Windows PowerShell module was introduced in Windows Server 2012.

## To set the ordering method for targets in folder referrals

Folders with targets inherit the ordering method from the namespace root. You can override the ordering method by using the following procedure:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a folder with targets, and then click **Properties**.
3. On the **Referrals** tab, select the **Exclude targets outside of the client's site** check box.

> **NOTE**
> To use Windows PowerShell to exclude folder targets outside of the client's site, use the Set-DfsnFolder –EnableInsiteReferrals cmdlet.

## Target referral ordering methods

The three ordering methods are:

- Random order
- Lowest cost
- Exclude targets outside of the client's site

## Random order

In this method, targets are ordered as follows:

1. Targets in the same Active Directory Directory Services (AD DS) site as the client are listed in random order at the top of the referral.
2. Targets outside of the client's site are listed in random order.

If no same-site target servers are available, the client computer is referred to a random target server regardless of how expensive the connection is or how distant the target.

## Lowest cost

In this method, targets are ordered as follows:

1. Targets in the same site as the client are listed in random order at the top of the referral.
2. Targets outside of the client's site are listed in order of lowest cost to highest cost. Referrals with the same cost are grouped together, and the targets are listed in random order within each group.

> **NOTE**
> Site link costs are not shown in the DFS Management snap-in. To view site link costs, use the Active Directory Sites and Services snap-in.

## Exclude targets outside of the client's site

In this method, the referral contains only the targets that are in the same site as the client. These same-site targets are listed in random order. If no same-site targets exist, the client does not receive a referral and cannot access that portion of the namespace.

> **NOTE**
> Targets that have target priority set to "First among all targets" or "Last among all targets" are still listed in the referral, even if the ordering method is set to **Exclude targets outside of the client's site**.

## Additional References

- Tuning DFS Namespaces
- Delegate Management Permissions for DFS Namespaces

# Set target priority to override referral ordering

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

A referral is an ordered list of targets that a client computer receives from a domain controller or namespace server when the user accesses a namespace root or folder with targets in the namespace. Each target in a referral is ordered according to the ordering method for the namespace root or folder.

To refine how targets are ordered, you can set priority on individual targets. For example, you can specify that the target is first among all targets, last among all targets, or first or last among all targets of equal cost.

## To set target priority on a root target for a domain-based namespace

To set target priority on a root target for a domain-based namespace, use the following procedure:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, click the domain-based namespace for the root targets for which you want to set priority.
3. In the **Details** pane, on the **Namespace Servers** tab, right-click the root target with the priority that you want to change, and then click **Properties**.
4. On the **Advanced** tab, click **Override referral ordering**, and then click the priority you want.
   - **First among all targets** Specifies that users should always be referred to this target if the target is available.
   - **Last among all targets** Specifies that users should never be referred to this target unless all other targets are unavailable.
   - **First among targets of equal cost** Specifies that users should be referred to this target before other targets of equal cost (which usually means other targets in the same site).
   - **Last among targets of equal cost** Specifies that users should never be referred to this target if there are other targets of equal cost available (which usually means other targets in the same site).

## To set target priority on a folder target

To set target priority on a folder target, use the following procedure:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, click the folder of the targets for which you want to set priority.
3. In the **Details** pane, on the **Folder Targets** tab, right-click the folder target with the priority that you want to change, and then click **Properties** .
4. On the **Advanced** tab, click **Override referral ordering** and then click the priority that you want.

**NOTE**

To set target priorities by using Windows PowerShell, use the Set-DfsnRootTarget and Set-DfsnFolderTarget cmdlets with the **ReferralPriorityClass** and **ReferralPriorityRank** parameters. These cmdlets were introduced in Windows Server 2012.

## Additional References

- Tuning DFS Namespaces
- Delegate Management Permissions for DFS Namespaces

# Optimize Namespace Polling

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

To maintain a consistent domain-based namespace across namespace servers, it is necessary for namespace servers to periodically poll Active Directory Domain Services (AD DS) to obtain the most current namespace data.

## To optimize namespace polling

Use the following procedure to optimize how namespace polling occurs:

1. Click **Start**, point to **Administrative Tools**, and then click **DFS Management**.
2. In the console tree, under the **Namespaces** node, right-click a domain-based namespace, and then click **Properties** .
3. On the **Advanced** tab, select whether you want the namespace optimized for consistency or scalability.
   - Choose **Optimize for consistency** if there are 16 or fewer namespace servers hosting the namespace.
   - Choose **Optimize for scalability** if there are more than 16 namespace servers. This reduces the load on the Primary Domain Controller (PDC) Emulator, but increases the time required for changes to the namespace to replicate to all namespace servers. Until changes replicate to all servers, users might have an inconsistent view of the namespace.

**NOTE**

To set the namespace polling mode by using Windows PowerShell, use the Set-DfsnRoot EnableRootScalability cmdlet, which was introduced in Windows Server 2012.

## Additional References

- Tuning DFS Namespaces
- Delegate Management Permissions for DFS Namespaces

# Enable access-based enumeration on a namespace

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Access-based enumeration hides files and folders that users do not have permissions to access. By default, this feature is not enabled for DFS namespaces. You can enable access-based enumeration of DFS folders by using DFS Management. To control access-based enumeration of files and folders in folder targets, you must enable access-based enumeration on each shared folder by using Share and Storage Management.

To enable access-based enumeration on a namespace, all namespace servers must be running Windows Server 2008 or newer. Additionally, domain-based namespaces must use the Windows Server 2008 mode. For information about the requirements of the Windows Server 2008 mode, see Choose a Namespace Type.

In some environments, enabling access-based enumeration can cause high CPU utilization on the server and slow response times for users.

**NOTE**

If you upgrade the domain functional level to Windows Server 2008 while there are existing domain-based namespaces, DFS Management will allow you to enable access-based enumeration on these namespaces. However, you will not be able to edit permissions to hide folders from any groups or users unless you migrate the namespaces to the Windows Server 2008 mode. For more information, see Migrate a Domain-based Namespace to Windows Server 2008 Mode.

To use access-based enumeration with DFS Namespaces, you must follow these steps:

- Enable access-based enumeration on a namespace
- Control which users and groups can view individual DFS folders

**WARNING**

Access-based enumeration does not prevent users from getting a referral to a folder target if they already know the DFS path. Only the share permissions or the NTFS file system permissions of the folder target (shared folder) itself can prevent users from accessing a folder target. DFS folder permissions are used only for displaying or hiding DFS folders, not for controlling access, making Read access the only relevant permission at the DFS folder level. For more information, see Using Inherited Permissions with Access-Based Enumeration

You can enable access-based enumeration on a namespace either by using the Windows interface or by using a command line.

## To enable access-based enumeration by using the Windows interface

1. In the console tree, under the **Namespaces** node, right-click the appropriate namespace and then click **Properties** .
2. Click the **Advanced** tab and then select the **Enable access-based enumeration for this namespace** check box.

## To enable access-based enumeration by using a command line

1. Open a command prompt window on a server that has the **Distributed File System** role service or **Distributed File System Tools** feature installed.
2. Type the following command, where *<namespace_root>* is the root of the namespace:

```
dfsutil property abe enable \\ <namespace_root>
```

> **TIP**
> To manage access-based enumeration on a namespace by using Windows PowerShell, use the Set-DfsnRoot, Grant-DfsnAccess, and Revoke-DfsnAccess cmdlets. The DFSN Windows PowerShell module was introduced in Windows Server 2012.

You can control which users and groups can view individual DFS folders either by using the Windows interface or by using a command line.

## To control folder visibility by using the Windows interface

1. In the console tree, under the **Namespaces** node, locate the folder with targets for which you want to control visibility, right-click it and then click **Properties**.
2. Click the **Advanced** tab.
3. Click **Set explicit view permissions on the DFS folder** and then **Configure view permissions**.
4. Add or remove groups or users by clicking **Add** or **Remove**.
5. To allow users to see the DFS folder, select the group or user, and then select the **Allow** check box.

   To hide the folder from a group or user, select the group or user, and then select the **Deny** check box.

## To control folder visibility by using a command line

1. Open a Command Prompt window on a server that has the **Distributed File System** role service or **Distributed File System Tools** feature installed.
2. Type the following command, where *<DFSPath>* is the path of the DFS folder (link), *<DOMAIN\Account>* is the name of the group or user account, and *(...)* is replaced with additional Access Control Entries (ACEs):

```
dfsutil property sd grant <DFSPath> DOMAIN\Account:R (...) Protect Replace
```

   For example, to replace existing permissions with permissions that allows the Domain Admins and CONTOSO\Trainers groups Read (R) access to the \contoso.office\public\training folder, type the following command:

```
dfsutil property sd grant \\contoso.office\public\training "CONTOSO\Domain Admins":R CONTOSO\Trainers:R
Protect Replace
```

3. To perform additional tasks from the command prompt, use the following commands:

| COMMAND | DESCRIPTION |
| --- | --- |
| Dfsutil property sd deny | Denies a group or user the ability to view the folder. |
| Dfsutil property sd reset | Removes all permissions from the folder. |
| Dfsutil property sd revoke | Removes a group or user ACE from the folder. |

## Additional References

- Create a DFS Namespace
- Delegate Management Permissions for DFS Namespaces
- Installing DFS
- Using Inherited Permissions with Access-Based Enumeration

# Using inherited permissions with Access-based Enumeration

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

By default, the permissions used for a DFS folder are inherited from the local file system of the namespace server. The permissions are inherited from the root directory of the system drive and grant the DOMAIN\Users group Read permissions. As a result, even after enabling access-based enumeration, all folders in the namespace remain visible to all domain users.

## Advantages and limitations of inherited permissions

There are two primary benefits to using inherited permissions to control which users can view folders in a DFS namespace:

- You can quickly apply inherited permissions to many folders without having to use scripts.
- You can apply inherited permissions to namespace roots and folders without targets.

Despite the benefits, inherited permissions in DFS Namespaces have many limitations that make them inappropriate for most environments:

- Modifications to inherited permissions are not replicated to other namespace servers. Therefore, use inherited permissions only on stand-alone namespaces or in environments where you can implement a third-party replication system to keep the Access Control Lists (ACLs) on all namespace servers synchronized.
- DFS Management and **Dfsutil** cannot view or modify inherited permissions. Therefore, you must use Windows Explorer or the **Icacls** command in addition to DFS Management or **Dfsutil** to manage the namespace.
- When using inherited permissions, you cannot modify the permissions of a folder with targets except by using the **Dfsutil** command. DFS Namespaces automatically removes permissions from folders with targets set using other tools or methods.
- If you set permissions on a folder with targets while you are using inherited permissions, the ACL that you set on the folder with targets combines with inherited permissions from the folder's parent in the file system. You must examine both sets of permissions to determine what the net permissions are.

> **NOTE**
> When using inherited permissions, it is simplest to set permissions on namespace roots and folders without targets. Then use inherited permissions on folders with targets so that they inherit all permissions from their parents.

## Using inherited permissions

To limit which users can view a DFS folder, you must perform one of the following tasks:

- **Set explicit permissions for the folder, disabling inheritance.** To set explicit permissions on a folder with targets (a link) using DFS Management or the **Dfsutil** command, see Enable Access-Based Enumeration on a Namespace.
- **Modify inherited permissions on the parent in the local file system.** To modify the permissions

inherited by a folder with targets, if you have already set explicit permissions on the folder, switch to inherited permissions from explicit permissions, as discussed in the following procedure. Then use Windows Explorer or the **Icacls** command to modify the permissions of the folder from which the folder with targets inherits its permissions.

> **NOTE**
>
> Access-based enumeration does not prevent users from obtaining a referral to a folder target if they already know the DFS path of the folder with targets. Permissions set using Windows Explorer or the **Icacls** command on namespace roots or folders without targets control whether users can access the DFS folder or namespace root. However, they do not prevent users from directly accessing a folder with targets. Only the share permissions or the NTFS file system permissions of the shared folder itself can prevent users from accessing folder targets.

## To switch from explicit permissions to inherited permissions

1. In the console tree, under the **Namespaces** node, locate the folder with targets whose visibility you want to control, right-click the folder and then click **Properties**.
2. Click the **Advanced** tab.
3. Click **Use inherited permissions from the local file system** and then click **OK** in the **Confirm Use of Inherited Permissions** dialog box. Doing this removes all explicitly set permissions on this folder, restoring inherited NTFS permissions from the local file system of the namespace server.
4. To change the inherited permissions for folders or namespace roots in a DFS namespace, use Windows Explorer or the **ICacls** command.

## Additional References

- Create a DFS Namespace

# DFS Replication overview

12/16/2020 • 5 minutes to read • Edit Online

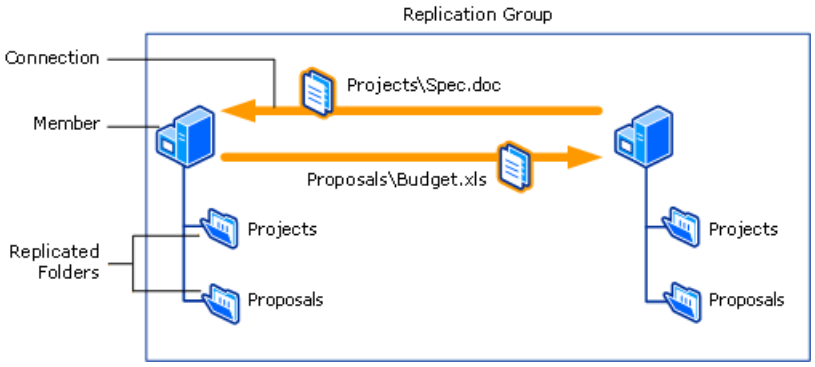
Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server (Semi-Annual Channel)

DFS Replication is a role service in Windows Server that enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites. DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. It replaces the File Replication Service (FRS) as the replication engine for DFS Namespaces, as well as for replicating the Active Directory Domain Services (AD DS) SYSVOL folder in domains that use the Windows Server 2008 or later domain functional level.

DFS Replication uses a compression algorithm known as remote differential compression (RDC). RDC detects changes to the data in a file and enables DFS Replication to replicate only the changed file blocks instead of the entire file.

For more information about replicating SYSVOL using DFS Replication, see Migrate the SYSVOL replication to DFS Replication.

To use DFS Replication, you must create replication groups and add replicated folders to the groups. Replication groups, replicated folders, and members are illustrated in the following figure.




This figure shows that a replication group is a set of servers, known as members, which participates in the replication of one or more replicated folders. A replicated folder is a folder that stays synchronized on each member. In the figure, there are two replicated folders: Projects and Proposals. As the data changes in each replicated folder, the changes are replicated across connections between the members of the replication group. The connections between all members form the replication topology. Creating multiple replicated folders in a single replication group simplifies the process of deploying replicated folders because the topology, schedule, and bandwidth throttling for the replication group are applied to each replicated folder. To deploy additional replicated folders, you can use Dfsradmin.exe or a follow the instructions in a wizard to define the local path and permissions for the new replicated folder.

Each replicated folder has unique settings, such as file and subfolder filters, so that you can filter out different files and subfolders for each replicated folder.

The replicated folders stored on each member can be located on different volumes in the member, and the replicated folders do not need to be shared folders or part of a namespace. However, the DFS Management snap-in makes it easy to share replicated folders and optionally publish them in an existing namespace.

You can administer DFS Replication by using DFS Management, the DfsrAdmin and Dfsrdiag commands, or scripts

that call WMI.

## Requirements

Before you can deploy DFS Replication, you must configure your servers as follows:

- Update the Active Directory Domain Services (AD DS) schema to include Windows Server 2003 R2 or later schema additions. You cannot use read-only replicated folders with the Windows Server 2003 R2 or older schema additions.
- Ensure that all servers in a replication group are located in the same forest. You cannot enable replication across servers in different forests.
- Install DFS Replication on all servers that will act as members of a replication group.
- Contact your antivirus software vendor to check that your antivirus software is compatible with DFS Replication.
- Locate any folders that you want to replicate on volumes formatted with the NTFS file system. DFS Replication does not support the Resilient File System (ReFS) or the FAT file system. DFS Replication also does not support replicating content stored on Cluster Shared Volumes.

## Interoperability with Azure virtual machines

Using DFS Replication on a virtual machine in Azure has been tested with Windows Server; however, there are some limitations and requirements that you must follow.

- Using snapshots or saved states to restore a server running DFS Replication for replication of anything other than the SYSVOL folder causes DFS Replication to fail, which requires special database recovery steps. Similarly, don't export, clone, or copy the virtual machines. For more information, see article 2517913 in the Microsoft Knowledge Base, as well as Safely Virtualizing DFSR.
- When backing up data in a replicated folder housed in a virtual machine, you must use backup software from within the guest virtual machine.
- DFS Replication requires access to physical or virtualized domain controllers – it can't communicate directly with Azure AD.
- DFS Replication requires a VPN connection between your on premises replication group members and any members hosted in Azure VMs. You also need to configure the on premises router (such as Forefront Threat Management Gateway) to allow the RPC Endpoint Mapper (port 135) and a randomly assigned port between 49152 and 65535 to pass over the VPN connection. You can use the Set-DfsrMachineConfiguration cmdlet or the Dfsrdiag command line tool to specify a static port instead of the random port. For more information about how to specify a static port for DFS Replication, see Set-DfsrServiceConfiguration. For information about related ports to open for managing Windows Server, see article 832017 in the Microsoft Knowledge Base.

To learn about how to get started with Azure virtual machines, visit the Microsoft Azure web site.

## Installing DFS Replication

DFS Replication is a part of the File and Storage Services role. The management tools for DFS (DFS Management, the DFS Replication module for Windows PowerShell, and command-line tools) are installed separately as part of the Remote Server Administration Tools.

Install DFS Replication by using Windows Admin Center, Server Manager, or PowerShell, as described in the next sections.

**To install DFS by using Server Manager**

1. Open Server Manager, click **Manage**, and then click **Add Roles and Features**. The Add Roles and Features Wizard appears.
2. On the **Server Selection** page, select the server or virtual hard disk (VHD) of an offline virtual machine on

which you want to install DFS.

3. Select the role services and features that you want to install.

   - To install the DFS Replication service, on the **Server Roles** page, select **DFS Replication**.
   - To install only the DFS Management Tools, on the **Features** page, expand **Remote Server Administration Tools**, **Role Administration Tools**, expand **File Services Tools**, and then select **DFS Management Tools**.

     **DFS Management Tools** installs the DFS Management snap-in, the DFS Replication and DFS Namespaces modules for Windows PowerShell, and command-line tools, but it does not install any DFS services on the server.

**To install DFS Replication by using Windows PowerShell**

Open a Windows PowerShell session with elevated user rights, and then type the following command, where <name> is the role service or feature that you want to install (see the following table for a list of relevant role service or feature names):

```
Install-WindowsFeature <name>
```

| ROLE SERVICE OR FEATURE | NAME |
|---|---|
| DFS Replication | `FS-DFS-Replication` |
| DFS Management Tools | `RSAT-DFS-Mgmt-Con` |

For example, to install the Distributed File System Tools portion of the Remote Server Administration Tools feature, type:

```
Install-WindowsFeature "RSAT-DFS-Mgmt-Con"
```

To install the DFS Replication, and the Distributed File System Tools portions of the Remote Server Administration Tools feature, type:

```
Install-WindowsFeature "FS-DFS-Replication", "RSAT-DFS-Mgmt-Con"
```

## Additional References

- DFS Namespaces and DFS Replication overview
- Checklist: Deploy DFS Replication
- Checklist: Manage DFS Replication
- Deploying DFS Replication
- Managing DFS Replication
- Troubleshooting DFS Replication

# Migrate SYSVOL replication to DFS Replication

12/16/2020 • 2 minutes to read • Edit Online

Updated: August 25, 2010

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008

Domain controllers use a special shared folder named SYSVOL to replicate logon scripts and Group Policy object files to other domain controllers. Windows 2000 Server and Windows Server 2003 use File Replication Service (FRS) to replicate SYSVOL, whereas Windows Server 2008 uses the newer DFS Replication service when in domains that use the Windows Server 2008 domain functional level, and FRS for domains that run older domain functional levels.

To use DFS Replication to replicate the SYSVOL folder, you can either create a new domain that uses the Windows Server 2008 domain functional level, or you can use the procedure that is discussed in this document to upgrade an existing domain and migrate replication to DFS Replication.

This document assumes that you have a basic knowledge of Active Directory Domain Services (AD DS), FRS, and Distributed File System Replication (DFS Replication). For more information, see Active Directory Domain Services Overview, FRS Overview, or Overview of DFS Replication

> **NOTE**
> To download a printable version of this guide, go to SYSVOL Replication Migration Guide: FRS to DFS Replication (https://go.microsoft.com/fwlink/?LinkId=150375)

## In this guide

- Dfsrmig
- SYSVOL Migration Tool Actions

## Additional references

SYSVOL Migration Series: Part 1 – Introduction to the SYSVOL migration process

SYSVOL Migration Series: Part 2 – Dfsrmig.exe: The SYSVOL migration tool

SYSVOL Migration Series: Part 3 - Migrating to the 'PREPARED' state

SYSVOL Migration Series: Part 4 – Migrating to the 'REDIRECTED' state

SYSVOL Migration Series: Part 5 – Migrating to the 'ELIMINATED' state

Distributed File Systems Step-by-Step Guide for Windows Server 2008

FRS Technical Reference

# Use Robocopy to pre-seed files for DFS Replication

11/2/2020 • 8 minutes to read • Edit Online

Applies to: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

This topic explains how to use the command-line tool, **Robocopy.exe**, to pre-seed files when setting up replication for Distributed File System (DFS) Replication (also known as DFSR or DFS-R) in Windows Server. By pre-seeding files before you set up DFS Replication, add a new replication partner, or replace a server, you can speed up initial synchronization and enable cloning of the DFS Replication database in Windows Server 2012 R2. The Robocopy method is one of several pre-seeding methods; for an overview, see Step 1: pre-seed files for DFS Replication.

The Robocopy (Robust File Copy) command-line utility is included with Windows Server. The utility provides extensive options that include copying security, backup API support, retry capabilities, and logging. Later versions include multi-threading and un-buffered I/O support.

**IMPORTANT**

Robocopy does not copy exclusively locked files. If users tend to lock many files for long periods on your file servers, consider using a different pre-seeding method. pre-seeding does not require a perfect match between file lists on the source and destination servers, but the more files that do not exist when initial synchronization is performed for DFS Replication, the less effective pre-seeding is. To minimize lock conflicts, use Robocopy during non-peak hours for your organization. Always examine the Robocopy logs after pre-seeding to ensure that you understand which files were skipped because of exclusive locks.

To use Robocopy to pre-seed files for DFS Replication, follow these steps:

1. Download and install the latest version of Robocopy.
2. Stabilize files that will be replicated.
3. Copy the replicated files to the destination server.

## Prerequisites

Because pre-seeding does not directly involve DFS Replication, you only need to meet the requirements for performing a file copy with Robocopy.

- You need an account that's a member of the local Administrators group on both the source and destination servers.
- Install the most recent version of Robocopy on the server that you will use to copy the files—either the source server or the destination server; you will need to install the most recent version for the operating system version. For instructions, see Step 2: Stabilize files that will be replicated. Unless you are pre-seeding files from a server running Windows Server 2003 R2, you can run Robocopy on either the source or destination server. The destination server, which typically has the more recent operating system version, gives you access to the most recent version of Robocopy.
- Ensure that sufficient storage space is available on the destination drive. Do not create a folder on the path that you plan to copy to: Robocopy must create the root folder.

> **NOTE**
> When you decide how much space to allocate for the pre-seeded files, consider expected data growth over time and storage requirements for DFS Replication. For planning help, see Edit the Quota Size of the Staging Folder and Conflict and Deleted Folder in Managing DFS Replication.

- On the source server, optionally install Process Monitor or Process Explorer, which you can use to check for applications that are locking files. For download information, see Process Monitor and Process Explorer.

## Step 1: Download and install the latest version of Robocopy

Before you use Robocopy to pre-seed files, you should download and install the latest version of **Robocopy.exe**. This ensures that DFS Replication doesn't skip files because of issues within Robocopy's shipping versions.

The source for the latest compatible Robocopy version depends on the version of Windows Server that is running on the server. For information about downloading the hotfix with the most recent version of Robocopy for Windows Server 2008 R2 or Windows Server 2008, see List of currently available hotfixes for Distributed File System (DFS) technologies in Windows Server 2008 and in Windows Server 2008 R2.

Alternatively, you can locate and install the latest hotfix for an operating system by taking the following steps.

**Locate and install the latest version of Robocopy for a specific version of Windows Server**

1. In a web browser, open https://support.microsoft.com.
2. In **Search Support**, enter the following string, replacing `<operating system version>` with the appropriate operating system, then press the Enter key:

   ```
   robocopy.exe kbqfe "<operating system version>"
   ```

   For example, enter **robocopy.exe kbqfe "Windows Server 2008 R2"**.
3. Locate and download the hotfix with the highest ID number (that is, the latest version).
4. Install the hotfix on the server.

## Step 2: Stabilize files that will be replicated

After you install the latest version of Robocopy on the server, you should prevent locked files from blocking copying by using the methods described in the following table. Most applications do not exclusively lock files. However, during normal operations, a small percentage of files might be locked on file servers.

| SOURCE OF THE LOCK | EXPLANATION | MITIGATION |
| --- | --- | --- |

| SOURCE OF THE LOCK | EXPLANATION | MITIGATION |
| --- | --- | --- |
| Users remotely open files on shares. | Employees connect to a standard file server and edit documents, multimedia content, or other files. Sometimes referred to as the traditional home folder or shared data workloads. | Only perform Robocopy operations during off-peak, non-business hours. This minimizes the number of files that Robocopy must skip during pre-seeding.<br><br>Consider temporarily setting Read-only access on the file shares that will be replicated by using the Windows PowerShell **Grant-SmbShareAccess** and **Close-SmbSession** cmdlets. If you set permissions for a common group such as Everyone or Authenticated Users to READ, standard users might be less likely to open files with exclusive locks (if their applications detect the Read-only access when files are opened).<br><br>You might also consider setting a temporary firewall rule for SMB port 445 inbound to that server to block access to files or use the **Block-SmbShareAccess** cmdlet. However, both of these methods are very disruptive to user operations. |
| Applications open files local. | Application workloads running on a file server sometimes lock files. | Temporarily disable or uninstall the applications that are locking files. You can use Process Monitor or Process Explorer to determine which applications are locking files. To download Process Monitor or Process Explorer, visit the Process Monitor and Process Explorer pages. |

## Step 3: Copy the replicated files to the destination server

After you minimize locks on the files that will be replicated, you can pre-seed the files from the source server to the destination server.

> **NOTE**
>
> You can run Robocopy on either the source computer or the destination computer. The following procedure describes running Robocopy on the destination server, which typically is running a more recent operating system, to take advantage of any additional Robocopy capabilities that the more recent operating system might provide.

**pre-seed the replicated files onto the destination server with Robocopy**

1. Sign in to the destination server with an account that's a member of the local Administrators group on both the source and destination servers.
2. Open an elevated command prompt.
3. To pre-seed the files from the source to destination server, run the following command, substituting your own source, destination, and log file paths for the bracketed values:

```
robocopy "<source replicated folder path>" "<destination replicated folder path>" /e /b /copyall /r:6
/w:5 /MT:64 /xd DfsrPrivate /tee /log:<log file path> /v
```

This command copies all contents of the source folder to the destination folder, with the following parameters:

| PARAMETER | DESCRIPTION |
|---|---|
| "<source replicated folder path>" | Specifies the source folder to pre-seed on the destination server. |
| "<destination replicated folder path>" | Specifies the path to the folder that will store the pre-seeded files.<br><br>The destination folder must not already exist on the destination server. To get matching file hashes, Robocopy must create the root folder when it pre-seeds the files. |
| /e | Copies subdirectories and their files, as well as empty subdirectories. |
| /b | Copies files in Backup mode. |
| /copyall | Copies all file information, including data, attributes, time stamps, the NTFS access control list (ACL), owner information, and auditing information. |
| /r:6 | Retries the operation six times when an error occurs. |
| /w:5 | Waits 5 seconds between retries. |
| MT:64 | Copies 64 files simultaneously. |
| /xd DfsrPrivate | Excludes the DfsrPrivate folder. |
| /tee | Writes status output to the console window, as well as to the log file. |
| /log <log file path> | Specifies the log file to write. Overwrites the file's existing contents. (To append the entries to the existing log file, use `/log+ <log file path>`.) |
| /v | Produces verbose output that includes skipped files. |

For example, the following command replicates files from the source replicated folder, E:\RF01, to data drive D on the destination server:

```
robocopy.exe "\\srv01\e$\rf01" "d:\rf01" /e /b /copyall /r:6 /w:5 /MT:64 /xd DfsrPrivate /tee
/log:c:\temp\pre-seedsrv02.log
```

> **NOTE**
>
> We recommend that you use the parameters described above when you use Robocopy to pre-seed files for DFS Replication. However, you can change some of their values or add additional parameters. For example, you might find out through testing that you have the capacity to set a higher value (thread count) for the */MT* parameter. Also, if you'll primarily replicate larger files, you might be able to increase copy performance by adding the **/j** option for unbuffered I/O. For more information about Robocopy parameters, see the Robocopy command-line reference.

> **WARNING**
>
> To avoid potential data loss when you use Robocopy to pre-seed files for DFS Replication, do not make the following changes to the recommended parameters:
>
> - Do not use the */mir* parameter (that mirrors a directory tree) or the */mov* parameter (that moves the files, then deletes them from the source).
> - Do not remove the **/e**, **/b**, and **/copyall** options.

4. After copying completes, examine the log for any errors or skipped files. Use Robocopy to copy any skipped files individually instead of recopying the entire set of files. If files were skipped because of exclusive locks, either try copying individual files with Robocopy later, or accept that those files will require over-the-wire replication by DFS Replication during initial synchronization.

## Next step

After you complete the initial copy, and use Robocopy to resolve issues with as many skipped files as possible, you will use the **Get-DfsrFileHash** cmdlet in Windows PowerShell or the **Dfsrdiag** command to validate the pre-seeded files by comparing file hashes on the source and destination servers. For detailed instructions, see Step 2: Validate pre-seeded Files for DFS Replication.

# DFS Replication: Frequently Asked Questions (FAQ)

12/16/2020 • 39 minutes to read • Edit Online

Updated: April 30, 2019

Applies To: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

This FAQ answers questions about Distributed File System (DFS) Replication (also known as DFS-R or DFSR) for Windows Server.

For information about DFS Namespaces, see DFS Namespaces: Frequently Asked Questions.

For information about what's new in DFS Replication, see the following topics:

- DFS Namespaces and DFS Replication Overview (in Windows Server 2012)
- What's New in Distributed File System topic in Changes in Functionality from Windows Server 2008 to Windows Server 2008 R2
- Distributed File System topic in Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008

For a list of recent changes to this topic, see the Change History section of this topic.

## Interoperability

**Can DFS Replication communicate with FRS?**

No. DFS Replication does not communicate with File Replication Service (FRS). DFS Replication and FRS can run on the same server at the same time, but they must never be configured to replicate the same folders or subfolders because doing so can cause data loss.

**Can DFS Replication replace FRS for SYSVOL replication**

Yes, DFS Replication can replace FRS for SYSVOL replication on servers running Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008. Servers running Windows Server 2003 R2 do not support using DFS Replication to replicate the SYSVOL folder.

For more information about replicating SYSVOL by using DFS Replication, see the SYSVOL Replication Migration Guide: FRS to DFS Replication.

**Can I upgrade from FRS to DFS Replication without losing configuration settings?**

Yes. To migrate replication from FRS to DFS Replication, see the following documents:

- To migrate replication of folders other than the SYSVOL folder, see DFS Operations Guide: Migrating from FRS to DFS Replication and FRS2DFSR – An FRS to DFSR Migration Utility (https://go.microsoft.com/fwlink/?LinkID=195437).
- To migrate replication of the SYSVOL folder to DFS Replication, see SYSVOL Replication Migration Guide: FRS to DFS Replication.

**Can I use DFS Replication in a mixed Windows/UNIX environment?**

Yes. Although DFS Replication only supports replicating content between servers running Windows Server, UNIX clients can access file shares on the Windows servers. To do so, install Services for Network File Systems (NFS) on the DFS Replication server.

You can also use the SMB/CIFS client functionality included in many UNIX clients to directly access the Windows file shares, although this functionality is often limited or requires modifications to the Windows environment (such as disabling SMB Signing by using Group Policy).

DFS Replication interoperates with NFS on a server running a Windows Server operating system, but you cannot replicate an NFS mount point.

**Can I use the Volume Shadow Copy Service with DFS Replication?**

Yes. DFS Replication is supported on Volume Shadow Copy Service (VSS) volumes and previous snapshots can be restored successfully with the Previous Versions Client.

**Can I use Windows Backup (Ntbackup.exe) to remotely back up a replicated folder?**

No, using Windows Backup (Ntbackup.exe) on a computer running Windows Server 2003 or earlier to back up the contents of a replicated folder on a computer running Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008 is not supported.

To back up files that are stored in a replicated folder, use Windows Server Backup or Microsoft® System Center Data Protection Manager. For information about Backup and Recovery functionality in Windows Server 2008 R2 and Windows Server 2008, see Backup and Recovery. For more information, see System Center Data Protection Manager (https://go.microsoft.com/fwlink/?LinkId=182261).

**Do file system policies impact DFS Replication?**

Yes. Do not configure file system policies on replicated folders. The file system policy reapplies NTFS permissions at every Group Policy refresh interval. This can result in sharing violations because an open file is not replicated until the file is closed.

**Does DFS Replication replicate mailboxes hosted on Microsoft Exchange Server?**

No. DFS Replication cannot be used to replicate mailboxes hosted on Microsoft Exchange Server.

**Does DFS Replication support file screens created by File Server Resource Manager?**

Yes. However, the File Server Resource Manager (FSRM) file screening settings must match on both ends of the replication. In addition, DFS Replication has its own filter mechanism for files and folders that you can use to exclude certain files and file types from replication.

The following are best practices for implementing file screens or quotas:

- The hidden DfsrPrivate folder must not be subject to quotas or file screens.
- Screened files must not exist in any replicated folder before screening is enabled.
- No folders may exceed the quota before the quota is enabled.
- You must use hard quotas with caution. It is possible for individual members of a replication group to stay within a quota before replication, but exceed it when files are replicated. For example, if a user copies a 10 megabyte (MB) file onto server A (which is then at the hard limit) and another user copies a 5 MB file onto server B, when the next replication occurs, both servers will exceed the quota by 5 megabytes. This can cause DFS Replication to continually retry replicating the files, causing holes in the version vector and possible performance problems.

**Is DFS Replication cluster aware?**

Yes, DFS Replication in Windows Server 2012 R2, Windows Server 2012 and Windows Server 2008 R2 includes the ability to add a failover cluster as a member of a replication group. For more information, see Add a Failover Cluster to a Replication Group (https://go.microsoft.com/fwlink/?LinkId=155085). The DFS Replication service on versions of Windows prior to Windows Server 2008 R2 is not designed to coordinate with a failover cluster, and the service will not fail over to another node.

> **NOTE**
> DFS Replication does not support replicating files on Cluster Shared Volumes.

**Is DFS Replication compatible with Data Deduplication?**

Yes, DFS Replication can replicate folders on volumes that use Data Deduplication in Windows Server.

**Is DFS Replication compatible with RIS and WDS?**

Yes. DFS Replication replicates volumes on which Single Instance Storage (SIS) is enabled. SIS is used by Remote Installation Services (RIS), Windows Deployment Services (WDS), and Windows Storage Server.

**Is it possible to use DFS Replication with Offline Files?**

You can safely use DFS Replication and Offline Files together in scenarios when there is only one user at a time who writes to the files. This is useful for users who travel between two branch offices and want to be able to access their files at either branch or while offline. Offline Files caches the files locally for offline use and DFS Replication replicates the data between each branch office.

Do not use DFS Replication with Offline Files in a multi-user environment because DFS Replication does not provide any distributed locking mechanism or file checkout capability. If two users modify the same file at the same time on different servers, DFS Replication moves the older file to the DfsrPrivate\ConflictandDeleted folder (located under the local path of the replicated folder) during the next replication.

**What antivirus applications are compatible with DFS Replication?**

Antivirus applications can cause excessive replication if their scanning activities alter the files in a replicated folder. For more information, Testing Antivirus Application Interoperability with DFS Replication (https://go.microsoft.com/fwlink/?LinkId=73990).

**What are the benefits of using DFS Replication instead of Windows SharePoint Services?**

Windows® SharePoint® Services provides tight coherency in the form of file check-out functionality that DFS Replication does not. If you are concerned about multiple people editing the same file, we recommend using Windows SharePoint Services. Windows SharePoint Services 2.0 with Service Pack 2 is available as part of Windows Server 2003 R2. Windows SharePoint Services can be downloaded from the Microsoft Web site; it is not included in newer versions of Windows Server. However, if you are replicating data across multiple sites and users will not edit the same files at the same time, DFS Replication provides greater bandwidth and simpler management.

# Limitations and requirements

**Can DFS Replication replicate between branch offices without a VPN connection?**

Yes—assuming that there is a private Wide Area Network (WAN) link (not the Internet) connecting the branch offices. However, you must open the proper ports in external firewalls. DFS Replication uses the RPC Endpoint Mapper (port 135) and a randomly assigned ephemeral port above 1024. You can use the **Dfsrdiag** command line tool to specify a static port instead of the ephemeral port. For more information about how to specify the RPC Endpoint Mapper, see article 154596 in the Microsoft Knowledge Base (https://go.microsoft.com/fwlink/?LinkId=73991).

**Can DFS Replication replicate files encrypted with the Encrypting File System?**

No. DFS Replication will not replicate files or folders that are encrypted using the Encrypting File System (EFS). If a user encrypts a file that was previously replicated, DFS Replication deletes the file from all other members of the replication group. This ensures that the only available copy of the file is the encrypted version on the server.

**Can DFS Replication replicate Outlook .pst or Microsoft Office Access database files?**

DFS Replication can safely replicate Microsoft Outlook personal folder files (.pst) and Microsoft Access files only if they are stored for archival purposes and are not accessed across the network by using a client such as Outlook or

Access (to open .pst or Access files, first copy the files to a local storage device). The reasons for this are as follows:

- Opening .pst files over network connections could lead to data corruption in the .pst files. For more information about why .pst files cannot be safely accessed from across a network, see article 297019 in the Microsoft Knowledge Base (https://go.microsoft.com/fwlink/?LinkId=125363).
- .pst and Access files tend to stay open for long periods of time while being accessed by a client such as Outlook or Office Access. This prevents DFS Replication from replicating these files until they are closed.

**Can I use DFS Replication in a workgroup?**

No. DFS Replication relies on Active Directory® Domain Services for configuration. It will only work in a domain.

**Can more than one folder be replicated on a single server?**

Yes. DFS Replication can replicate numerous folders between servers. Ensure that each of the replicated folders has a unique root path and that they do not overlap. For example, D:\Sales and D:\Accounting can be the root paths for two replicated folders, but D:\Sales and D:\Sales\Reports cannot be the root paths for two replicated folders.

**Does DFS Replication require DFS Namespaces?**

No. DFS Replication and DFS Namespaces can be used separately or together. In addition, DFS Replication can be used to replicate standalone DFS namespaces, which was not possible with FRS.

**Does DFS Replication require time synchronization between servers?**

No. DFS Replication does not explicitly require time synchronization between servers. However, DFS Replication does require that the server clocks match closely. The server clocks must be set within five minutes of each other (by default) for Kerberos authentication to function properly. For example, DFS Replication uses time stamps to determine which file takes precedence in the event of a conflict. Accurate times are also important for garbage collection, schedules, and other features.

**Does DFS Replication support replicating an entire volume?**

Yes. However, you must first install Windows Server 2003 Service Pack 2 or the hotfix. For more information, see article 920335 in the Microsoft Knowledge Base (https://go.microsoft.com/fwlink/?LinkId=76776). Additionally, replicating an entire volume can cause the following problems:

- If the volume contains a Windows paging file, replication fails and logs DFSR event 4312 in the system event log.
- DFS Replication sets the System and Hidden attributes on the replicated folder on the destination server(s). This occurs because Windows applies the System and Hidden attributes to the volume root folder by default. If the local path of the replicated folder on the destination server(s) is also a volume root, no further changes are made to the folder attributes.
- When replicating a volume that contains the Windows system folder, DFS Replication recognizes the %WINDIR% folder and does not replicate it. However, DFS Replication does replicate folders used by non-Microsoft applications, which might cause the applications to fail on the destination server(s) if the applications have interoperability issues with DFS Replication.

**Does DFS Replication support RPC over HTTP?**

No.

**Does DFS Replication work across wireless networks?**

Yes. DFS Replication is independent of the connection type.

**Does DFS Replication work on ReFS or FAT volumes?**

No. DFS Replication supports volumes formatted with the NTFS file system only; the Resilient File System (ReFS) and the FAT file system are not supported. DFS Replication requires NTFS because it uses the NTFS change journal and other features of the NTFS file system.

**Does DFS Replication work with sparse files?**

Yes. You can replicate sparse files. The `Sparse` attribute is preserved on the receiving member.

**Do I need to log in as administrator to replicate files?**

No. DFS Replication is a service that runs under the local system account, so you do not need to log in as administrator to replicate. However, you must be a domain administrator or local administrator of the affected file servers to make changes to the DFS Replication configuration.

For more information, see "DFS Replication security requirements and delegation" in the Delegate the Ability to Manage DFS Replication (https://go.microsoft.com/fwlink/?LinkId=182294).

**How can I upgrade or replace a DFS Replication member?**

To upgrade or replace a DFS Replication member, see this blog post on the Ask the Directory Services Team blog: Replacing DFSR Member Hardware or OS.

**Is DFS Replication suitable for replicating roaming profiles?**

Yes. Certain scenarios are supported when replicating roaming user profiles. For information about the supported scenarios, see Microsoft's Support Statement Around Replicated User Profile Data (https://go.microsoft.com/fwlink/?LinkId=201282).

**Is there a file character limit or limit to the folder depth?**

Windows and DFS Replication support folder paths with up to 32 thousand characters. DFS Replication is not limited to folder paths of 260 characters.

**Must members of a replication group reside in the same domain?**

No. Replication groups can span across domains within a single forest but not across different forests.

**What are the supported limits of DFS Replication?**

The following list provides a set of scalability guidelines that have been tested by Microsoft and apply to Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019

- Size of all replicated files on a server: 100 terabytes.
- Number of replicated files on a volume: 70 million.
- Maximum file size: 250 gigabytes.

> **IMPORTANT**
> When creating replication groups with a large number or size of files we recommend exporting a database clone and using pre-seeding techniques to minimize the duration of initial replication. For more information, see DFS Replication Initial Sync in Windows Server 2012 R2: Attack of the Clones.

The following list provides a set of scalability guidelines that have been tested by Microsoft on Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008:

- Size of all replicated files on a server: 10 terabytes.
- Number of replicated files on a volume: 11 million.
- Maximum file size: 64 gigabytes.

> **NOTE**
> There is no longer a limit to the number of replication groups, replicated folders, connections, or replication group members.

For a list of scalability guidelines that have been tested by Microsoft for Windows Server 2003 R2, see DFS Replication scalability guidelines (https://go.microsoft.com/fwlink/?LinkId=75043).

**When should I not use DFS Replication?**

Do not use DFS Replication in an environment where multiple users update or modify the same files simultaneously on different servers. Doing so can cause DFS Replication to move conflicting copies of the files to the hidden DfsrPrivate\ConflictandDeleted folder.

When multiple users need to modify the same files at the same time on different servers, use the file check-out feature of Windows SharePoint Services to ensure that only one user is working on a file. Windows SharePoint Services 2.0 with Service Pack 2 is available as part of Windows Server 2003 R2. Windows SharePoint Services can be downloaded from the Microsoft Web site; it is not included in newer versions of Windows Server.

**Why is a schema update required for DFS Replication?**

DFS Replication uses new objects in the domain-naming context of Active Directory Domain Services to store configuration information. These objects are created when you update the Active Directory Domain Services schema. For more information, see Review Requirements for DFS Replication (https://go.microsoft.com/fwlink/?LinkId=182264).

## Monitoring and management tools

**Can I automate the health report to receive warnings?**

Yes. There are three ways to automate health reports:

- Use the DFSR Windows PowerShell module included in Windows Server 2012 R2 or DfsrAdmin.exe in conjunction with Scheduled Tasks to regularly generate health reports. For more information, see Automating DFS Replication Health Reports (https://go.microsoft.com/fwlink/?LinkId=74010).
- Use the DFS Replication Management Pack for System Center Operations Manager to create alerts that are based on specified conditions.
- Use the DFS Replication WMI provider to script alerts.

**Can I use Microsoft System Center Operations Manager to monitor DFS Replication?**

Yes. For more information, see the DFS Replication Management Pack for System Center Operations Manager 2007 in the Microsoft Download Center (https://go.microsoft.com/fwlink/?LinkId=182265).

**Does DFS Replication support remote management?**

Yes. DFS Replication supports remote management using the DFS Management console and the **Add Replication Group** command. For example, on server A, you can connect to a replication group defined in the forest with servers A and B as members.

DFS Management is included with Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 R2. To manage DFS Replication from other versions of Windows, use Remote Desktop or the Remote Server Administration Tools for Windows 7.

> **IMPORTANT**
>
> To view or manage replication groups that contain read-only replicated folders or members that are failover clusters, you must use the version of DFS Management that is included with Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, the Remote Server Administration Tools for Windows 8, or the Remote Server Administration Tools for Windows 7.

**Do Ultrasound and Sonar work with DFS Replication?**

No. DFS Replication has its own set of monitoring and diagnostics tools. Ultrasound and Sonar are only capable of

monitoring FRS.

**How can files be recovered from the ConflictAndDeleted or PreExisting folders?**

To recover lost files, restore the files from the file system folder or shared folder using File History, the **Restore previous versions** command in File Explorer, or by restoring the files from backup. To recover files directly from the ConflictAndDeleted or PreExisting folder, use the `Get-DfsrPreservedFiles` and `Restore-DfsrPreservedFiles` Windows PowerShell cmdlets (included with the DFSR module in Windows Server 2012 R2), or the RestoreDFSR sample script from the MSDN Code Gallery. This script is intended only for disaster recovery and is provided AS-IS, without warranty.

**Is there a way to know the state of replication?**

Yes. There are a number of ways to monitor replication:

- DFS Replication has a management pack for System Center Operations Manager that provides proactive monitoring.
- DFS Management has an in-box diagnostic report for the replication backlog, replication efficiency, and the number of files and folders in a given replication group.
- The DFSR Windows PowerShell module in Windows Server 2012 R2 contains cmdlets for starting propagation tests and writing propagation and health reports. For more information, see Distributed File System Replication Cmdlets in Windows PowerShell.
- Dfsrdiag.exe is a command-line tool that can generate a backlog count or trigger a propagation test. Both show the state of replication. Propagation shows you if files are being replicated to all nodes. Backlog shows you how many files still need to replicate before two computers are in sync. The backlog count is the number of updates that a replication group member has not processed. On computers running Windows Server 2012 R2, Windows Server 2012 or Windows Server 2008 R2, Dfsrdiag.exe can also display the updates that DFS Replication is currently replicating.
- Scripts can use WMI to collect backlog information—manually or through MOM.

# Performance

**Does DFS Replication support dial-up connections?**

Although DFS Replication will work at dial-up speeds, it can get backlogged if there are large numbers of changes to replicate. If small changes are made to existing files, DFS Replication with Remote Differential Compression (RDC) will provide a much higher performance than copying the file directly.

**Does DFS Replication perform bandwidth sensing?**

No. DFS Replication does not perform bandwidth sensing. You can configure DFS Replication to use a limited amount of bandwidth on a per-connection basis (bandwidth throttling). However, DFS Replication does not further reduce bandwidth utilization if the network interface becomes saturated, and DFS Replication can saturate the link for short periods. Bandwidth throttling with DFS Replication is not completely accurate because DFS Replication throttles bandwidth by throttling RPC calls. As a result, various buffers in lower levels of the network stack (including RPC) may interfere, causing bursts of network traffic.

**Does DFS Replication throttle bandwidth per schedule, per server, or per connection?**

If you configure bandwidth throttling when specifying the schedule, all connections for that replication group will use that setting for bandwidth throttling. Bandwidth throttling can be also set as a connection-level setting using DFS Management.

**Does DFS Replication use Active Directory Domain Services to calculate site links and connection costs?**

No. DFS Replication uses the topology defined by the administrator, which is independent of Active Directory Domain Services site costing.

**How can I improve replication performance?**

To learn about different methods of tuning replication performance, see Tuning Replication Performance in DFSR on the Ask the Directory Services Team blog.

**How does DFS Replication avoid saturating a connection?**

In DFS Replication you set the maximum bandwidth you want to use on a connection, and the service maintains that level of network usage. This is different from the Background Intelligent Transfer Service (BITS), and DFS Replication does not saturate the connection if you set it appropriately.

Nonetheless, the bandwidth throttling is not 100% accurate and DFS Replication can saturate the link for short periods of time. This is because DFS Replication throttles bandwidth by throttling RPC calls. Because this process relies on various buffers in lower levels of the network stack, including RPC, the replication traffic tends to travel in bursts which may at times saturate the network links.

DFS Replication in Windows Server 2008 includes several performance enhancements, as discussed in Distributed File System, a topic in Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008.

**How does DFS Replication performance compare with FRS?**

DFS Replication is much faster than FRS, particularly when small changes are made to large files and RDC is enabled. For example, with RDC, a small change to a 2 MB PowerPoint® presentation can result in only 60 kilobytes (KB) being sent across the network—a 97 percent savings in bytes transferred.

RDC is not used on files smaller than 64 KB and might not be beneficial on high-speed LANs where network bandwidth is not contended. RDC can be disabled on a per-connection basis using DFS Management.

**How frequently does DFS Replication replicate data?**

Data replicates according to the schedule you set. For example, you can set the schedule to 15-minute intervals, seven days a week. During these intervals, replication is enabled. Replication starts soon after a file change is detected (generally within seconds).

The replication group schedule may be set to Universal Time Coordinate (UTC) while the connection schedule is set to the local time of the receiving member. Take this into account when the replication group spans multiple time zones. Local time means the time of the member hosting the inbound connection. The displayed schedule of the inbound connection and the corresponding outbound connection reflect time zone differences when the schedule is set to local time.

**How much of my server's system resources will DFS Replication consume?**

The disk, memory, and CPU resources used by DFS Replication depend on a number of factors, including the number and size of the files, rate of change, number of replication group members, and number of replicated folders. In addition, some resources are harder to estimate. For example, the Extensible Storage Engine (ESE) technology used for the DFS Replication database can consume a large percentage of available memory, which it releases on demand. Applications other than DFS Replication can be hosted on the same server depending on the server configuration. However, when hosting multiple applications or server roles on a single server, it is important that you test this configuration before implementing it in a production environment.

**What happens if a WAN link fails during replication?**

If the connection goes down, DFS Replication will keep trying to replicate while the schedule is open. There will also be connectivity errors noted in the DFS Replication event log that can be harvested using MOM (proactively through alerts) and the DFS Replication Health Report (reactively, such as when an administrator runs it).

## Remote Differential Compression details

**Are changes compressed before being replicated?**

Yes. Changed portions of files are compressed before being sent for all file types except the following (which are already compressed): .wma, .wmv, .zip, .jpg, .mpg, .mpeg, .m1v, .mp2, .mp3, .mpa, .cab, .wav, .snd, .au, .asf, .wm, .avi,

.z, .gz, .tgz, and .frx. Compression settings for these file types are not configurable in Windows Server 2003 R2.

**Can an administrator turn off RDC or change the threshold?**

Yes. You can turn off RDC through the property page of a given connection. Disabling RDC can reduce CPU utilization and replication latency on fast local area network (LAN) links that have no bandwidth constraints or for replication groups that consist primarily of files smaller than 64 KB. If you choose to disable RDC on a connection, test the replication efficiency before and after the change to verify that you have improved replication performance.

You can change the RDC size threshold by using the **Dfsradmin Connection Set** command, the DFS Replication WMI Provider, or by manually editing the configuration XML file.

**Does RDC work on all file types?**

Yes. RDC computes differences at the block level irrespective of file data type. However, RDC works more efficiently on certain file types such as Word docs, PST files, and VHD images.

**How does RDC work on a compressed file?**

DFS Replication uses RDC, which computes the blocks in the file that have changed and sends only those blocks over the network. DFS Replication does not need to know anything about the contents of the file—only which blocks have changed.

**Is cross-file RDC enabled when upgrading to Windows Server Enterprise Edition or Datacenter Edition?**

The Standard Editions of Windows Server do not support cross-file RDC. However, it is automatically enabled when you upgrade to an edition that supports cross-file RDC, or if a member of the replication connection is running a supported edition. For a list of editions that support cross-file RDC, see Which editions of the Windows operating system support cross-file RDC?

**Is RDC true block-level replication?**

No. RDC is a general purpose protocol for compressing file transfer. DFS Replication uses RDC on blocks at the file level, not at the disk block level. RDC divides a file into blocks. For each block in a file, it calculates a signature, which is a small number of bytes that can represent the larger block. The set of signatures is transferred from server to client. The client compares the server signatures to its own. The client then requests the server send only the data for signatures that are not already on the client.

**What happens if I rename a file?**

DFS Replication renames the file on all other members of the replication group during the next replication. Files are tracked using a unique ID, so renaming a file and moving the file within the replica has no effect on the ability of DFS Replication to replicate a file.

**What is cross-file RDC?**

Cross-file RDC allows DFS Replication to use RDC even when a file with the same name does not exist at the client end. Cross-file RDC uses a heuristic to determine files that are similar to the file that needs to be replicated, and uses blocks of the similar files that are identical to the replicating file to minimize the amount of data transferred over the WAN. Cross-file RDC can use blocks of up to five similar files in this process.

To use cross-file RDC, one member of the replication connection must be running an edition of Windows that supports cross-file RDC. For a list of editions that support cross-file RDC, see Which editions of the Windows operating system support cross-file RDC?

**What is RDC?**

Remote differential compression (RDC) is a client-server protocol that can be used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, and rearrangements of data in files, enabling DFS Replication to replicate only the changes when files are updated. RDC is used only for files that are 64 KB or larger by default. RDC can use an older version of a file with the same name in the replicated folder or in the DfsrPrivate\ConflictandDeleted folder (located under the local path of the replicated folder).

### When is RDC used for replication?

RDC is used when the file exceeds a minimum size threshold. This size threshold is 64 KB by default. After a file exceeding that threshold has been replicated, updated versions of the file always use RDC, unless a large portion of the file is changed or RDC is disabled.

### Which editions of the Windows operating system support cross-file RDC?

To use cross-file RDC, one member of the replication connection must be running an edition of the Windows operating system that supports cross-file RDC. The following table shows which editions of the Windows operating system support cross-file RDC.

**Cross-file RDC availability in editions of the Windows operating system**

| OPERATING SYSTEM VERSION | STANDARD EDITION | ENTERPRISE EDITION | DATACENTER EDITION |
|---|---|---|---|
| Windows Server 2012 R2 | Yes | Not available | Yes |
| Windows Server 2012 | Yes | Not available | Yes |
| Windows Server 2008 R2 | No | Yes | Yes |
| Windows Server 2008 | No | Yes | No |
| Windows Server 2003 R2 | No | Yes | No |

* You can optionally disable cross-file RDC on Windows Server 2012 R2.

## Replication details

### Can I change the path for a replicated folder after it is created?

No. If you need to change the path of a replicated folder, you must delete it in DFS Management and add it back as a new replicated folder. DFS Replication then uses Remote Differential Compression (RDC) to perform a synchronization that determines whether the data is the same on the sending and receiving members. It does not replicate all the data in the folder again.

### Can I configure which file attributes are replicated?

No, you cannot configure which file attributes that DFS Replication replicates.

For a list of attribute values and their descriptions, see File Attributes on MSDN (https://go.microsoft.com/fwlink/?LinkId=182268).

The following attribute values are set by using the `SetFileAttributes dwFileAttributes` function, and they are replicated by DFS Replication. Changes to these attribute values trigger replication of the attributes. The contents of the file are not replicated unless the contents change as well. For more information, see SetFileAttributes Function in the MSDN library (https://go.microsoft.com/fwlink/?LinkId=182269).

- FILE_ATTRIBUTE_HIDDEN
- FILE_ATTRIBUTE_READONLY

- FILE_ATTRIBUTE_SYSTEM
- FILE_ATTRIBUTE_NOT_CONTENT_INDEXED
- FILE_ATTRIBUTE_OFFLINE

The following attribute values are replicated by DFS Replication, but they do not trigger replication.

- FILE_ATTRIBUTE_ARCHIVE
- FILE_ATTRIBUTE_NORMAL

The following file attribute values also trigger replication, although they cannot be set by using the `SetFileAttributes` function (use the `GetFileAttributes` function to view the attribute values).

- FILE_ATTRIBUTE_REPARSE_POINT

> **NOTE**
> DFS Replication does not replicate reparse point attribute values unless the reparse tag is IO_REPARSE_TAG_SYMLINK. Files with the IO_REPARSE_TAG_DEDUP, IO_REPARSE_TAG_SIS or IO_REPARSE_TAG_HSM reparse tags are replicated as normal files. However, the reparse tag and reparse data buffers are not replicated to other servers because the reparse point only works on the local system.

- FILE_ATTRIBUTE_COMPRESSED
- FILE_ATTRIBUTE_ENCRYPTED

> **NOTE**
> DFS Replication does not replicate files that are encrypted by using the Encrypting File System (EFS). DFS Replication does replicate files that are encrypted by using non-Microsoft software, but only if it does not set the FILE_ATTRIBUTE_ENCRYPTED attribute value on the file.

- FILE_ATTRIBUTE_SPARSE_FILE
- FILE_ATTRIBUTE_DIRECTORY

DFS Replication does not replicate the FILE_ATTRIBUTE_TEMPORARY value.

**Can I control which member is replicated?**

Yes. You can choose a topology when you create a replication group. Or you can select **No topology** and manually configure connections after the replication group has been created.

**Can I seed a replication group member with data prior to the initial replication?**

Yes. DFS Replication supports copying files to a replication group member before the initial replication. This "prestaging" can dramatically reduce the amount of data replicated during the initial replication.

The initial replication does not need to replicate contents when files differ only by real attributes or time stamps. A real attribute is an attribute that can be set by the Win32 function `SetFileAttributes`. For more information, see SetFileAttributes Function in the MSDN library (https://go.microsoft.com/fwlink/?LinkId=182269). If two files differ by other attributes, such as compression, then the contents of the file are replicated.

To prestage a replication group member, copy the files to the appropriate folder on the destination server(s), create the replication group, and then choose a primary member. Choose the member that has the most up-to-date files that you want to replicate because the primary member's content is considered "authoritative." This means that during initial replication, the primary member's files will always overwrite other versions of the files on other

members of the replication group.

For information about pre-seeding and cloning the DFSR database, see DFS Replication Initial Sync in Windows Server 2012 R2: Attack of the Clones.

For more information about the initial replication, see Create a Replication Group.

**Does DFS Replication overcome common File Replication Service issues?**

Yes. DFS Replication overcomes three common FRS issues:

- Journal wraps: DFS Replication recovers from journal wraps on the fly. Each existing file or folder will be marked as journalWrap and verified against the file system before replication is enabled again. During the recovery, this volume is not available for replication in either direction.
- Excessive replication: To prevent excessive replication, DFS Replication uses a system of credits.
- Morphed folders: To prevent morphed folder names, DFS Replication stores conflicting data in a hidden DfsrPrivate\ConflictandDeleted folder (located under the local path of the replicated folder). For example, creating multiple folders simultaneously with identical names on different servers replicated using FRS causes FRS to rename the older folder(s). DFS Replication instead moves the older folder(s) to the local Conflict and Deleted folder.

**Does DFS Replication replicate files in chronological order?**

No. Files may be replicated out of order.

**Does DFS Replication replicate files that are being used by another application?**

If an application opens a file and creates a file lock on it (preventing it from being used by other applications while it is open), DFS Replication will not replicate the file until it is closed. If the application opens the file with read-share access, the file can still be replicated.

**Does DFS Replication replicate NTFS file permissions, alternate data streams, hard links, and reparse points?**

- DFS Replication replicates NTFS file permissions and alternate data streams.
- Microsoft does not support creating NTFS hard links to or from files in a replicated folder – doing so can cause replication issues with the affected files. Hard link files are ignored by DFS Replication and are not replicated. Junction points also are not replicated, and DFS Replication logs event 4406 for each junction point it encounters.
- The only reparse points replicated by DFS Replication are those that use the IO_REPARSE_TAG_SYMLINK tag; however, DFS Replication does not guarantee that the target of a symlink is also replicated. For more information, see the Ask the Directory Services Team blog.
- Files with the IO_REPARSE_TAG_DEDUP, IO_REPARSE_TAG_SIS, or IO_REPARSE_TAG_HSM reparse tags are replicated as normal files. The reparse tag and reparse data buffers are not replicated to other servers because the reparse point only works on the local system. As such, DFS Replication can replicate folders on volumes that use Data Deduplication in Windows Server 2012, or Single Instance Storage (SIS), however, data deduplication information is maintained separately by each server on which the role service is enabled.

**Does DFS Replication replicate timestamp changes if no other changes are made to the file?**

No, DFS Replication does not replicate files for which the only change is a change to the timestamp. Additionally, the changed timestamp is not replicated to other members of the replication group unless other changes are made to the file.

**Does DFS Replication replicate updated permissions on a file or folder?**

Yes. DFS Replication replicates permission changes for files and folders. Only the part of the file associated with the Access Control List (ACL) is replicated, although DFS Replication must still read the entire file into the staging area.

> **NOTE**
> Changing ACLs on a large number of files can have an impact on replication performance. However, when using RDC, the amount of data transferred is proportionate to the size of the ACLs, not the size of the entire file. The amount of disk traffic is still proportional to the size of the files because the files must be read to and from the staging folder.

**Does DFS Replication support merging text files in the event of a conflict?**

DFS Replication does not merge files when there is a conflict. However, it does attempt to preserve the older version of the file in the hidden DfsrPrivate\ConflictandDeleted folder on the computer where the conflict was detected.

**Does DFS Replication use encryption when transmitting data?**

Yes. DFS Replication uses Remote Procedure Call (RPC) connections with encryption.

**Is it possible to disable the use of encrypted RPC?**

No. The DFS Replication service uses remote procedure calls (RPC) over TCP to replicate data. To secure data transfers across the Internet, the DFS Replication service is designed to always use the authentication-level constant, `RPC_C_AUTHN_LEVEL_PKT_PRIVACY`. This ensures that the RPC communication across the Internet is always encrypted. Therefore, it is not possible to disable the use of encrypted RPC by the DFS Replication service.

For more information, see the following Microsoft Web sites:

- RPC Technical Reference
- About Remote Differential Compression
- Authentication-Level Constants

**How are simultaneous replications handled?**

There is one update manager per replicated folder. Update managers work independently of one another.

By default, a maximum of 16 (four in Windows Server 2003 R2) concurrent downloads are shared among all connections and replication groups. Because connections and replication group updates are not serialized, there is no specific order in which updates are received. If two schedules are opened, updates are generally received and installed from both connections at the same time.

**How do I force replication or polling?**

You can force replication immediately by using DFS Management, as described in Edit Replication Schedules. You can also force replication by using the `Sync-DfsReplicationGroup` cmdlet, included in the DFSR PowerShell module introduced with Windows Server 2012 R2, or the **Dfsrdiag SyncNow** command. You can force polling by using the `Update-DfsrConfigurationFromAD` cmdlet, or the **Dfsrdiag PollAD** command.

**Is it possible to configure a quiet time between replications for files that change frequently?**

No. If the schedule is open, DFS Replication will replicate changes as it notices them. There is no way to configure a quiet time for files.

**Is it possible to configure one-way replication with DFS Replication?**

Yes. If you are using Windows Server 2012 or Windows Server 2008 R2, you can create a read-only replicated folder that replicates content through a one-way connection. For more information, see Make a Replicated Folder Read-Only on a Particular Member (https://go.microsoft.com/fwlink/?LinkId=156740).

We do not support creating a one-way replication connection with DFS Replication in Windows Server 2008 or Windows Server 2003 R2. Doing so can cause numerous problems including health-check topology errors, staging issues, and problems with the DFS Replication database.

If you are using Windows Server 2008 or Windows Server 2003 R2, you can simulate a one-way connection by

performing the following actions:

- Train administrators to make changes only on the server(s) that you want to designate as primary servers. Then let the changes replicate to the destination servers.
- Configure the share permissions on the destination servers so that end users do not have Write permissions. If no changes are allowed on the branch servers, then there is nothing to replicate back, simulating a one-way connection and keeping WAN utilization low.

**Is there a way to force a complete replication of all files including unchanged files?**

No. If DFS Replication considers the files identical, it will not replicate them. If changed files have not been replicated, DFS Replication will automatically replicate them when configured to do so. To overwrite the configured schedule, use the WMI method **ForceReplicate()**. However, this is only a schedule override, and it does not force replication of unchanged or identical files.

**What happens if the primary member suffers a database loss during initial replication?**

During initial replication, the primary member's files will always take precedence in the conflict resolution that occurs if the receiving members have different versions of files on the primary member. The primary member designation is stored in Active Directory Domain Services, and the designation is cleared after the primary member is ready to replicate, but before all members of the replication group replicate.

If the initial replication fails or the DFS Replication service restarts during the replication, the primary member sees the primary member designation in the local DFS Replication database and retries the initial replication. If the primary member's DFS Replication database is lost after clearing the primary designation in Active Directory Domain Services, but before all members of the replication group complete the initial replication, all members of the replication group fail to replicate the folder because no server is designated as the primary member. If this happens, use the **Dfsradmin membership /set /isprimary:true** command on the primary member server to restore the primary member designation manually.

For more information about initial replication, see Create a Replication Group.

> **WARNING**
> The primary member designation is used only during the initial replication process. If you use the **Dfsradmin** command to specify a primary member for a replicated folder after replication is complete, DFS Replication does not designate the server as a primary member in Active Directory Domain Services. However, if the DFS Replication database on the server subsequently suffers irreversible corruption or data loss, the server attempts to perform an initial replication as the primary member instead of recovering its data from another member of the replication group. Essentially, the server becomes a rogue primary server, which can cause conflicts. For this reason, specify the primary member manually only if you are certain that the initial replication has irretrievably failed.

**What happens if the replication schedule closes while a file is being replicated?**

If remote differential compression (RDC) is enabled on the connection, inbound replication of a file larger than 64 KB that began replicating immediately prior to the schedule closing (or changing to **No bandwidth**) continues when the schedule opens (or changes to something other than **No bandwidth**). The replication continues from the state it was in when replication stopped.

If RDC is turned off, DFS Replication completely restarts the file transfer. This can delay when the file is available on the receiving member.

**What happens when two users simultaneously update the same file on different servers?**

When DFS Replication detects a conflict, it uses the version of the file that was saved last. It moves the other file into the DfsrPrivate\ConflictandDeleted folder (under the local path of the replicated folder on the computer that resolved the conflict). It remains there until Conflict and Deleted folder cleanup, which occurs when the Conflict and Deleted folder exceeds the configured size or DFS Replication encounters an Out of disk space error. The Conflict

and Deleted folder is not replicated, and this method of conflict resolution avoids the problem of morphed directories that was possible in FRS.

When a conflict occurs, DFS Replication logs an informational event to the DFS Replication event log. This event does not require user action for the following reasons:

- It is not visible to users (it is visible only to server administrators).
- DFS Replication treats the Conflict and Deleted folder as a cache. When a quota threshold is reached, it cleans out some of those files. There is no guarantee that conflicting files will be saved.
- The conflict could reside on a server different from the origin of the conflict.

## Staging

**Does DFS Replication continue staging files when replication is disabled by a schedule or bandwidth throttling quota, or when a connection is manually disabled?**

No. DFS Replication does not continue to stage files outside of scheduled replication times, if the bandwidth throttling quota has been exceeded, or when connections are disabled.

**Does DFS Replication prevent other applications from accessing a file during staging?**

No. DFS Replication opens files in a way that does not block users or applications from opening files in the replication folder. This method is known as "opportunistic locking."

**Is it possible to change the location of the staging folder with the DFS Management Tool?**

Yes. The staging folder location is configured on the **Advanced** tab of the **Properties** dialog box for each member of a replication group.

**When are files staged?**

Files are staged on the sending member when the receiving member requests the file (unless the file is 64 KB or smaller) as shown in the following table. If Remote Differential Compression (RDC) is disabled on the connection, the file is staged unless it is 256 KB or smaller. Files are also staged on the receiving member as they are transferred if they are less than 64 KB in size, although you can configure this setting between 16 KB and 1 MB. If the schedule is closed, files are not staged.

**The minimum file sizes for staging files**

| | RDC ENABLED | RDC DISABLED |
|---|---|---|
| Sending member | 64 KB | 256 KB |
| Receiving member | 64 KB by default | 64 KB by default |

**What happens if a file is changed after it is staged but before it is completely transmitted to the remote site?**

If any part of the file is already being transmitted, DFS Replication continues the transmission. If the file is changed before DFS Replication begins transmitting the file, then the newer version of the file is sent.

## Change History

| DATE | DESCRIPTION | REASON |
|---|---|---|
| November 15, 2018 | Updated for Windows Server 2019. | New operating system. |

| DATE | DESCRIPTION | REASON |
| --- | --- | --- |
| October 9th, 2013 | Updated the What are the supported limits of DFS Replication? section with results from tests on Windows Server 2012 R2. | Updates for the latest version of Windows Server |
| January 30th, 2013 | Added the Does DFS Replication continue staging files when replication is disabled by a schedule or bandwidth throttling quota, or when a connection is manually disabled? entry. | Customer questions |
| October 31st, 2012 | Edited the What are the supported limits of DFS Replication? entry to increase the tested number of replicated files on a volume. | Customer feedback |
| August 15, 2012 | Edited the Does DFS Replication replicate NTFS file permissions, alternate data streams, hard links, and reparse points? entry to further clarify how DFS Replication handles hard links and reparse points. | Feedback from Customer Support Services |
| June 13, 2012 | Edited the Does DFS Replication work on ReFS or FAT volumes? entry to add discussion of ReFS. | Customer feedback |
| April 25, 2012 | Edited the Does DFS Replication replicate NTFS file permissions, alternate data streams, hard links, and reparse points? entry to clarify how DFS Replication handles hard links. | Reduce potential confusion |
| March 30, 2011 | Edited the Can DFS Replication replicate Outlook .pst or Microsoft Office Access database files? entry to correct the potential impact of using DFS Replication with .pst and Access files.<br>Added How can I improve replication performance? | Customer questions about the previous entry, which incorrectly indicated that replicating .pst or Access files could corrupt the DFS Replication database. |
| January 26, 2011 | Added How can files be recovered from the ConflictAndDeleted or PreExisting folders? | Customer feedback |
| October 20, 2010 | Added How can I upgrade or replace a DFS Replication member? | Customer feedback |

# How to determine the minimum staging area DFSR needs for a replicated folder

11/2/2020 • 7 minutes to read • Edit Online

This article is a quick reference guide on how to calculate the minimum staging area needed for DFSR to function properly. Values lower than these may cause replication to go slowly or stop altogether.

Keep in mind these are *minimums only*. When considering staging area size, the bigger the staging area the better, up to the size of the Replicated Folder. See the section "How to determine if you have a staging area problem" and the blog posts linked at the end of this article for more details on why it is important to have a properly sized staging area.

> **NOTE**
> We also have a hotfix to help you with calculating staging sizes. Update for the DFS Replication (DFSR) Management interface is available

## Rules of thumb

**Windows Server 2003 R2** – The staging area quota must be as large as the 9 largest files in the Replicated Folder

**Windows Server 2008 and 2008 R2** – The staging area quota must be as large as the 32 largest files in the Replicated Folder

Initial Replication will make much more use of the staging area than day-to-day replication. Setting the staging area higher than the minimum during initial replication is strongly encouraged if you have the drive space available

## Where do I get PowerShell?

PowerShell is included on Windows 2008 and higher. You must install PowerShell on Windows Server 2003. You can download PowerShell for Windows 2003 here.

## How do you find these X largest files?

Use a PowerShell script to find the 32 or 9 largest files and determine how many gigabytes they add up to (thanks to Ned Pyle for the PowerShell commands). I am actually going to present you with three PowerShell scripts. Each is useful on its own; however, number 3 is the most useful.

1. Run the following command:

   ```
   Get-ChildItem c:\\temp -recurse | Sort-Object length -descending | select-object -first 32 | ft
   name,length -wrap –auto
   ```

   This command will return the file names and the size of the files in bytes. Useful if you want to know what 32 files are the largest in the Replicated Folder so you can “visit” their owners.

2. Run the following command:

```
Get-ChildItem c:\\temp -recurse | Sort-Object length -descending | select-object -first 32 | measure-object -property length –sum
```

This command will return the total number of bytes of the 32 largest files in the folder without listing the file names.

3. Run the following command:

```
$big32 = Get-ChildItem c:\\temp -recurse | Sort-Object length -descending | select-object -first 32 | measure-object -property length –sum

$big32.sum /1gb
```

This command will get the total number of bytes of 32 largest files in the folder and do the math to convert bytes to gigabytes for you. This command is two separate lines. You can paste both them into the PowerShell command shell at once or run them back to back.

# Manual Walkthrough

To demonstrate the process and hopefully increase understanding of what we are doing, I am going to manually step through each part.

Running command 1 will return results similar to the output below. This example only uses 16 files for brevity. Always use 32 for Windows 2008 and later operating systems and 9 for Windows 2003 R2

**Example Data returned by PowerShell**

| Name | Length |
|---|---|
| **File5.zip** | 10286089216 |
| **archive.zip** | 6029853696 |
| **BACKUP.zip** | 5751522304 |
| **file9.zip** | 5472683008 |
| **MENTOS.zip** | 5241586688 |
| **File7.zip** | 4321264640 |
| **file2.zip** | 4176765952 |
| **frd2.zip** | 4176765952 |
| **BACKUP.zip** | 4078994432 |
| **File44.zip** | 4058424320 |
| **file11.zip** | 3858056192 |
| **Backup2.zip** | 3815138304 |

| | |
|---|---|
| **BACKUP3.zip** | 3815138304 |
| **Current.zip** | 3576931328 |
| **Backup8.zip** | 3307488256 |
| **File999.zip** | 3274982400 |

**How to use this data to determine the minimum staging area size:**

- Name = Name of the file.
- Length = bytes
- One Gigabyte = 1073741824 Bytes

First, you need to sum the total number of bytes. Next divide the total by 1073741824. I suggest using Excel or your spreadsheet of choice to do the math.

**Example**

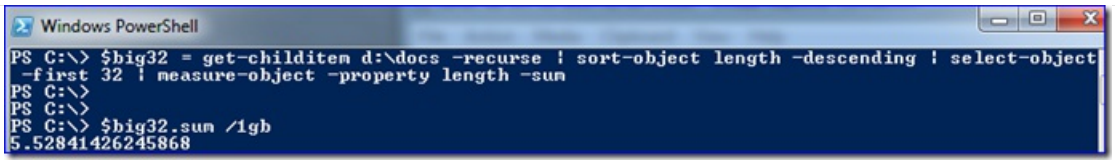
From the example above the total number of bytes = 75241684992. To get the minimum staging area quota needed I need to divide 75241684992 by 1073741824.

> 75241684992 / 1073741824 = 70.07 GB

Based on this data I would set my staging area to 71 GB if I round up to the nearest whole number.

**Real World Scenario:**

While a manual walkthrough is interesting it is likely not the best use of your time to do the math yourself. To automate the process, use command 3 from the examples above. The results will look like this




Using the example command 3 without any extra effort except for rounding to the nearest whole number, I can determine that I need a 6 GB staging area quota for d:\docs.

## Do I Need to Reboot or Restart the Service for the Changes to be Picked Up?

Changes to the staging area quota do not require a reboot or restart of the service to take effect. You will need to wait on AD replication and DFSR's AD polling cycle for the changes to be applied.

## How to determine if you have a staging area problem

You detect staging area problems by monitoring for specific events IDs on your DFSR servers. The list of events is 4202, 4204, 4206, 4208 and 4212. The texts of these events are listed below. It is important to distinguish between 4202 and 4204 and the other events. It is possible to log a high number of 4202 and 4204 events under normal operating conditions. Think of 4202 and 4204 events as being analogous to taking your pulse whereas 4206, 4208 and 4212 are like chest pains. I explain below how to interpret your 4202 and 4204 events below.

**Staging Area Events**

> Event ID: **4202** Severity: **Warning**

> The DFS Replication service has detected that the staging space in use for the replicated folder at local path (path) is above the high watermark. The service will attempt to delete the oldest staging files. Performance may be affected.
>
> Event ID: **4204** Severity: **Informational**
>
> The DFS Replication service has successfully deleted old staging files for the replicated folder at local path (path). The staging space is now below the high watermark.
>
> Event ID: **4206** Severity: **Warning**
>
> The DFS Replication service failed to clean up old staging files for the replicated folder at local path (path). The service might fail to replicate some large files and the replicated folder might get out of sync. The service will automatically retry staging space cleanup in (x) minutes. The service may start cleanup earlier if it detects some staging files have been unlocked.
>
> Event ID: **4208** Severity: **Warning**
>
> The DFS Replication service detected that the staging space usage is above the staging quota for the replicated folder at local path (path). The service might fail to replicate some large files and the replicated folder might get out of sync. The service will attempt to clean up staging space automatically.
>
> Event ID: **4212** Severity: **Error**
>
> The DFS Replication service could not replicate the replicated folder at local path (path) because the staging path is invalid or inaccessible.

## What is the difference between 4202 and 4208?

Events 4202 and 4208 have similar text; i.e. DFSR detected the staging area usage exceeds the high watermark. The difference is that 4208 is logged after staging area cleanup has run and the staging quota is still exceeded. 4202 is a normal and expected event whereas 4208 is abnormal and requires intervention.

## How many 4202, 4204 events are too many?

There is no single answer to this question. Unlike 4206, 4208 or 4212 events, which are always bad and indicate action is needed, 4202 and 4204 events occur under normal operating conditions. Seeing many 4202 and 4204 events *may* indicate a problem. Things to consider:

1. Is the Replicated Folder (RF) logging 4202 performing initial replication? If so, it is normal to log 4202 and 4204 events. You will want to keep these to down to as few as possible during Initial Replication by providing as much staging area as possible
2. Simply checking the total number of 4202 events is not sufficient. You have to know how many were logged per RF. If you log twenty 4202 events for one RF in a 24 hour period that is high. However if you have 20 Replicated Folders and there is one event per folder, you are doing well.
3. You should examine several days of data to establish trends.

I usually counsel customers to allow no more than one 4202 event per Replicated Folder per day under normal operating conditions. "Normal" meaning no Initial Replication is occurring. I base this on the reasoning that:

1. Time spent cleaning up the staging area is time spent not replicating files. Replication is paused while the staging area is cleared.
2. DFSR benefits from a full staging area using it for RDC and cross-file RDC or replicating the same files to other members
3. The more 4202 and 4204 events you log the greater the odds you will run into the condition where DFSR cannot clean up the staging area or will have to prematurely purge files from the staging area.

4. 4206, 4208 and 4212 events are, in my experience, always preceded and followed by a high number of 4202 and 4204 events.

While allowing for only one 4202 event per RF per day is conservative it greatly decreases your odds of running into staging area problems and better utilizes your DFSR server's resources for the intended purpose of replicating files.

# Understanding (the Lack of) Distributed File Locking in DFSR

11/2/2020 • 7 minutes to read • Edit Online

This article discusses the absence of a multi-host distributed file locking mechanism within Windows, and specifically within folders replicated by DFSR.

## Some Background

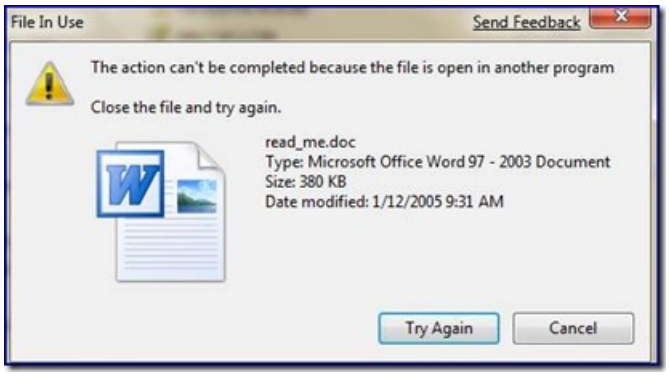
- Distributed File Locking – this refers to the concept of having multiple copies of a file on several computers and when one file is opened for writing, all other copies are locked. This prevents a file from being modified on multiple servers at the same time by several users.
- Distributed File System Replication – DFSR operates in a multi-master, state-based design. In state-based replication, each server in the multi-master system applies updates to its replica as they arrive, without exchanging log files (it instead uses version vectors to maintain "up-to-dateness" information). No one server is ever arbitrarily authoritative after initial sync, so it is highly available and very flexible on various network topologies.
- Server Message Block - SMB is the common protocol used in Windows for accessing files over the network. In simplified terms, it's a client-server protocol that makes use of a redirector to have remote file systems appear to be local file systems. It is not specific to Windows and is quite common – a well known non-Microsoft example is Samba, which allows Linux, Mac, and other operating systems to act as SMB clients/servers and participate in Windows networks.

It's important to make a clear delineation of where DFSR and SMB live in your replicated data environment. SMB allows users to access their files, and it has no awareness of DFSR. Likewise, DFSR (using the RPC protocol) keeps files in sync between servers and has no awareness of SMB. Don't confuse distributed locking as defined in this post and Opportunistic Locking.

So here's where things can go pear-shaped, as the Brits say.

Since users can modify data on multiple servers, and since each Windows server only knows about a file lock on itself, *and* since DFSR doesn't know anything about those locks on other servers, it becomes possible for users to overwrite each other's changes. DFSR uses a "last writer wins" conflict algorithm, so someone has to lose and the person to save last gets to keep their changes. The losing file copy is chucked into the *ConflictAndDeleted* folder.

Now, this is far *less* common than people like to believe. Typically, true shared files are modified in a local environment; in the branch office or in the same row of cubicles. They are usually worked on by people on the same team, so people are generally aware of colleagues modifying data. And since they are usually in the same site, the odds are much higher that all the users working on a shared doc will be using the same server. Windows SMB handles the situation here. When a user has a file locked for modification and his coworker tries to edit it, the other user will get an error like:




And if the application opening the file is really clever, like Word 2007, it might give you:


DFSR does have a mechanism for locked files, but it is only within the server's own context. DFSR will not replicate a file in or out if its local copy has an exclusive lock. But this doesn't prevent anyone on another server from modifying the file.

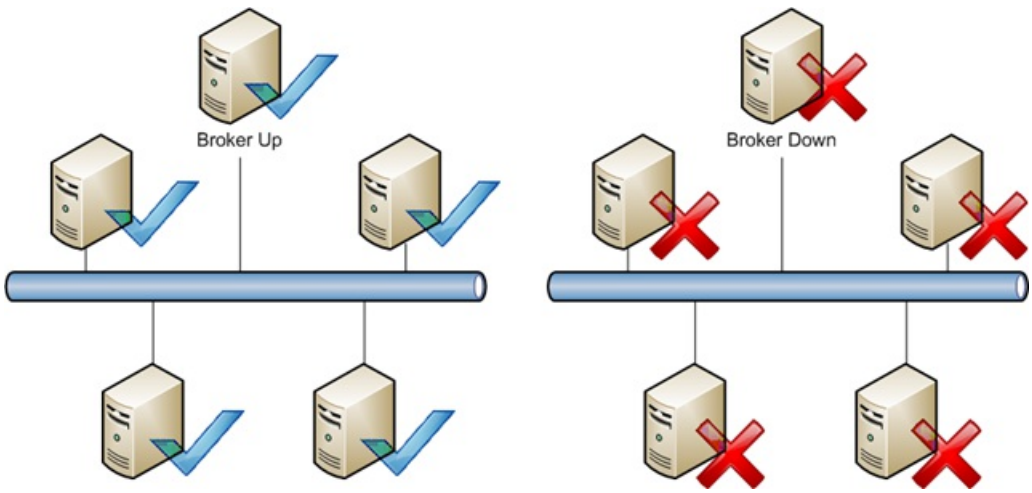
Back on topic, the issue of shared data being modified geographically *does* exist, and for some folks it's pretty gnarly. We're occasionally asked why DFSR doesn't handle this locking and take of everything with a wave of the magic wand. It turns out this is an interesting and difficult scenario to solve for a multi-master replication system. Let's explore.

## Third-Party Solutions

There are some vendor solutions that take on this problem, which they typically tackle through one or more of the following methods*:

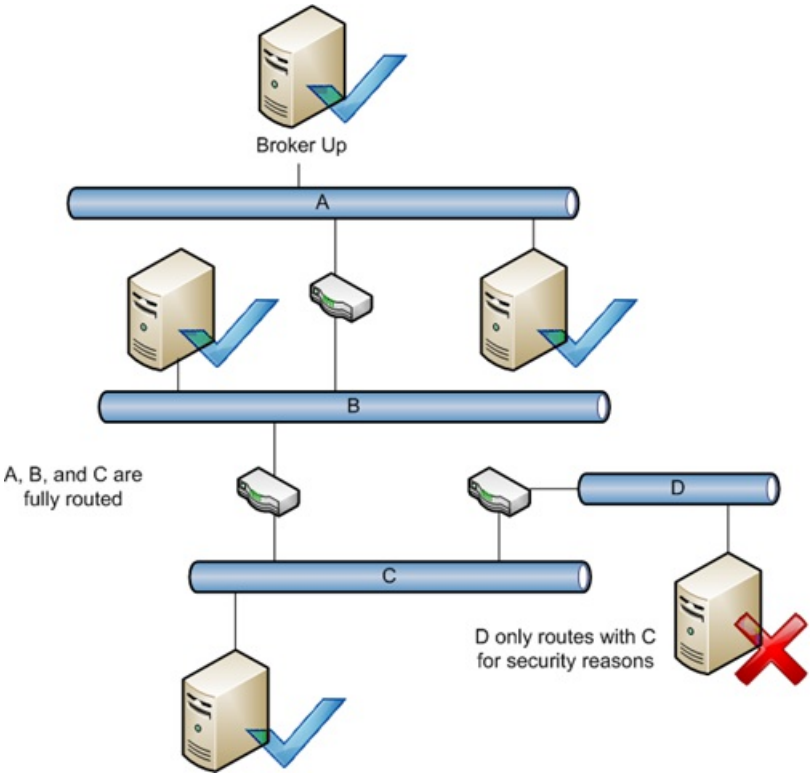
- Use of a broker mechanism

> Having a central 'traffic cop' allows one server to be aware of all the other servers and which files they have locked by users. Unfortunately this also means that there is often a single point of failure in the distributed locking system.




- Requirement for a fully routed network

> Since a central broker must be able to talk to all servers participating in file replication, this removes the ability to handle complex network topologies. Ring topologies and multi hub-and-spoke topologies are not usually possible. In a non-fully routed network, some servers may not be able to directly contact each other or a broker, and can only talk to a partner who himself can talk to another server – and so on. This is fine in a multi-master environment, but not with a brokering mechanism.




- Are limited to a pair of servers

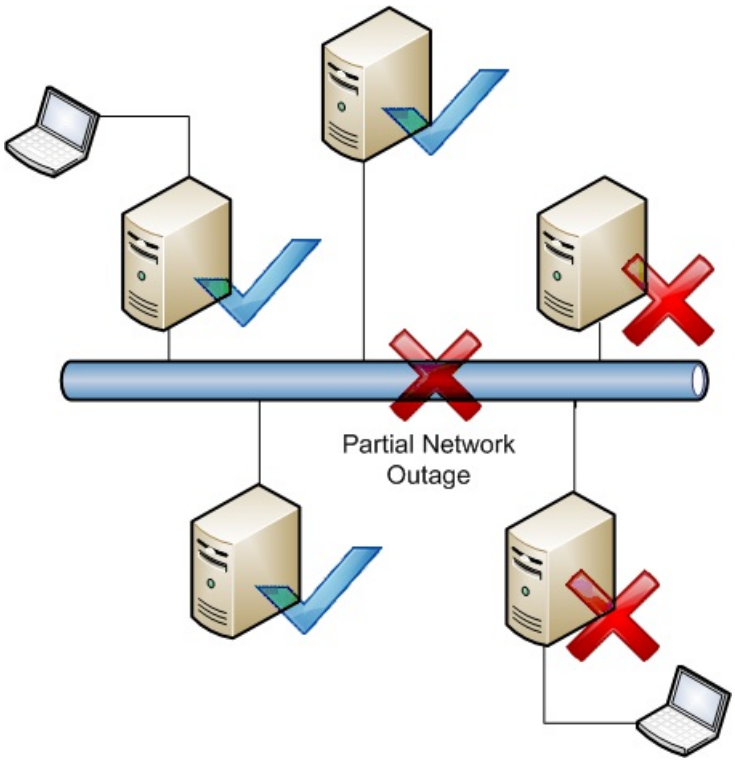
> Some solutions limit the topology to a pair of servers in order to simplify their distributed locking mechanism. For larger environments this is may not be feasible.

- Make use of agents on clients and servers
- Do not use multi-master replication
- Do not make use of MS clustering
- Make use of specialty appliances

** Note that I say typically! Please do not post death threats because you have a solution that does/does not implement one or more of those methods!*

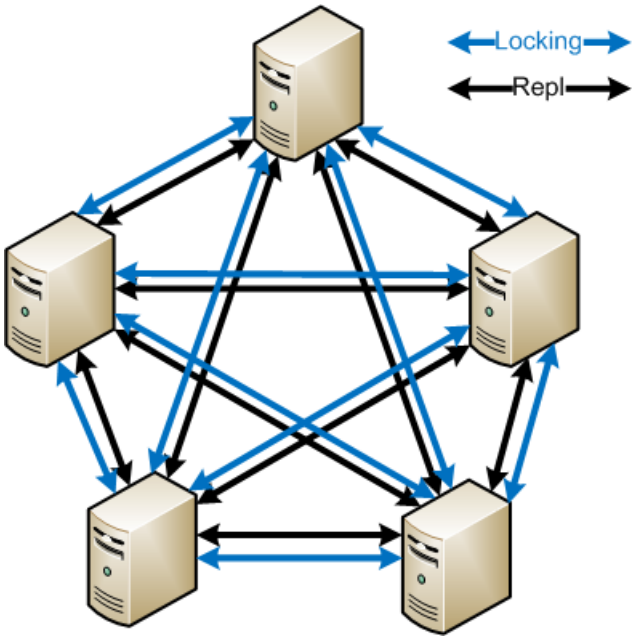
## Deeper Thoughts

As you think further about this issue, some fundamental issues start to crop up. For example, if we have four servers with data that can be modified by users in four sites, and the WAN connection to one of them goes offline, what do we do? The users can still access their individual servers – but should we let them? We don't want them to make changes that conflict, but we definitely want them to keep working and making our company money. If we arbitrarily block changes at that point, no users can work even though there may not actually be any conflicts happening! There's no way to tell the other servers that the file is in use and you're back at square one.




Then there's SMB itself and the error handling of reporting locks. We can't really change how SMB reports sharing violations as we'd break a ton of applications and clients wouldn't understand new extended error messages anyways. Applications like Word 2007 do some undercover trickery to figure out who is locking files, but the vast majority of applications don't know who has a file in use (or even that SMB exists. Really.). So when a user gets the message 'This file is in use' it's not particularly actionable – should they all call the help desk? Does the help desk have access to all the file servers to see which users are accessing files? Messy.

Since we want multi-master for high availability, a broker system is less desirable; we might need to have something running on all servers that allows them all to communicate even through non-fully routed networks. This will require very complex synchronization techniques. It will add some overhead on the network (although probably not much) and it will need to be lightning fast to make sure that we are not holding up the user in their work; it needs to outrun file replication itself - in fact, it might need to actually be tied to replication somehow. It will also have to account for server outages that are network related and not server crashes, somehow.




And then we're back to special client software for this scenario that better understands the locks and can give the user some useful info ("Go call Susie in accounting and tell her to release that doc", "Sorry, the file locking topology is broken and your administrator is preventing you from opening this file until it's fixed", etc). Getting this to play

nicely with the millions of applications running in Windows will definitely be interesting. There are plenty of OS's that would not be supported or get the software – Windows 2000 is out of mainstream support and XP soon will be. Linux and Mac clients wouldn't have this software until they felt it was important, so the customer would have to hope their vendors made something analogous.

## More inforamtion

Right now the easiest way to control this situation in DFSR is to use DFS Namespaces to guide users to predictable locations, with a consistent namespace. By correctly configuring your DFSN site topology and server links, you force users to all share the same local server and only allow them to access remote computers when their 'main' server is down. For most environments, this works quite well. Alternative to DFSR, SharePoint is an option because of its check-out/check-in system. BranchCache (coming in Windows Server 2008 R2 and Windows 7) may be an option for you as it is designed for easing the reading of files in a branch scenario, but in the end the authoritative data will still live on one server only – more on this here. And again, those vendors have their solutions.

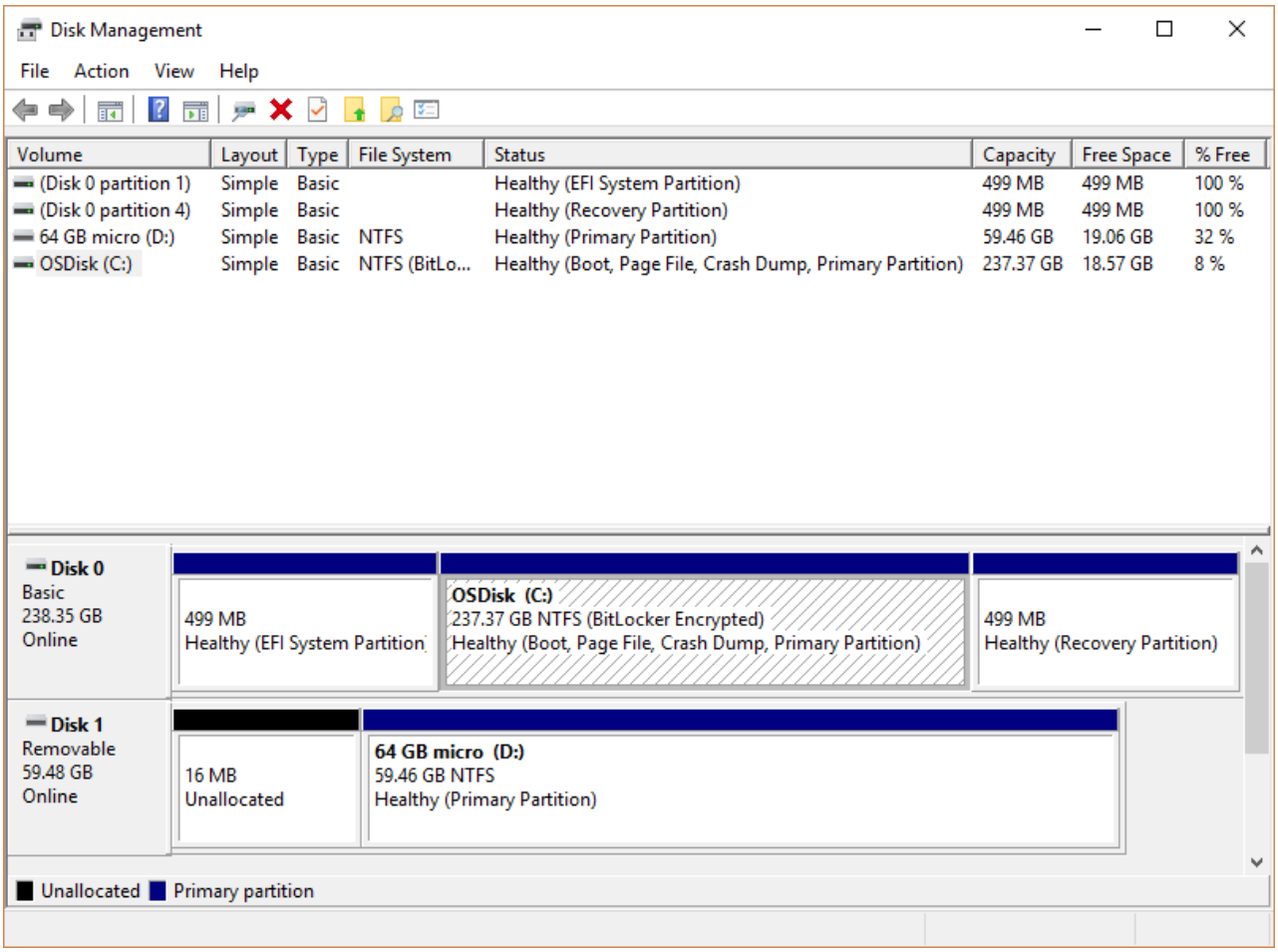
# Overview of Disk Management

11/2/2020 • 2 minutes to read • Edit Online

**Applies To:** Windows 10, Windows 8.1, Windows 7, Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Here are some of the things Disk Management is good for:

- To setup a new drive, see Initializing a new drive.
- To extend a volume into space that's not already part of a volume on the same drive, see Extend a basic volume.
- To shrink a partition, usually so that you can extend a neighboring partition, see Shrink a basic volume.
- To change a drive letter or assign a new drive letter, see Change a drive letter.




**TIP**

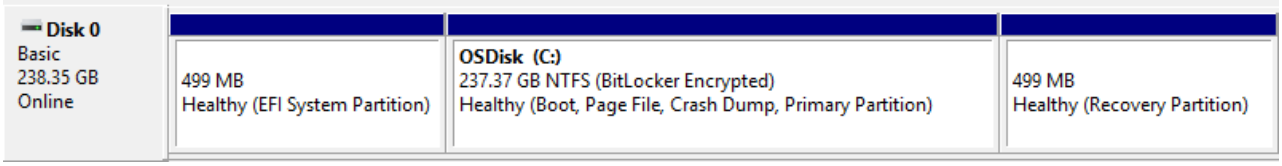
If you get an error or something doesn't work when following these procedures, take a peek at the Troubleshooting Disk Management topic. If that doesn't help - don't panic! There's a ton of info on the Microsoft community site - try searching the Files, folders, and storage section, and if you still need help, post a question there and Microsoft or other members of the community will try to help. If you have feedback on how to improve these topics, we'd love to hear from you! Just answer the *Is this page helpful?* prompt, and leave any comments there or in the public comments thread at the bottom of this topic.

Here are some common tasks you might want to do but that use other tools in Windows:

- To free up disk space, see Free up drive space in Windows 10.
- To defragment your drives, see Defragment your Windows 10 PC.
- To take multiple hard drives and pool them together, similar to a RAID, see Storage Spaces.

## About those extra recovery partitions

In case you're curious (we've read your comments!), Windows typically includes three partitions on your main drive (usually the C:\ drive):




- **EFI system partition** - This is used by modern PCs to start (boot) your PC and your operating system.
- **Windows operating system drive (C:)** - This is where Windows is installed, and usually where you put the rest of your apps and files.
- **Recovery partition** - This is where special tools are stored to help you recover Windows in case it has trouble starting or runs into other serious issues.

Although Disk Management might show the EFI system partition and the recovery partition as 100% free, it's lying. These partitions are generally pretty full with really important files your PC needs to operate properly. It's best to just leave them alone to do their jobs starting your PC and helping you recover from problems.

## Additional References

- Manage disks
- Manage basic volumes
- Troubleshooting Disk Management
- Recovery options in Windows 10
- Find lost files after the update to Windows 10
- Back up and restore your files
- Create a recovery drive
- Create a system restore point
- Find my BitLocker recovery key

# Overview of file sharing using the SMB 3 protocol in Windows Server

11/2/2020 • 11 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes the SMB 3 feature in Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012—practical uses for the feature, the most significant new or updated functionality in this version compared to previous versions, and the hardware requirements. SMB is also a fabric protocol used by software-defined data center (SDDC) solutions such as Storage Spaces Direct, Storage Replica, and others. SMB version 3.0 was introduced with Windows Server 2012 and has been incrementally improved in subsequent releases.

## Feature description

The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Using the SMB protocol, an application (or the user of an application) can access files or other resources at a remote server. This allows applications to read, create, and update files on the remote server. SMB can also communicate with any server program that is set up to receive an SMB client request. SMB is a fabric protocol that is used by Software-defined Data Center (SDDC) computing technologies, such as Storage Spaces Direct, Storage Replica. For more information, see Windows Server software-defined datacenter.

## Practical applications

This section discusses some new practical ways to use the new SMB 3.0 protocol.

- **File storage for virtualization (Hyper-V™ over SMB)**. Hyper-V can store virtual machine files, such as configuration, Virtual hard disk (VHD) files, and snapshots, in file shares over the SMB 3.0 protocol. This can be used for both stand-alone file servers and clustered file servers that use Hyper-V together with shared file storage for the cluster.
- **Microsoft SQL Server over SMB**. SQL Server can store user database files on SMB file shares. Currently, this is supported with SQL Server 2008 R2 for stand-alone SQL servers. Upcoming versions of SQL Server will add support for clustered SQL servers and system databases.
- **Traditional storage for end-user data**. The SMB 3.0 protocol provides enhancements to the Information Worker (or client) workloads. These enhancements include reducing the application latencies experienced by branch office users when accessing data over wide area networks (WAN) and protecting data from eavesdropping attacks.

## New and changed functionality

The following sections describe functionality that was added in SMB 3 and subsequent updates.

## Features added in Windows Server 2019 and Windows 10, version 1809

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| Ability to require write-through to disk on file shares that aren't continuously available | New | To provide some added assurance that writes to a file share make it all the way through the software and hardware stack to the physical disk prior to the write operation returning as completed, you can enable write-through on the file share using either the `NET USE /WRITETHROUGH` command or the `New-SMBMapping -UseWriteThrough` PowerShell cmdlet. There's some amount of performance hit to using write-through; see the blog post Controlling write-through behaviors in SMB for further discussion. |

## Features added in Windows Server, version 1709, and Windows 10, version 1709

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| Guest access to file shares is disabled | New | The SMB client no longer allows the following actions: Guest account access to a remote server; Fallback to the Guest account after invalid credentials are provided. For details, see Guest access in SMB2 disabled by default in Windows. |
| SMB global mapping | New | Maps a remote SMB share to a drive letter that is accessible to all users on the local host, including containers. This is required to enable container I/O on the data volume to traverse the remote mount point. Be aware that when using SMB global mapping for containers, all users on the container host can access the remote share. Any application running on the container host also have access to the mapped remote share. For details, see Container Storage Support with Cluster Shared Volumes (CSV), Storage Spaces Direct, SMB Global Mapping. |
| SMB dialect control | New | You can now set registry values to control the minimum SMB version (dialect) and maximum SMB version used. For details, see Controlling SMB Dialects. |

## Features added in SMB 3.11 with Windows Server 2016 and Windows 10, version 1607

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| SMB Encryption | Updated | SMB 3.1.1 encryption with Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) is faster than SMB Signing or previous SMB encryption using AES-CCM. |
| Directory Caching | New | SMB 3.1.1 includes enhancements to directory caching. Windows clients can now cache much larger directories, approximately 500K entries. Windows clients will attempt directory queries with 1 MB buffers to reduce round trips and improve performance. |
| Pre-Authentication Integrity | New | In SMB 3.1.1, pre-authentication integrity provides improved protection from a man-in-the-middle attacker tampering with SMB's connection establishment and authentication messages. For details, see SMB 3.1.1 Pre-authentication integrity in Windows 10. |
| SMB Encryption Improvements | New | SMB 3.1.1 offers a mechanism to negotiate the crypto algorithm per connection, with options for AES-128-CCM and AES-128-GCM. AES-128-GCM is the default for new Windows versions, while older versions will continue to use AES-128-CCM. |
| Rolling cluster upgrade support | New | Enables rolling cluster upgrades by letting SMB appear to support different max versions of SMB for clusters in the process of being upgraded. For more details on letting SMB communicate using different versions (dialects) of the protocol, see the blog post Controlling SMB Dialects. |
| SMB Direct client support in Windows 10 | New | Windows 10 Enterprise, Windows 10 Education, and Windows 10 Pro for Workstations now include SMB Direct client support. |
| Native support for FileNormalizedNameInformation API calls | New | Adds native support for querying the normalized name of a file. For details, see FileNormalizedNameInformation. |

For additional details, see the blog post What's new in SMB 3.1.1 in the Windows Server 2016 Technical Preview 2.

## Features added in SMB 3.02 with Windows Server 2012 R2 and Windows 8.1

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| Automatic rebalancing of Scale-Out File Server clients | New | Improves scalability and manageability for Scale-Out File Servers. SMB client connections are tracked per file share (instead of per server), and clients are then redirected to the cluster node with the best access to the volume used by the file share. This improves efficiency by reducing redirection traffic between file server nodes. Clients are redirected following an initial connection and when cluster storage is reconfigured. |
| Performance over WAN | Updated | Windows 8.1 and Windows 10 provide improved CopyFile SRV_COPYCHUNK over SMB support when you use File Explorer for remote copies from one location on a remote machine to another copy on the same server. You will copy only a small amount of metadata over the network (1/2KiB per 16MiB of file data is transmitted). This results in a significant performance improvement. This is an OS-level and File Explorer-level distinction for SMB. |
| SMB Direct | Updated | Improves performance for small I/O workloads by increasing efficiency when hosting workloads with small I/Os (such as an online transaction processing (OLTP) database in a virtual machine). These improvements are evident when using higher speed network interfaces, such as 40 Gbps Ethernet and 56 Gbps InfiniBand. |
| SMB bandwidth limits | New | You can now use Set-SmbBandwidthLimit to set bandwidth limits in three categories: VirtualMachine (Hyper-V over SMB traffic), LiveMigration (Hyper-V Live Migration traffic over SMB), or Default (all other types of SMB traffic). |

For more information on new and changed SMB functionality in Windows Server 2012 R2, see What's New in SMB in Windows Server.

## Features added in SMB 3.0 with Windows Server 2012 and Windows 8

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| SMB Transparent Failover | New | Enables administrators to perform hardware or software maintenance of nodes in a clustered file server without interrupting server applications storing data on these file shares. Also, if a hardware or software failure occurs on a cluster node, SMB clients transparently reconnect to another cluster node without interrupting server applications that are storing data on these file shares. |
| SMB Scale Out | New | Support for multiple SMB instances on a Scale-Out File Server. Using Cluster Shared Volumes (CSV) version 2, administrators can create file shares that provide simultaneous access to data files, with direct I/O, through all nodes in a file server cluster. This provides better utilization of network bandwidth and load balancing of the file server clients, and optimizes performance for server applications. |
| SMB Multichannel | New | Enables aggregation of network bandwidth and network fault tolerance if multiple paths are available between the SMB client and server. This enables server applications to take full advantage of all available network bandwidth and be resilient to a network failure.<br><br>SMB Multichannel in SMB 3 contributes to a substantial increase in performance compared to previous versions of SMB. |
| SMB Direct | New | Supports the use of network adapters that have RDMA capability and can function at full speed with very low latency, while using very little CPU. For workloads such as Hyper-V or Microsoft SQL Server, this enables a remote file server to resemble local storage.<br><br>SMB Direct in SMB 3 contributes to a substantial increase in performance compared to previous versions of SMB. |
| Performance Counters for server applications | New | The new SMB performance counters provide detailed, per-share information about throughput, latency, and I/O per second (IOPS), allowing administrators to analyze the performance of SMB file shares where their data is stored. These counters are specifically designed for server applications, such as Hyper-V and SQL Server, which store files on remote file shares. |

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| Performance optimizations | Updated | Both the SMB client and server have been optimized for small random read/write I/O, which is common in server applications such as SQL Server OLTP. In addition, large Maximum Transmission Unit (MTU) is turned on by default, which significantly enhances performance in large sequential transfers, such as SQL Server data warehouse, database backup or restore, deploying or copying virtual hard disks. |
| SMB-specific Windows PowerShell cmdlets | New | With Windows PowerShell cmdlets for SMB, an administrator can manage file shares on the file server, end to end, from the command line. |
| SMB Encryption | New | Provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on untrusted networks. Requires no new deployment costs, and no need for Internet Protocol security (IPsec), specialized hardware, or WAN accelerators. It may be configured on a per share basis, or for the entire file server, and may be enabled for a variety of scenarios where data traverses untrusted networks. |
| SMB Directory Leasing | New | Improves application response times in branch offices. With the use of directory leases, roundtrips from client to server are reduced since metadata is retrieved from a longer living directory cache. Cache coherency is maintained because clients are notified when directory information on the server changes. Directory leases work with scenarios for HomeFolder (read/write with no sharing) and Publication (read-only with sharing). |

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | SUMMARY |
| --- | --- | --- |
| Performance over WAN | New | Directory opportunistic locks (oplocks) and oplock leases were introduced in SMB 3.0. For typical office/client workloads, oplocks/leases are shown to reduce network round trips by approximately 15%.<br><br>In SMB 3, the Windows implementation of SMB has been refined to improve the caching behavior on the client as well as the ability to push higher throughputs.<br><br>SMB 3 features improvements to the CopyFile() API, as well as to associated tools such as Robocopy, to push significantly more data over the network. |
| Secure dialect negotiation | New | Helps protect against man-in-the-middle attempt to downgrade dialect negotiation. The idea is to prevent an eavesdropper from downgrading the initially negotiated dialect and capabilities between the client and the server. For details, see SMB3 Secure Dialect Negotiation. Note that this has been superceded by the SMB 3.1.1 Pre-authentication integrity in Windows 10 feature in SMB 3.1.1. |

## Hardware requirements

SMB Transparent Failover has the following requirements:

- A failover cluster running Windows Server 2012 or Windows Server 2016 with at least two nodes configured. The cluster must pass the cluster validation tests included in the validation wizard.
- File shares must be created with the Continuous Availability (CA) property, which is the default.
- File shares must be created on CSV volume paths to attain SMB Scale-Out.
- Client computers must be running Windows® 8 or Windows Server 2012, both of which include the updated SMB client that supports continuous availability.

> **NOTE**
> Down-level clients can connect to file shares that have the CA property, but transparent failover will not be supported for these clients.

SMB Multichannel has the following requirements:

- At least two computers running Windows Server 2012 are required. No extra features need to be installed—the technology is on by default.
- For information on recommended network configurations, see the See Also section at the end of this overview topic.

SMB Direct has the following requirements:

- At least two computers running Windows Server 2012 are required. No extra features need to be installed—the

technology is on by default.

- Network adapters with RDMA capability are required. Currently, these adapters are available in three different types: iWARP, Infiniband, or RoCE (RDMA over Converged Ethernet).

## More information

The following list provides additional resources on the web about SMB and related technologies in Windows Server 2012 R2, Windows Server 2012, and Windows Server 2016.

- Storage in Windows Server
- Scale-Out File Server for Application Data
- Improve Performance of a File Server with SMB Direct
- Deploy Hyper-V over SMB
- Deploy SMB Multichannel
- Deploying Fast and Efficient File Servers for Server Applications
- SMB: Troubleshooting Guide

# SMB Direct

11/2/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2012 R2, Windows Server 2012, Windows Server 2016

Windows Server 2012 R2, Windows Server 2012, and Windows Server 2016 include a feature called SMB Direct, which supports the use of network adapters that have Remote Direct Memory Access (RDMA) capability. Network adapters that have RDMA can function at full speed with very low latency, while using very little CPU. For workloads such as Hyper-V or Microsoft SQL Server, this enables a remote file server to resemble local storage. SMB Direct includes:

- Increased throughput: Leverages the full throughput of high speed networks where the network adapters coordinate the transfer of large amounts of data at line speed.
- Low latency: Provides extremely fast responses to network requests, and, as a result, makes remote file storage feel as if it is directly attached block storage.
- Low CPU utilization: Uses fewer CPU cycles when transferring data over the network, which leaves more power available to server applications.

SMB Direct is automatically configured by Windows Server 2012 R2 and Windows Server 2012.

## SMB Multichannel and SMB Direct

SMB Multichannel is the feature responsible for detecting the RDMA capabilities of network adapters to enable SMB Direct. Without SMB Multichannel, SMB uses regular TCP/IP with the RDMA-capable network adapters (all network adapters provide a TCP/IP stack along with the new RDMA stack).

With SMB Multichannel, SMB detects whether a network adapter has the RDMA capability, and then creates multiple RDMA connections for that single session (two per interface). This allows SMB to use the high throughput, low latency, and low CPU utilization offered by RDMA-capable network adapters. It also offers fault tolerance if you are using multiple RDMA interfaces.

> **NOTE**
> You should not team RDMA-capable network adapters if you intend to use the RDMA capability of the network adapters. When teamed, the network adapters will not support RDMA. After at least one RDMA network connection is created, the TCP/IP connection used for the original protocol negotiation is no longer used. However, the TCP/IP connection is retained in case the RDMA network connections fail.

## Requirements

SMB Direct requires the following:

- At least two computers running Windows Server 2012 R2 or Windows Server 2012
- One or more network adapters with RDMA capability.

**Considerations when using SMB Direct**

- You can use SMB Direct in a failover cluster; however, you need to make sure that the cluster networks used for client access are adequate for SMB Direct. Failover clustering supports using multiple networks for client access, along with network adapters that are RSS (Receive Side Scaling)-capable and RDMA-capable.
- You can use SMB Direct on the Hyper-V management operating system to support using Hyper-V over SMB,

and to provide storage to a virtual machine that uses the Hyper-V storage stack. However, RDMA-capable network adapters are not directly exposed to a Hyper-V client. If you connect an RDMA-capable network adapter to a virtual switch, the virtual network adapters from the switch will not be RDMA-capable.

- If you disable SMB Multichannel, SMB Direct is also disabled. Since SMB Multichannel detects network adapter capabilities and determines whether a network adapter is RDMA-capable, SMB Direct cannot be used by the client if SMB Multichannel is disabled.
- SMB Direct is not supported on Windows RT. SMB Direct requires support for RDMA-capable network adapters, which is available only on Windows Server 2012 R2 and Windows Server 2012.
- SMB Direct is not supported on down-level versions of Windows Server. It is supported only on Windows Server 2012 R2 and Windows Server 2012.

## Enabling and disabling SMB Direct

SMB Direct is enabled by default when Windows Server 2012 R2 or Windows Server 2012 is installed. The SMB client automatically detects and uses multiple network connections if an appropriate configuration is identified.

### Disable SMB Direct

Typically, you will not need to disable SMB Direct, however, you can disable it by running one of the following Windows PowerShell scripts.

To disable RDMA for a specific interface, type:

```
Disable-NetAdapterRdma <name>
```

To disable RDMA for all interfaces, type:

```
Set-NetOffloadGlobalSetting -NetworkDirect Disabled
```

When you disable RDMA on either the client or the server, the systems cannot use it. *Network Direct* is the internal name for Windows Server 2012 R2 and Windows Server 2012 basic networking support for RDMA interfaces.

### Re-enable SMB Direct

After disabling RDMA, you can re-enable it by running one of the following Windows PowerShell scripts.

To re-enable RDMA for a specific interface, type:

```
Enable-NetAdapterRDMA <name>
```

To re-enable RDMA for all interfaces, type:

```
Set-NetOffloadGlobalSetting -NetworkDirect Enabled
```

You need to enable RDMA on both the client and the server to start using it again.

## Test performance of SMB Direct

You can test how the performance is working by using one of the following procedures.

### Compare a file copy with and without using SMB Direct

Here's how to measure the increased throughput of SMB Direct:

1. Configure SMB Direct

2. Measure the amount of time to run a large file copy using SMB Direct.
3. Disable RDMA on the network adapter, see Enabling and disabling SMB Direct.
4. Measure the amount of time to run a large file copy without using SMB Direct.
5. Re-enable RDMA on the network adapter, and then compare the two results.
6. To avoid the impact of caching, you should do the following:
    a. Copy a large amount of data (more data than memory is capable of handling).
    b. Copy the data twice, with the first copy as practice and then timing the second copy.
    c. Restart both the server and the client before each test to make sure they operate under similar conditions.

**Fail one of multiple network adapters during a file copy with SMB Direct**

Here's how to confirm the failover capability of SMB Direct:

1. Ensure that SMB Direct is functioning in a multiple network adapter configuration.
2. Run a large file copy. While the copying is run, simulate a failure of one of the network paths by disconnecting one of the cables (or by disabling one of the network adapters).
3. Confirm that the file copying continues using one of the remaining network adapters, and that there are no file copy errors.

> **NOTE**
> To avoid failures of a workload that does not use SMB Direct, make sure there are no other workloads using the disconnected network path.

## More information

- Server Message Block overview
- Increasing Server, Storage, and Network Availability: Scenario Overview
- Deploy Hyper-V over SMB

# SMB security enhancements

11/2/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2012 R2, Windows Server 2012, Windows Server 2016

This topic explains the SMB security enhancements in Windows Server 2012 R2, Windows Server 2012, and Windows Server 2016.

## SMB Encryption

SMB Encryption provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on untrusted networks. You can deploy SMB Encryption with minimal effort, but it may require small additional costs for specialized hardware or software. It has no requirements for Internet Protocol security (IPsec) or WAN accelerators. SMB Encryption can be configured on a per share basis or for the entire file server, and it can be enabled for a variety of scenarios where data traverses untrusted networks.

> **NOTE**
> SMB Encryption does not cover security at rest, which is typically handled by BitLocker Drive Encryption.

SMB Encryption should be considered for any scenario in which sensitive data needs to be protected from man-in-the-middle attacks. Possible scenarios include:

- An information worker's sensitive data is moved by using the SMB protocol. SMB Encryption offers an end-to-end privacy and integrity assurance between the file server and the client, regardless of the networks traversed, such as wide area network (WAN) connections that are maintained by non-Microsoft providers.
- SMB 3.0 enables file servers to provide continuously available storage for server applications, such as SQL Server or Hyper-V. Enabling SMB Encryption provides an opportunity to protect that information from snooping attacks. SMB Encryption is simpler to use than the dedicated hardware solutions that are required for most storage area networks (SANs).

> **IMPORTANT**
> You should note that there is a notable performance operating cost with any end-to-end encryption protection when compared to non-encrypted.

## Enable SMB Encryption

You can enable SMB Encryption for the entire file server or only for specific file shares. Use one of the following procedures to enable SMB Encryption:

### Enable SMB Encryption with Windows PowerShell

1. To enable SMB Encryption for an individual file share, type the following script on the server:

```
Set-SmbShare –Name <sharename> -EncryptData $true
```

2. To enable SMB Encryption for the entire file server, type the following script on the server:

```
Set-SmbServerConfiguration –EncryptData $true
```

3. To create a new SMB file share with SMB Encryption enabled, type the following script:

```
New-SmbShare –Name <sharename> -Path <pathname> –EncryptData $true
```

**Enable SMB Encryption with Server Manager**

1. In Server Manager, open **File and Storage Services**.
2. Select **Shares** to open the Shares management page.
3. Right-click the share on which you want to enable SMB Encryption, and then select **Properties**.
4. On the **Settings** page of the share, select **Encrypt data access**. Remote file access to this share is encrypted.

**Considerations for deploying SMB Encryption**

By default, when SMB Encryption is enabled for a file share or server, only SMB 3.0 clients are allowed to access the specified file shares. This enforces the administrator's intent of safeguarding the data for all clients that access the shares. However, in some circumstances, an administrator may want to allow unencrypted access for clients that do not support SMB 3.0 (for example, during a transition period when mixed client operating system versions are being used). To allow unencrypted access for clients that do not support SMB 3.0, type the following script in Windows PowerShell:

```
Set-SmbServerConfiguration –RejectUnencryptedAccess $false
```

The secure dialect negotiation capability described in the next section prevents a man-in-the-middle attack from downgrading a connection from SMB 3.0 to SMB 2.0 (which would use unencrypted access). However, it does not prevent a downgrade to SMB 1.0, which would also result in unencrypted access. To guarantee that SMB 3.0 clients always use SMB Encryption to access encrypted shares, you must disable the SMB 1.0 server. (For instructions, see the section Disabling SMB 1.0.) If the **–RejectUnencryptedAccess** setting is left at its default setting of **$true**, only encryption-capable SMB 3.0 clients are allowed to access the file shares (SMB 1.0 clients will also be rejected).

**NOTE**

- SMB Encryption uses the Advanced Encryption Standard (AES)-CCM algorithm to encrypt and decrypt the data. AES-CCM also provides data integrity validation (signing) for encrypted file shares, regardless of the SMB signing settings. If you want to enable SMB signing without encryption, you can continue to do this. For more information, see The Basics of SMB Signing.
- You may encounter issues when you attempt to access the file share or server if your organization uses wide area network (WAN) acceleration appliances.
- With a default configuration (where there is no unencrypted access allowed to encrypted file shares), if clients that do not support SMB 3.0 attempt to access an encrypted file share, Event ID 1003 is logged to the Microsoft-Windows-SmbServer/Operational event log, and the client will receive an **Access denied** error message.
- SMB Encryption and the Encrypting File System (EFS) in the NTFS file system are unrelated, and SMB Encryption does not require or depend on using EFS.
- SMB Encryption and the BitLocker Drive Encryption are unrelated, and SMB Encryption does not require or depend on using BitLocker Drive Encryption.

## Secure dialect negotiation

SMB 3.0 is capable of detecting man-in-the-middle attacks that attempt to downgrade the SMB 2.0 or SMB 3.0 protocol or the capabilities that the client and server negotiate. When such an attack is detected by the client or the server, the connection is disconnected and event ID 1005 is logged in the Microsoft-Windows-

SmbServer/Operational event log. Secure dialect negotiation cannot detect or prevent downgrades from SMB 2.0 or 3.0 to SMB 1.0. Because of this, and to take advantage of the full capabilities of SMB Encryption, we strongly recommend that you disable the SMB 1.0 server. For more information, see Disabling SMB 1.0.

The secure dialect negotiation capability that is described in the next section prevents a man-in-the-middle attack from downgrading a connection from SMB 3 to SMB 2 (which would use unencrypted access); however, it does not prevent downgrades to SMB 1, which would also result in unencrypted access. For more information on potential issues with earlier non-Windows implementations of SMB, see the Microsoft Knowledge Base.

## New signing algorithm

SMB 3.0 uses a more recent encryption algorithm for signing: Advanced Encryption Standard (AES)-cipher-based message authentication code (CMAC). SMB 2.0 used the older HMAC-SHA256 encryption algorithm. AES-CMAC and AES-CCM can significantly accelerate data encryption on most modern CPUs that have AES instruction support. For more information, see The Basics of SMB Signing.

## Disabling SMB 1.0

The legacy computer browser service and Remote Administration Protocol features in SMB 1.0 are now separate, and they can be eliminated. These features are still enabled by default, but if you do not have older SMB clients, such as computers running Windows Server 2003 or Windows XP, you can remove the SMB 1.0 features to increase security and potentially reduce patching.

> **NOTE**
> SMB 2.0 was introduced in Windows Server 2008 and Windows Vista. Older clients, such as computers running Windows Server 2003 or Windows XP, do not support SMB 2.0; and therefore, they will not be able to access file shares or print shares if the SMB 1.0 server is disabled. In addition, some non-Microsoft SMB clients may not be able to access SMB 2.0 file shares or print shares (for example, printers with "scan-to-share" functionality).

Before you start disabling SMB 1.0, you'll need to find out if your SMB clients are currently connected to the server running SMB 1.0. To do this, enter the following cmdlet in Windows PowerShell:

```
Get-SmbSession | Select Dialect,ClientComputerName,ClientUserName | ? Dialect -lt 2
```

> **NOTE**
> You should run this script repeatedly over the course of a week (multiple times each day) to build an audit trail. You could also run this as a scheduled task.

To disable SMB 1.0, enter the following script in Windows PowerShell:

```
Set-SmbServerConfiguration –EnableSMB1Protocol $false
```

> **NOTE**
> If an SMB client connection is denied because the server running SMB 1.0 has been disabled, event ID 1001 will be logged in the Microsoft-Windows-SmbServer/Operational event log.

## More information

Here are some additional resources about SMB and related technologies in Windows Server 2012.

- Server Message Block
- Storage in Windows Server
- Scale-Out File Server for Application Data

# SMB: File and printer sharing ports should be open

12/16/2020 • 2 minutes to read • Edit Online

Updated: February 2, 2011

Applies To: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012, Windows Server 2008 R2

*This topic is intended to address a specific issue identified by a Best Practices Analyzer scan. You should apply the information in this topic only to computers that have had the File Services Best Practices Analyzer run against them and are experiencing the issue addressed by this topic. For more information about best practices and scans, see* Best Practices Analyzer.

| | |
|---|---|
| **Operating System** | Windows Server |
| **Product/Feature** | File Services |
| **Severity** | Error |
| **Category** | Configuration |

## Issue

> *The firewall ports necessary for file and printer sharing are not open (ports 445 and 139).*

## Impact

> *Computers will not be able to access shared folders and other Server Message Block (SMB)-based network services on this server.*

## Resolution

> *Enable File and Printer Sharing to communicate through the computer's firewall.*

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure.

## To open the firewall ports to enable file and printer sharing

1. Open Control Panel, click **System and Security**, and then click **Windows Firewall**.
2. In the left pane, click **Advanced settings**, and in the console tree, click **Inbound Rules**.
3. Under **Inbound Rules**, locate the rules **File and Printer Sharing (NB-Session-In)** and **File and Printer Sharing (SMB-In)**.
4. For each rule, right-click the rule, and then click **Enable Rule**.

# Additional references

Understanding Shared Folders and the Windows Firewall(https://technet.microsoft.com/library/cc731402.aspx)

# Network File System overview

12/16/2020 • 6 minutes to read • Edit Online

> Applies to: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes the Network File System role service and features included with the File and Storage Services server role in Windows Server. Network File System (NFS) provides a file sharing solution for enterprises that have heterogeneous environments that include both Windows and non-Windows computers.

## Feature description

Using the NFS protocol, you can transfer files between computers running Windows and other non-Windows operating systems, such as Linux or UNIX.

NFS in Windows Server includes Server for NFS and Client for NFS. A computer running Windows Server can use Server for NFS to act as a NFS file server for other non-Windows client computers. Client for NFS allows a Windows-based computer running Windows Server to access files stored on a non-Windows NFS server.

## Windows and Windows Server versions

Windows supports multiple versions ofthe NFS client and server, depending on operating system version and family.

| OPERATING SYSTEMS | NFS SERVER VERSIONS | NFS CLIENT VERSIONS |
|---|---|---|
| Windows 7, Windows 8.1, Windows 10 | N/A | NFSv2, NFSv3 |
| Windows Server 2008, Windows Server 2008 R2 | NFSv2, NFSv3 | NFSv2, NFSv3 |
| Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 | NFSv2, NFSv3, NFSv4.1 | NFSv2, NFSv3 |

## Practical applications

Here are some ways you can use NFS:

- Use a Windows NFS file server to provide multi-protocol access to the same file share over both SMB and NFS protocols from multi-platform clients.
- Deploy a Windows NFS file server in a predominantly non-Windows operating system environment to provide non-Windows client computers access to NFS file shares.
- Migrate applications from one operating system to another by storing the data on file shares accessible through both SMB and NFS protocols.

## New and changed functionality

New and changed functionality in Network File System includes support for the NFS version 4.1 and improved deployment and manageability. For information about functionality that is new or changed in Windows Server 2012, review the following table:

| FEATURE/FUNCTIONALITY | NEW OR UPDATED | DESCRIPTION |
| --- | --- | --- |
| NFS version 4.1 | New | Increased security, performance, and interoperability compared to NFS version 3. |
| NFS infrastructure | Updated | Improves deployment and manageability, and increases security. |
| NFS version 3 continuous availability | Updated | Improves continuous availability on NFS version 3 clients. |
| Deployment and manageability improvements | Updated | Enables you to easily deploy and manage NFS with new Windows PowerShell cmdlets and a new WMI provider. |

## NFS version 4.1

NFS version 4.1 implements all of the required aspects, in addition to some of the optional aspects, of RFC 5661:

- **Pseudo file system**, a file system that separates physical and logical namespace and is compatible with NFS version 3 and NFS version 2. An alias is provided for the exported file system, which is part of the pseudo file system.
- **Compound RPCs** combine relevant operations and reduce chattiness.
- **Sessions and session trunking** enables just one semantic and allows continuous availability and better performance while utilizing multiple networks between NFS 4.1 clients and the NFS Server.

## NFS infrastructure

Improvements to the overall NFS infrastructure in Windows Server 2012 are detailed below:

- The **Remote Procedure Call (RPC)/External Data Representation (XDR)** transport infrastructure, powered by the WinSock network protocol, is available for both Server for NFS and Client for NFS. This replaces Transport Device Interface (TDI), offers better support, and provides better scalability and Receive Side Scaling (RSS).
- The **RPC port multiplexer** feature is firewall-friendly (less ports to manage) and simplifies deployment of NFS.
- **Auto-tuned caches and thread pools** are resource management capabilities of the new RPC/XDR infrastructure that are dynamic, automatically tuning caches and thread pools based on workload. This completely removes the guesswork involved when tuning parameters, providing optimal performance as soon as NFS is deployed.
- **New Kerberos privacy implementation and authentication options** with the addition of Kerberos privacy (Krb5p) support along with the existing krb5 and krb5i authentication options.
- **Identity Mapping Windows PowerShell module** cmdlets make it easier to manage identity mapping, configure Active Directory Lightweight Directory Services (AD LDS), and set up UNIX and Linux passwd and flat files.
- **Volume mount point** lets you access volumes mounted under an NFS share with NFS version 4.1.
- The **Port Multiplexing** feature supports the RPC port multiplexer (port 2049), which is firewall-friendly and simplifies NFS deployment.

## NFS version 3 continuous availability

NFS version 3 clients can have fast and transparent planned failovers with more availability and reduced downtime. The failover process is faster for NFS version 3 clients because:

- The clustering infrastructure now allows one resource per network name instead of one resource per share, which significantly improves resources' failover time.
- Failover paths within an NFS server are tuned for better performance.
- Wildcard registration in an NFS server is no longer required, and the failovers are more fine-tuned.
- Network Status Monitor (NSM) notifications are sent out after a failover process, and clients no longer need to wait for TCP timeouts to reconnect to the failed over server.

Note that Server for NFS supports transparent failover only when manually initiated, typically during planned maintenance. If an unplanned failover occurs, NFS clients lose their connections. Server for NFS also doesn't have any integration with the Resume Key filter. This means that if a local app or SMB session attempts to access the same file that an NFS client is accessing immediately after a planned failover, the NFS client might lose its connections (transparent failover wouldn't succeed).

## Deployment and manageability improvements

Deploying and managing NFS has improved in the following ways:

- Over forty new Windows PowerShell cmdlets make it easier to configure and manage NFS file shares. For more information, see NFS Cmdlets in Windows PowerShell.
- Identity mapping is improved with a local flat file mapping store and new Windows PowerShell cmdlets for configuring identity mapping.
- The Server Manager graphical user interface is easier to use.
- The new WMI version 2 provider is available for easier management.
- The RPC port multiplexer (port 2049) is firewall-friendly and simplifies deployment of NFS.

## Server Manager information

In Server Manager - or the newer Windows Admin Center - use the Add Roles and Features Wizard to add the Server for NFS role service (under the File and iSCSI Services role). For general information about installing features, see Install or Uninstall Roles, Role Services, or Features. Server for NFS tools include the Services for Network File System MMC snap-in to manage the Server for NFS and Client for NFS components. Using the snap-in, you can manage the Server for NFS components installed on the computer. Server for NFS also contains several Windows command-line administration tools:

- **Mount** mounts a remote NFS share (also known as an export) locally and maps it to a local drive letter on the Windows client computer.
- **Nfsadmin** manages configuration settings of the Server for NFS and Client for NFS components.
- **Nfsshare** configures NFS share settings for folders that are shared using Server for NFS.
- **Nfsstat** displays or resets statistics of calls received by Server for NFS.
- **Showmount** displays mounted file systems exported by Server for NFS.
- **Umount** removes NFS-mounted drives.

NFS in Windows Server 2012 introduces the NFS module for Windows PowerShell with several new cmdlets specifically for NFS. These cmdlets provide an easy way to automate NFS management tasks. For more information, see NFS cmdlets in Windows PowerShell.

## Additional information

The following table provides additional resources for evaluating NFS.

| CONTENT TYPE | REFERENCES |
| --- | --- |
| Deployment | Deploy Network File System |
| Operations | NFS cmdlets in Windows PowerShell |
| Related technologies | Storage in Windows Server |

# Deploy Network File System

11/2/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Network File System (NFS) provides a file sharing solution that lets you transfer files between computers running Windows Server and UNIX operating systems using the NFS protocol. This topic describe the steps you should follow to deploy NFS.

## What's new in Network File System

Here's what's changed for NFS in Windows Server 2012:

- **Support for NFS version 4.1**. This protocol version includes the following enhancements.
  - Navigating firewalls is easier, improving accessibility.
  - Supports the RPCSEC_GSS protocol, providing stronger security and allowing clients and servers to negotiate security.
  - Supports UNIX and Windows file semantics.
  - Takes advantage of clustered file server deployments.
  - Supports WAN-friendly compound procedures.
- **NFS module for Windows PowerShell**. The availability of built-in NFS cmdlets makes it easier to automate various operations. The cmdlet names are consistent with other Windows PowerShell cmdlets (using verbs such as "Get" and "Set"), making it easier for users familiar with Windows PowerShell to learn to use new cmdlets.
- **NFS management improvements**. A new centralized UI-based management console simplifies configuration and management of SMB and NFS shares, quotas, file screens and classification, in addition to managing clustered file servers.
- **Identity Mapping improvements**. New UI support and task-based Windows PowerShell cmdlets for configuring identity mapping, which allows administrators to quickly configure an identity mapping source, and then create individual mapped identities for users. Improvements make it easy for administrators to set up a share for multi-protocol access over both NFS and SMB.
- **Cluster resource model restructure**. This improvement brings consistency between the cluster resource model for the Windows NFS and SMB protocol servers and simplifies administration. For NFS servers that have many shares, the resource network and the number of WMI calls required fail over a volume containing a large number of NFS shares are reduced.
- **Integration with Resume Key Manager**. The Resume Key Manager is a component that tracks file server and file system state and enables the Windows SMB and NFS protocol servers to fail over without disrupting clients or server applications that store their data on the file server. This improvement is a key component of the continuous availability capability of the file server running Windows Server 2012.

## Scenarios for using Network File System

NFS supports a mixed environment of Windows-based and UNIX-based operating systems. The following deployment scenarios are examples of how you can deploy a continuously available Windows Server 2012 file server using NFS.

**Provision file shares in heterogeneous environments**

This scenario applies to organizations with heterogeneous environments that consist of both Windows and other operating systems, such as UNIX or Linux-based client computers. With this scenario, you can provide multi-protocol access to the same file share over both the SMB and NFS protocols. Typically, when you deploy a Windows file server in this scenario, you want to facilitate collaboration between users on Windows and UNIX-based computers. When a file share is configured, it is shared with both the SMB and NFS protocols, with Windows users accessing their files over the SMB protocol, and users on UNIX-based computers typically access their files over the NFS protocol.

For this scenario, you must have a valid identity mapping source configuration. Windows Server 2012 supports the following identity mapping stores:

- Mapping File
- Active Directory Domain Services (AD DS)
- RFC 2307-compliant LDAP stores such as Active Directory Lightweight Directory Services (AD LDS)
- User Name Mapping (UNM) server

**Provision file shares in UNIX-based environments**

In this scenario, Windows file servers are deployed in a predominantly UNIX-based environment to provide access to NFS file shares for UNIX-based client computers. An Unmapped UNIX User Access (UUUA) option was initially implemented for NFS shares in Windows Server 2008 R2 so that Windows servers can be used for storing NFS data without creating UNIX-to-Windows account mapping. UUUA allows administrators to quickly provision and deploy NFS without having to configure account mapping. When enabled for NFS, UUUA creates custom security identifiers (SIDs) to represent unmapped users. Mapped user accounts use standard Windows security identifiers (SIDs), and unmapped users use custom NFS SIDs.

# System requirements

Server for NFS can be installed on any version of Windows Server 2012. You can use NFS with UNIX-based computers that are running an NFS server or NFS client if these NFS server and client implementations comply with one of the following protocol specifications:

1. NFS Version 4.1 Protocol Specification (as defined in RFC 5661)
2. NFS Version 3 Protocol Specification (as defined in RFC 1813)
3. NFS Version 2 Protocol Specification (as defined in RFC 1094)

# Deploy NFS infrastructure

You need to deploy the following computers and connect them on a local area network (LAN):

- One or more computers running Windows Server 2012 on which you will install the two main Services for NFS components: Server for NFS and Client for NFS. You can install these components on the same computer or on different computers.
- One or more UNIX-based computers that are running NFS server and NFS client software. The UNIX-based computer that is running NFS server hosts an NFS file share or export, which is accessed by a computer that is running Windows Server 2012 as a client using Client for NFS. You can install NFS server and client software either in the same UNIX-based computer or on different UNIX-based computers, as desired.
- A domain controller running at the Windows Server 2008 R2 functional level. The domain controller provides user authentication information and mapping for the Windows environment.
- When a domain controller is not deployed, you can use a Network Information Service (NIS) server to provide user authentication information for the UNIX environment. Or, if you prefer, you can use Password and Group files that are stored on the computer that is running the User Name Mapping service.

**Install Network File System on the server with Server Manager**

1. From the Add Roles and Features Wizard, under Server Roles, select **File and Storage Services** if it has not already been installed.
2. Under **File and iSCSI Services**, select **File Server** and **Server for NFS**. Select **Add Features** to include selected NFS features.
3. Select **Install** to install the NFS components on the server.

**Install Network File System on the server with Windows PowerShell**

1. Start Windows PowerShell. Right-click the PowerShell icon on the taskbar, and select **Run as Administrator**.
2. Run the following Windows PowerShell commands:

```
Import-Module ServerManager
Add-WindowsFeature FS-NFS-Service
Import-Module NFS
```

## Configure NFS authentication

When using the NFS version 4.1 and NFS version 3.0 protocols, you have the following authentication and security options.

- RPCSEC_GSS
  - **Krb5**. Uses the Kerberos version 5 protocol to authenticate users before granting access to the file share.
  - **Krb5i**. Uses Kerberos version 5 protocol to authenticate with integrity checking (checksums), which verifies that the data has not been altered.
  - **Krb5p** Uses Kerberos version 5 protocol, which authenticates NFS traffic with encryption for privacy.
- AUTH_SYS

You can also choose not to use server authorization (AUTH_SYS), which gives you the option to enable unmapped user access. When using unmapped user access, you can specify to allow unmapped user access by UID / GID, which is the default, or allow anonymous access.

Instructions for configuring NFS authentication on discussed in the following section.

## Create an NFS file share

You can create an NFS file share using either Server Manager or Windows PowerShell NFS cmdlets.

**Create an NFS file share with Server Manager**

1. Log on to the server as a member of the local Administrators group.
2. Server Manager will start automatically. If it does not automatically start, select **Start**, type **servermanager.exe**, and then select **Server Manager**.
3. On the left, select **File and Storage Services**, and then select **Shares**.
4. Select **To create a file share, start the New Share Wizard**.
5. On the **Select Profile** page, select either **NFS Share – Quick** or **NFS Share - Advanced**, then select **Next**.
6. On the **Share Location** page, select a server and a volume, and select **Next**.
7. On the **Share Name** page, specify a name for the new share, and select **Next**.
8. On the **Authentication** page, specify the authentication method you want to use for this share.
9. On the **Share Permissions** page, select **Add**, and then specify the host, client group or netgroup you want to grant permission to the share.
10. In **Permissions**, configure the type of access control you want the users to have, and select **OK**.
11. On the **Confirmation** page, review your configuration, and select **Create** to create the NFS file share.

**Windows PowerShell equivalent commands**

The following Windows PowerShell cmdlet can also create an NFS file share (where `nfs1` is the name of the share and `C:\\shares\\nfsfolder` is the file path):

```
New-NfsShare -name nfs1 -Path C:\shares\nfsfolder
```

**Known issue**

NFS version 4.1 allows the file names to be created or copied using illegal characters. If you attempt to open the files with vi editor, it shows as being corrupt. You cannot save the file from vi, rename, move it or change permissions. Avoid using illegal characters.

# NTFS overview

11/2/2020 • 5 minutes to read • Edit Online

Applies to: Windows 10, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

NTFS—the primary file system for recent versions of Windows and Windows Server—provides a full set of features including security descriptors, encryption, disk quotas, and rich metadata, and can be used with Cluster Shared Volumes (CSV) to provide continuously available volumes that can be accessed simultaneously from multiple nodes of a failover cluster.

For additional feature information, see the Additional information section of this topic. To learn about the newer Resilient File System (ReFS), see Resilient File System (ReFS) overview.

## Increased reliability

NTFS uses its log file and checkpoint information to restore the consistency of the file system when the computer is restarted after a system failure. After a bad-sector error, NTFS dynamically remaps the cluster that contains the bad sector, allocates a new cluster for the data, marks the original cluster as bad, and no longer uses the old cluster. For example, after a server crash, NTFS can recover data by replaying its log files.

NTFS continuously monitors and corrects transient corruption issues in the background without taking the volume offline (this feature is known as self-healing NTFS, introduced in Windows Server 2008). For larger corruption issues, the Chkdsk utility, in Windows Server 2012 and later, scans and analyzes the drive while the volume is online, limiting time offline to the time required to restore data consistency on the volume. When NTFS is used with Cluster Shared Volumes, no downtime is required. For more information, see NTFS Health and Chkdsk.

## Increased security

- **Access Control List (ACL)-based security for files and folders**—NTFS allows you to set permissions on a file or folder, specify the groups and users whose access you want to restrict or allow, and select access type.
- **Support for BitLocker Drive Encryption**—BitLocker Drive Encryption provides additional security for critical system information and other data stored on NTFS volumes. Beginning in Windows Server 2012 R2 and Windows 8.1, BitLocker provides support for device encryption on x86 and x64-based computers with a Trusted Platform Module (TPM) that supports connected stand-by (previously available only on Windows RT devices). Device encryption helps protect data on Windows-based computers, and it helps block malicious users from accessing the system files they rely on to discover the user's password, or from accessing a drive by physically removing it from the PC and installing it on a different one. For more information, see What's new in BitLocker.

## Support for large volumes

NTFS can support volumes as large as 8 petabytes on Windows Server 2019 and newer and Windows 10, version 1709 and newer (older versions support up to 256 TB). Supported volume sizes are affected by the cluster size and the number of clusters. With ($2^{32} - 1$) clusters (the maximum number of clusters that NTFS supports), the following volume and file sizes are supported.

| CLUSTER SIZE | LARGEST VOLUME AND FILE |
| --- | --- |
| 4 KB (default size) | 16 TB |
| 8 KB | 32 TB |
| 16 KB | 64 TB |
| 32 KB | 128 TB |
| 64 KB (earlier max) | 256 TB |
| 128 KB | 512 TB |
| 256 KB | 1 PB |
| 512 KB | 2 PB |
| 1024 KB | 4 PB |
| 2048 KB (max size) | 8 PB |

Note that if you try to mount a volume with a cluster size larger than the supported maximum of the version of Windows you're using, you get the error STATUS_UNRECOGNIZED_VOLUME.

> **IMPORTANT**
> Services and apps might impose additional limits on file and volume sizes. For example, the volume size limit is 64 TB if you're using the Previous Versions feature or a backup app that makes use of Volume Shadow Copy Service (VSS) snapshots (and you're not using a SAN or RAID enclosure). However, you might need to use smaller volume sizes depending on your workload and the performance of your storage.

## Formatting requirements for large files

To allow proper extension of large .vhdx files, there are new recommendations for formatting volumes. When formatting volumes that will be used with Data Deduplication or will host very large files, such as .vhdx files larger than 1 TB, use the **Format-Volume** cmdlet in Windows PowerShell with the following parameters.

| PARAMETER | DESCRIPTION |
| --- | --- |
| -AllocationUnitSize 64KB | Sets a 64 KB NTFS allocation unit size. |
| -UseLargeFRS | Enables support for large file record segments (FRS). This is needed to increase the number of extents allowed per file on the volume. For large FRS records, the limit increases from about 1.5 million extents to about 6 million extents. |

For example, the following cmdlet formats drive D as an NTFS volume, with FRS enabled and an allocation unit size of 64 KB.

```
Format-Volume -DriveLetter D -FileSystem NTFS -AllocationUnitSize 64KB -UseLargeFRS
```

You also can use the **format** command. At a system command prompt, enter the following command, where **/L**

formats a large FRS volume and **/A:64k** sets a 64 KB allocation unit size:

```
format /L /A:64k
```

## Maximum file name and path

NTFS supports long file names and extended-length paths, with the following maximum values:

- **Support for long file names, with backward compatibility**—NTFS allows long file names, storing an 8.3 alias on disk (in Unicode) to provide compatibility with file systems that impose an 8.3 limit on file names and extensions. If needed (for performance reasons), you can selectively disable 8.3 aliasing on individual NTFS volumes in Windows Server 2008 R2, Windows 8, and more recent versions of the Windows operating system. In Windows Server 2008 R2 and later systems, short names are disabled by default when a volume is formatted using the operating system. For application compatibility, short names still are enabled on the system volume.
- **Support for extended-length paths**—Many Windows API functions have Unicode versions that allow an extended-length path of approximately 32,767 characters—beyond the 260-character path limit defined by the MAX_PATH setting. For detailed file name and path format requirements, and guidance for implementing extended-length paths, see Naming Files, Paths, and Namespaces.
- **Clustered storage**—When used in failover clusters, NTFS supports continuously available volumes that can be accessed by multiple cluster nodes simultaneously when used in conjunction with the Cluster Shared Volumes (CSV) file system. For more information, see Use Cluster Shared Volumes in a Failover Cluster.

## Flexible allocation of capacity

If the space on a volume is limited, NTFS provides the following ways to work with the storage capacity of a server:

- Use disk quotas to track and control disk space usage on NTFS volumes for individual users.
- Use file system compression to maximize the amount of data that can be stored.
- Increase the size of an NTFS volume by adding unallocated space from the same disk or from a different disk.
- Mount a volume at any empty folder on a local NTFS volume if you run out of drive letters or need to create additional space that is accessible from an existing folder.

## Additional information

- Cluster size recommendations for ReFS and NTFS
- Resilient File System (ReFS) overview
- What's New in NTFS (Windows Server 2012 R2)
- What's New in NTFS (Windows Server 2008 R2, Windows 7)
- NTFS Health and Chkdsk
- Self-Healing NTFS (introduced in Windows Server 2008)
- Transactional NTFS (introduced in Windows Server 2008)
- Storage in Windows Server

# Volume Shadow Copy Service

12/16/2020 • 24 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2, Windows Server 2008, Windows 10, Windows 8.1, Windows 8, Windows 7

Backing up and restoring critical business data can be very complex due to the following issues:

- The data usually needs to be backed up while the applications that produce the data are still running. This means that some of the data files might be open or they might be in an inconsistent state.
- If the data set is large, it can be difficult to back up all of it at one time.

Correctly performing backup and restore operations requires close coordination between the backup applications, the line-of-business applications that are being backed up, and the storage management hardware and software. The Volume Shadow Copy Service (VSS), which was introduced in Windows Server® 2003, facilitates the conversation between these components to allow them to work better together. When all the components support VSS, you can use them to back up your application data without taking the applications offline.

VSS coordinates the actions that are required to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up. The shadow copy can be used as-is, or it can be used in scenarios such as the following:

- You want to back up application data and system state information, including archiving data to another hard disk drive, to tape, or to other removable media.
- You are data mining.
- You are performing disk-to-disk backups.
- You need a fast recovery from data loss by restoring data to the original Logical Unit Number (LUN) or to an entirely new LUN that replaces an original LUN that failed.

Windows features and applications that use VSS include the following:

- Windows Server Backup (https://go.microsoft.com/fwlink/?LinkId=180891)
- Shadow Copies of Shared Folders (https://go.microsoft.com/fwlink/?LinkId=142874)
- System Center Data Protection Manager (https://go.microsoft.com/fwlink/?LinkId=180892)
- System Restore (https://go.microsoft.com/fwlink/?LinkId=180893)

## How Volume Shadow Copy Service Works

A complete VSS solution requires all of the following basic parts:

**VSS service** Part of the Windows operating system that ensures the other components can communicate with each other properly and work together.

**VSS requester** The software that requests the actual creation of shadow copies (or other high-level operations like importing or deleting them). Typically, this is the backup application. The Windows Server Backup utility and the System Center Data Protection Manager application are VSS requesters. Non-Microsoft® VSS requesters include nearly all backup software that runs on Windows.

**VSS writer** The component that guarantees we have a consistent data set to back up. This is typically provided as

part of a line-of-business application, such as SQL Server® or Exchange Server. VSS writers for various Windows components, such as the registry, are included with the Windows operating system. Non-Microsoft VSS writers are included with many applications for Windows that need to guarantee data consistency during back up.

**VSS provider** The component that creates and maintains the shadow copies. This can occur in the software or in the hardware. The Windows operating system includes a VSS provider that uses copy-on-write. If you use a storage area network (SAN), it is important that you install the VSS hardware provider for the SAN, if one is provided. A hardware provider offloads the task of creating and maintaining a shadow copy from the host operating system.

The following diagram illustrates how the VSS service coordinates with requesters, writers, and providers to create a shadow copy of a volume.

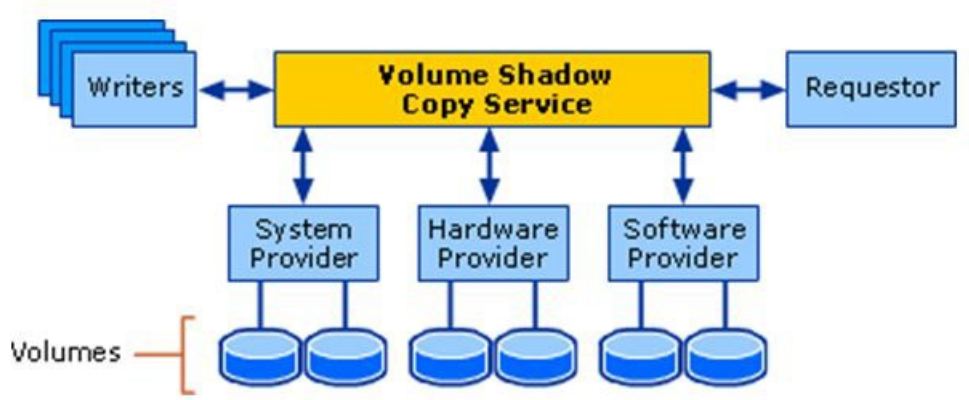



**Figure 1** Architectural diagram of Volume Shadow Copy Service

### How a Shadow Copy Is Created

This section puts the various roles of the requester, writer, and provider into context by listing the steps that need to be taken to create a shadow copy. The following diagram shows how the Volume Shadow Copy Service controls the overall coordination of the requester, writer, and provider.

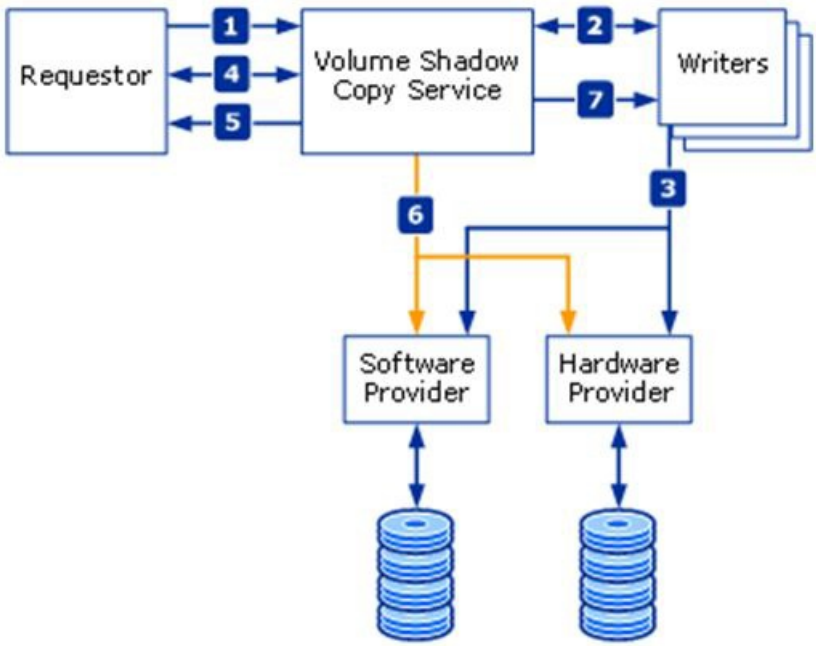



**Figure 2** Shadow copy creation process

To create a shadow copy, the requester, writer, and provider perform the following actions:

1. The requester asks the Volume Shadow Copy Service to enumerate the writers, gather the writer metadata, and prepare for shadow copy creation.
2. Each writer creates an XML description of the components and data stores that need to be backed up and

provides it to the Volume Shadow Copy Service. The writer also defines a restore method, which is used for all components. The Volume Shadow Copy Service provides the writer's description to the requester, which selects the components that will be backed up.

3. The Volume Shadow Copy Service notifies all the writers to prepare their data for making a shadow copy.
4. Each writer prepares the data as appropriate, such as completing all open transactions, rolling transaction logs, and flushing caches. When the data is ready to be shadow-copied, the writer notifies the Volume Shadow Copy Service.
5. The Volume Shadow Copy Service tells the writers to temporarily freeze application write I/O requests (read I/O requests are still possible) for the few seconds that are required to create the shadow copy of the volume or volumes. The application freeze is not allowed to take longer than 60 seconds. The Volume Shadow Copy Service flushes the file system buffers and then freezes the file system, which ensures that the file system metadata is recorded correctly and the data to be shadow-copied is written in a consistent order.
6. The Volume Shadow Copy Service tells the provider to create the shadow copy. The shadow copy creation period lasts no more than 10 seconds, during which all write I/O requests to the file system remain frozen.
7. The Volume Shadow Copy Service releases file system write I/O requests.
8. VSS tells the writers to thaw application write I/O requests. At this point applications are free to resume writing data to the disk that is being shadow-copied.

> **NOTE**
> The shadow copy creation can be aborted if the writers are kept in the freeze state for longer than 60 seconds or if the providers take longer than 10 seconds to commit the shadow copy.

9. The requester can retry the process (go back to step 1) or notify the administrator to retry at a later time.
10. If the shadow copy is successfully created, the Volume Shadow Copy Service returns the location information for the shadow copy to the requester. In some cases, the shadow copy can be temporarily made available as a read-write volume so that VSS and one or more applications can alter the contents of the shadow copy before the shadow copy is finished. After VSS and the applications make their alterations, the shadow copy is made read-only. This phase is called Auto-recovery, and it is used to undo any file-system or application transactions on the shadow copy volume that were not completed before the shadow copy was created.

**How the Provider Creates a Shadow Copy**

A hardware or software shadow copy provider uses one of the following methods for creating a shadow copy:

**Complete copy** This method makes a complete copy (called a "full copy" or "clone") of the original volume at a given point in time. This copy is read-only.

**Copy-on-write** This method does not copy the original volume. Instead, it makes a differential copy by copying all changes (completed write I/O requests) that are made to the volume after a given point in time.

**Redirect-on-write** This method does not copy the original volume, and it does not make any changes to the original volume after a given point in time. Instead, it makes a differential copy by redirecting all changes to a different volume.

## Complete copy

A complete copy is usually created by making a "split mirror" as follows:

1. The original volume and the shadow copy volume are a mirrored volume set.

2. The shadow copy volume is separated from the original volume. This breaks the mirror connection.

After the mirror connection is broken, the original volume and the shadow copy volume are independent. The original volume continues to accept all changes (write I/O requests), while the shadow copy volume remains an exact read-only copy of the original data at the time of the break.

**Copy-on-write method**

In the copy-on-write method, when a change to the original volume occurs (but before the write I/O request is completed), each block to be modified is read and then written to the volume's shadow copy storage area (also called its "diff area"). The shadow copy storage area can be on the same volume or a different volume. This preserves a copy of the data block on the original volume before the change overwrites it.

| TIME | SOURCE DATA (STATUS AND DATA) | SHADOW COPY (STATUS AND DATA) |
|---|---|---|
| T0 | Original data: 1 2 3 4 5 | No copy: — |
| T1 | Data changed in cache: 3 to 3' | Shadow copy created (differences only): 3 |
| T2 | Original data overwritten: 1 2 3' 4 5 | Differences and index stored on shadow copy: 3 |

**Table 1** The copy-on-write method of creating shadow copies

The copy-on-write method is a quick method for creating a shadow copy, because it copies only data that is changed. The copied blocks in the diff area can be combined with the changed data on the original volume to restore the volume to its state before any of the changes were made. If there are many changes, the copy-on-write method can become expensive.

**Redirect-on-write method**

In the redirect-on-write method, whenever the original volume receives a change (write I/O request), the change is not applied to the original volume. Instead, the change is written to another volume's shadow copy storage area.

| TIME | SOURCE DATA (STATUS AND DATA) | SHADOW COPY (STATUS AND DATA) |
|---|---|---|
| T0 | Original data: 1 2 3 4 5 | No copy: — |
| T1 | Data changed in cache: 3 to 3' | Shadow copy created (differences only): 3' |
| T2 | Original data unchanged: 1 2 3 4 5 | Differences and index stored on shadow copy: 3' |

**Table 2** The redirect-on-write method of creating shadow copies

Like the copy-on-write method, the redirect-on-write method is a quick method for creating a shadow copy, because it copies only changes to the data. The copied blocks in the diff area can be combined with the unchanged data on the original volume to create a complete, up-to-date copy of the data. If there are many read I/O requests, the redirect-on-write method can become expensive.

## Shadow Copy Providers

There are two types of shadow copy providers: hardware-based providers and software-based providers. There is also a system provider, which is a software provider that is built in to the Windows operating system.

**Hardware-based providers**

Hardware-based shadow copy providers act as an interface between the Volume Shadow Copy Service and the hardware level by working in conjunction with a hardware storage adapter or controller. The work of creating and maintaining the shadow copy is performed by the storage array.

Hardware providers always take the shadow copy of an entire LUN, but the Volume Shadow Copy Service only exposes the shadow copy of the volume or volumes that were requested.

A hardware-based shadow copy provider makes use of the Volume Shadow Copy Service functionality that defines the point in time, allows data synchronization, manages the shadow copy, and provides a common interface with backup applications. However, the Volume Shadow Copy Service does not specify the underlying mechanism by which the hardware-based provider produces and maintains shadow copies.

**Software-based providers**

Software-based shadow copy providers typically intercept and process read and write I/O requests in a software layer between the file system and the volume manager software.

These providers are implemented as a user-mode DLL component and at least one kernel-mode device driver, typically a storage filter driver. Unlike hardware-based providers, software-based providers create shadow copies at the software level, not the hardware level.

A software-based shadow copy provider must maintain a "point-in-time" view of a volume by having access to a data set that can be used to re-create volume status before the shadow copy creation time. An example is the copy-on-write technique of the system provider. However, the Volume Shadow Copy Service places no restrictions on what technique the software-based providers use to create and maintain shadow copies.

A software provider is applicable to a wider range of storage platforms than a hardware-based provider, and it should work with basic disks or logical volumes equally well. (A logical volume is a volume that is created by combining free space from two or more disks.) In contrast to hardware shadow copies, software providers consume operating system resources to maintain the shadow copy.

For more information about basic disks, see What Are Basic Disks and Volumes? (https://go.microsoft.com/fwlink/?LinkId=180894) on TechNet.

**System provider**

One shadow copy provider, the system provider, is supplied in the Windows operating system. Although a default provider is supplied in Windows, other vendors are free to supply implementations that are optimized for their storage hardware and software applications.

To maintain the "point-in-time" view of a volume that is contained in a shadow copy, the system provider uses a copy-on-write technique. Copies of the blocks on volume that have been modified since the beginning of the shadow copy creation are stored in a shadow copy storage area.

The system provider can expose the production volume, which can be written to and read from normally. When the shadow copy is needed, it logically applies the differences to data on the production volume to expose the complete shadow copy.

For the system provider, the shadow copy storage area must be on an NTFS volume. The volume to be shadow copied does not need to be an NTFS volume, but at least one volume mounted on the system must be an NTFS volume.

The component files that make up the system provider are swprv.dll and volsnap.sys.

**In-Box VSS Writers**

The Windows operating system includes a set of VSS writers that are responsible for enumerating the data that is required by various Windows features.

For more information about these writers, see the following Microsoft Docs Web page:

- In-Box VSS Writers (https://docs.microsoft.com/windows/win32/vss/in-box-vss-writers)

## How Shadow Copies Are Used

In addition to backing up application data and system state information, shadow copies can be used for a number of purposes, including the following:

- Restoring LUNs (LUN resynchronization and LUN swapping)
- Restoring individual files (Shadow Copies for Shared Folders)
- Data mining by using transportable shadow copies

**Restoring LUNs (LUN resynchronization and LUN swapping)**

In Windows Server 2008 R2 and Windows 7, VSS requesters can use a hardware shadow copy provider feature called LUN resynchronization (or "LUN resync"). This is a fast-recovery scheme that allows an application administrator to restore data from a shadow copy to the original LUN or to a new LUN.

The shadow copy can be a full clone or a differential shadow copy. In either case, at the end of the resync operation, the destination LUN will have the same contents as the shadow copy LUN. During the resync operation, the array performs a block-level copy from the shadow copy to the destination LUN.

> **NOTE**
> The shadow copy must be a transportable hardware shadow copy.

Most arrays allow production I/O operations to resume shortly after the resync operation begins. While the resync operation is in progress, read requests are redirected to the shadow copy LUN, and write requests to the destination LUN. This allows arrays to recover very large data sets and resume normal operations in several seconds.

LUN resynchronization is different from LUN swapping. A LUN swap is a fast recovery scenario that VSS has supported since Windows Server 2003 SP1. In a LUN swap, the shadow copy is imported and then converted into a read-write volume. The conversion is an irreversible operation, and the volume and underlying LUN cannot be controlled with the VSS APIs after that. The following list describes how LUN resynchronization compares with LUN swapping:

- In LUN resynchronization, the shadow copy is not altered, so it can be used several times. In LUN swapping, the shadow copy can be used only once for a recovery. For the most safety-conscious administrators, this is important. When LUN resynchronization is used, the requester can retry the entire restore operation if something goes wrong the first time.
- At the end of a LUN swap, the shadow copy LUN is used for production I/O requests. For this reason, the shadow copy LUN must use the same quality of storage as the original production LUN to ensure that performance is not impacted after the recovery operation. If LUN resynchronization is used instead, the hardware provider can maintain the shadow copy on storage that is less expensive than production-quality storage.
- If the destination LUN is unusable and needs to be recreated, LUN swapping may be more economical because it doesn't require a destination LUN.

**WARNING**

All of the operations listed are LUN-level operations. If you attempt to recover a specific volume by using LUN resynchronization, you are unwittingly going to revert all the other volumes that are sharing the LUN.

**Restoring individual files (Shadow Copies for Shared Folders)**

Shadow Copies for Shared Folders uses the Volume Shadow Copy Service to provide point-in-time copies of files that are located on a shared network resource, such as a file server. With Shadow Copies for Shared Folders, users can quickly recover deleted or changed files that are stored on the network. Because they can do so without administrator assistance, Shadow Copies for Shared Folders can increase productivity and reduce administrative costs.

For more information about Shadow Copies for Shared Folders, see Shadow Copies for Shared Folders (https://go.microsoft.com/fwlink/?LinkId=180898) on TechNet.

**Data mining by using transportable shadow copies**

With a hardware provider that is designed for use with the Volume Shadow Copy Service, you can create transportable shadow copies that can be imported onto servers within the same subsystem (for example, a SAN). These shadow copies can be used to seed a production or test installation with read-only data for data mining.

With the Volume Shadow Copy Service and a storage array with a hardware provider that is designed for use with the Volume Shadow Copy Service, it is possible to create a shadow copy of the source data volume on one server, and then import the shadow copy onto another server (or back to the same server). This process is accomplished in a few minutes, regardless of the size of the data. The transport process is accomplished through a series of steps that use a shadow copy requester (a storage-management application) that supports transportable shadow copies.

## To transport a shadow copy

1. Create a transportable shadow copy of the source data on a server.
2. Import the shadow copy to a server that is connected to the SAN (you can import to a different server or the same server).
3. The data is now ready to be used.

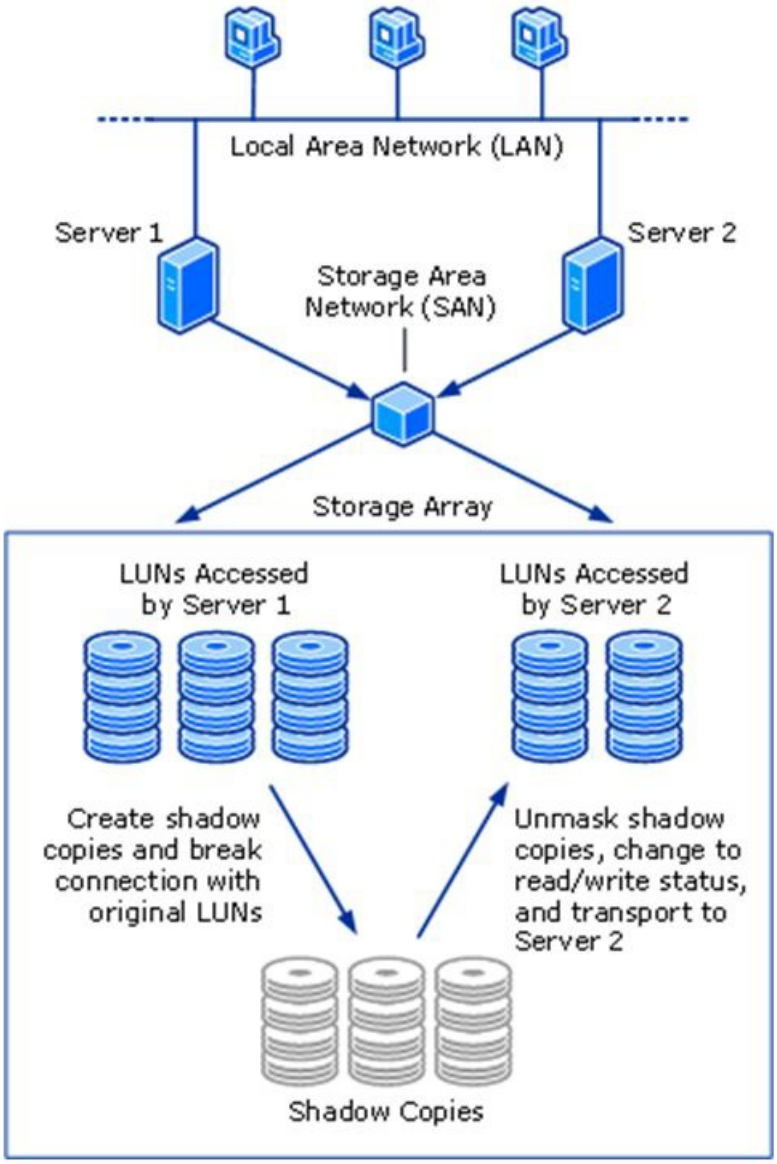



**Figure 3** Shadow copy creation and transport between two servers

> **NOTE**
>
> A transportable shadow copy that is created on Windows Server 2003 cannot be imported onto a server that is running Windows Server 2008 or Windows Server 2008 R2. A transportable shadow copy that was created on Windows Server 2008 or Windows Server 2008 R2 cannot be imported onto a server that is running Windows Server 2003. However, a shadow copy that is created on Windows Server 2008 can be imported onto a server that is running Windows Server 2008 R2 and vice versa.

Shadow copies are read-only. If you want to convert a shadow copy to a read/write LUN, you can use a Virtual Disk Service-based storage-management application (including some requesters) in addition to the Volume Shadow Copy Service. By using this application, you can remove the shadow copy from Volume Shadow Copy Service management and convert it to a read/write LUN.

Volume Shadow Copy Service transport is an advanced solution on computers running Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition, Windows Server 2008, or Windows Server 2008 R2. It works only if there is a hardware provider on the storage array. Shadow copy transport can be used for a number of purposes, including tape backups, data mining, and testing.

## Frequently Asked Questions

This FAQ answers questions about Volume Shadow Copy Service (VSS) for system administrators. For information

about VSS application programming interfaces, see Volume Shadow Copy Service (https://go.microsoft.com/fwlink/?LinkId=180899) in the Windows Developer Center Library.

**When was Volume Shadow Copy Service introduced? On which Windows operating system versions is it available?**

VSS was introduced in Windows XP. It is available on Windows XP, Windows Server 2003, Windows Vista®, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

**What is the difference between a shadow copy and a backup?**

In the case of a hard disk drive backup, the shadow copy created is also the backup. Data can be copied off the shadow copy for a restore or the shadow copy can be used for a fast recovery scenario—for example, LUN resynchronization or LUN swapping.

When data is copied from the shadow copy to tape or other removable media, the content that is stored on the media constitutes the backup. The shadow copy itself can be deleted after the data is copied from it.

**What is the largest size volume that Volume Shadow Copy Service supports?**

Volume Shadow Copy Service supports a volume size of up to 64 TB.

**I made a backup on Windows Server 2008. Can I restore it on Windows Server 2008 R2?**

It depends on the backup software that you used. Most backup programs support this scenario for data but not for system state backups.

Shadow copies that are created on either of these versions of Windows can be used on the other.

**I made a backup on Windows Server 2003. Can I restore it on Windows Server 2008?**

It depends on the backup software you used. If you create a shadow copy on Windows Server 2003, you cannot use it on Windows Server 2008. Also, if you create a shadow copy on Windows Server 2008, you cannot restore it on Windows Server 2003.

**How can I disable VSS?**

It is possible to disable the Volume Shadow Copy Service by using the Microsoft Management Console. However, you should not do this. Disabling VSS adversely affects any software you use that depends on it, such as System Restore and Windows Server Backup.

For more information, see the following Microsoft TechNet Web sites:

- System Restore (https://go.microsoft.com/fwlink/?LinkID=157113)
- Windows Server Backup (https://go.microsoft.com/fwlink/?LinkID=180891)

**Can I exclude files from a shadow copy to save space?**

VSS is designed to create shadow copies of entire volumes. Temporary files, such as paging files, are automatically omitted from shadow copies to save space.

To exclude specific files from shadow copies, use the following registry key: **FilesNotToSnapshot**.

**NOTE**

The **FilesNotToSnapshot** registry key is intended to be used only by applications. Users who attempt to use it will encounter limitations such as the following:

- It cannot delete files from a shadow copy that was created on a Windows Server by using the Previous Versions feature.
- It cannot delete files from shadow copies for shared folders.
- It can delete files from a shadow copy that was created by using the Diskshadow utility, but it cannot delete files from a shadow copy that was created by using the Vssadmin utility.
- Files are deleted from a shadow copy on a best-effort basis. This means that they are not guaranteed to be deleted.

For more information, see Excluding Files from Shadow Copies (https://go.microsoft.com/fwlink/?LinkId=180904) on MSDN.

**My non-Microsoft backup program failed with a VSS error. What can I do?**

Check the product support section of the Web site of the company that created the backup program. There may be a product update that you can download and install to fix the problem. If not, contact the company's product support department.

System administrators can use the VSS troubleshooting information on the following Microsoft TechNet Library Web site to gather diagnostic information about VSS-related issues.

For more information, see Volume Shadow Copy Service (https://go.microsoft.com/fwlink/?LinkId=180905) on TechNet.

**What is the "diff area"?**

The shadow copy storage area (or "diff area") is the location where the data for the shadow copy that is created by the system software provider is stored.

**Where is the diff area located?**

The diff area can be located on any local volume. However, it must be located on an NTFS volume that has enough space to store it.

**How is the diff area location determined?**

The following criteria are evaluated, in this order, to determine the diff area location:

- If a volume already has an existing shadow copy, that location is used.
- If there is a preconfigured manual association between the original volume and the shadow copy volume location, then that location is used.
- If the previous two criteria do not provide a location, the shadow copy service chooses a location based on available free space. If more than one volume is being shadow copied, the shadow copy service creates a list of possible snapshot locations based on the size of free space, in descending order. The number of locations provided is equal to the number of volumes being shadow copied.
- If the volume being shadow copied is one of the possible locations, then a local association is created. Otherwise an association with the volume with the most available space is created.

**Can VSS create shadow copies of non-NTFS volumes?**

Yes. However, persistent shadow copies can be made only for NTFS volumes. In addition, at least one volume mounted on the system must be an NTFS volume.

**What's the maximum number of shadow copies I can create at one time?**

The maximum number of shadow copied volumes in a single shadow copy set is 64. Note that this is not the same as the number of shadow copies.

**What's the maximum number of software shadow copies created by the system provider that I can maintain for a volume?**

The max number is of software shadow copies for each volume is 512. However, by default you can only maintain 64 shadow copies that are used by the Shadow Copies of Shared Folders feature. To change the limit for the Shadow Copies of Shared Folders feature, use the following registry key: **MaxShadowCopies**.

**How can I control the space that is used for shadow copy storage space?**

Type the **vssadmin resize shadowstorage** command.

For more information, see Vssadmin resize shadowstorage (https://go.microsoft.com/fwlink/?LinkId=180906) on TechNet.

**What happens when I run out of space?**

Shadow copies for the volume are deleted, beginning with the oldest shadow copy.

# Volume Shadow Copy Service Tools

The Windows operating system provides the following tools for working with VSS:

- DiskShadow (https://go.microsoft.com/fwlink/?LinkId=180907)
- VssAdmin (https://go.microsoft.com/fwlink/?LinkId=84008)

**DiskShadow**

DiskShadow is a VSS requester that you can use to manage all the hardware and software snapshots that you can have on a system. DiskShadow includes commands such as the following:

- **list**: Lists VSS writers, VSS providers, and shadow copies
- **create**: Creates a new shadow copy
- **import**: Imports a transportable shadow copy
- **expose**: Exposes a persistent shadow copy (as a drive letter, for example)
- **revert**: Reverts a volume back to a specified shadow copy

This tool is intended for use by IT professionals, but developers might also find it useful when testing a VSS writer or VSS provider.

DiskShadow is available only on Windows Server operating systems. It is not available on Windows client operating systems.

**VssAdmin**

VssAdmin is used to create, delete, and list information about shadow copies. It can also be used to resize the shadow copy storage area ("diff area").

VssAdmin includes commands such as the following:

- **create shadow**: Creates a new shadow copy
- **delete shadows**: Deletes shadow copies
- **list providers**: Lists all registered VSS providers
- **list writers**: Lists all subscribed VSS writers

- **resize shadowstorage**: Changes the maximum size of the shadow copy storage area

VssAdmin can only be used to administer shadow copies that are created by the system software provider.

VssAdmin is available on Windows client and Windows Server operating system versions.

## Volume Shadow Copy Service Registry Keys

The following registry keys are available for use with VSS:

- **VssAccessControl**
- **MaxShadowCopies**
- **MinDiffAreaFileSize**

**VssAccessControl**

This key is used to specify which users have access to shadow copies.

For more information, see the following entries on the MSDN Web site:

- Security Considerations for Writers (https://go.microsoft.com/fwlink/?LinkId=157739)
- Security Considerations for Requesters (https://go.microsoft.com/fwlink/?LinkId=180908)

**MaxShadowCopies**

This key specifies the maximum number of client-accessible shadow copies that can be stored on each volume of the computer. Client-accessible shadow copies are used by Shadow Copies for Shared Folders.

For more information, see the following entry on the MSDN Web site:

**MaxShadowCopies** under Registry Keys for Backup and Restore (https://go.microsoft.com/fwlink/?LinkId=180909)

**MinDiffAreaFileSize**

This key specifies the minimum initial size, in MB, of the shadow copy storage area.

For more information, see the following entry on the MSDN Web site:

**MinDiffAreaFileSize** under Registry Keys for Backup and Restore (https://go.microsoft.com/fwlink/?LinkId=180910)

**Supported Operating System Versions**

The following table lists the minimum supported operating system versions for VSS features.

| VSS FEATURE | MINIMUM SUPPORTED CLIENT | MINIMUM SUPPORTED SERVER |
|---|---|---|
| LUN resynchronization | None supported | Windows Server 2008 R2 |
| **FilesNotToSnapshot** registry key | Windows Vista | Windows Server 2008 |
| Transportable shadow copies | None supported | Windows Server 2003 with SP1 |
| Hardware shadow copies | None supported | Windows Server 2003 |

| VSS FEATURE | MINIMUM SUPPORTED CLIENT | MINIMUM SUPPORTED SERVER |
| --- | --- | --- |
| Previous versions of Windows Server | Windows Vista | Windows Server 2003 |
| Fast recovery using LUN swap | None supported | Windows Server 2003 with SP1 |
| Multiple imports of hardware shadow copies<br><br>**NOTE**<br>This is the ability to import a shadow copy more than once. Only one import operation can be performed at a time. | None supported | Windows Server 2008 |
| Shadow Copies for Shared Folders | None supported | Windows Server 2003 |
| Transportable auto-recovered shadow copies | None supported | Windows Server 2008 |
| Concurrent backup sessions (up to 64) | Windows XP | Windows Server 2003 |
| Single restore session concurrent with backups | Windows Vista | Windows Server 2003 with SP2 |
| Up to 8 restore sessions concurrent with backups | Windows 7 | Windows Server 2003 R2 |

# Additional References

Volume Shadow Copy Service in Windows Developer Center

# Using Disk Cleanup on Windows Server

11/2/2020 • 2 minutes to read • Edit Online

> Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

The Disk Cleanup tool clears unnecessary files in a Windows Server environment. This tool is available by default on Windows Server 2019 and Windows Server 2016, but you might have to take a few manual steps to enable it on earlier versions of Windows Server.

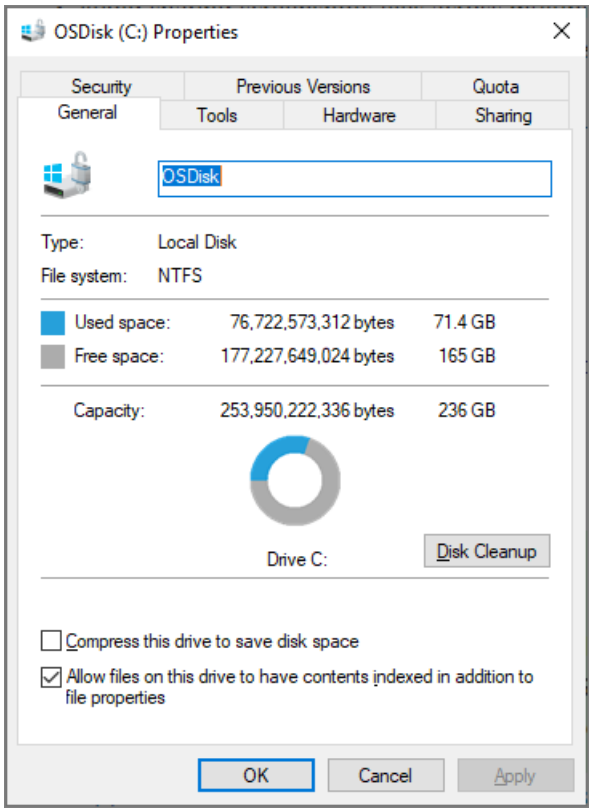
To start the Disk Cleanup tool, either run the Cleanmgr.exe command, or select **Start**, select **Windows Administrative Tools**, and then select **Disk Cleanup**.

You can also run Disk Cleanup by using the cleanmgr Windows command and use command-line options to specify that Disk Cleanup cleans up certain files.

## Enable Disk Cleanup on an earlier version of Windows Server by installing the Desktop Experience

Follow these steps to use the Add Roles and Features Wizard to install the Desktop Experience on a server running Windows Server 2012 R2 or earlier, which also installs Disk Cleanup.

1. If Server Manager is already open, go on to the next step. If Server Manager is not already open, open it by doing one of the following.
   - On the Windows desktop, start Server Manager by clicking **Server Manager** in the Windows taskbar.
   - Go to **Start** and select the Server Manager tile.
2. On the **Manage** menu, select add **Roles and Features**.
3. On the **Before you begin** page, verify that your destination server and network environment are prepared for the feature that you want to install. Select **Next**.
4. On the **Select installation type** page, select **Role-based or feature-based installation** to install all parts features on a single server. Select **Next**.
5. On the **Select destination server** page, select a server from the server pool, or select an offline VHD. Select **Next**.
6. On the **Select server roles** page, select **Next**.
7. On the **Select features** page, select **User Interface and Infrastructure**, and then select **Desktop Experience**.
8. In **Add features that are required for Desktop Experience?**, select **Add Features**.
9. Proceed with the installation, and then reboot the system.
10. Verify that the **Disk Cleanup** option button appears in the Properties dialog box.




## Manually add Disk Cleanup to an earlier version of Windows Server

The Disk Cleanup tool (cleanmgr.exe) isn't present on Windows Server 2012 R2 or earlier unless you have the Desktop Experience feature installed.

To use cleanmgr.exe, install the Desktop Experience as described earlier, or copy two files that are already present on the server, cleanmgr.exe and cleanmgr.exe.mui. Use the following table to locate the files for your operating system.

| OPERATING SYSTEM | ARCHITECTURE | FILE LOCATION |
|---|---|---|
| Windows Server 2008 R2 | 64-bit | C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr_31bf3856ad364e35_6.1.7600.16385_none_c9392808773cd7da\cleanmgr.exe |
| Windows Server 2008 R2 | 64-bit | C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9cb6194b257cc63\cleanmgr.exe.mui |

Locate cleanmgr.exe and move the file to **%systemroot%\System32**.

Locate cleanmgr.exe.mui and move the files to **%systemroot%\System32\en-US**.

You can now launch the Disk cleanup tool by running Cleanmgr.exe from Command Prompt, or by clicking **Start** and typing **Cleanmgr** into the search bar.

To have Disk Cleanup button appear on a disk's Properties dialog, you will also need to install the Desktop Experience feature.

## Additional references

Free up drive space in Windows 10

cleanmgr

# Advanced Troubleshooting Server Message Block (SMB)

7/22/2020 • 5 minutes to read • Edit Online

Server Message Block (SMB) is a network transport protocol for file systems operations to enable a client to access resources on a server. The primary purpose of the SMB protocol is to enable remote file system access between two systems over TCP/IP.

SMB troubleshooting can be extremely complex. This article is not an exhaustive troubleshooting guide Instead, it is a short primer to understand the basics of how to effectively troubleshoot SMB.

## Tools and data collection

One key aspect of quality SMB troubleshooting is communicating the correct terminology. Therefore, this article introduces basic SMB terminology to ensure accuracy of data collection and analysis.

> **NOTE**
> The *SMB Server (SRV)* refers to the system that is hosting the file system, also known as the file server. *The SMB Client (CLI)* refers to the system that is trying to access the file system, regardless of the OS version or edition.

For example, if you use Windows Server 2016 to reach an SMB share that is hosted on Windows 10, Windows Server 2016 is the SMB Client and Windows 10 the SMB Server.

### Collect data

Before you troubleshoot SMB issues, we recommend that you first collect a network trace on both the client and server sides. The following guidelines apply:

- On Windows systems, you can use netshell (netsh), Network Monitor, Message Analyser, or Wireshark to collect a network trace.
- Third-party devices generally have an in-box packet capture tool, such as tcpdump (Linux/FreeBSD/Unix), or pktt (NetApp). For example, if the SMB client or SMB server is a Unix host, you can collect data by running the following command:

  ```
  # tcpdump -s0 -n -i any -w /tmp/$(hostname)-smbtrace.pcap
  ```

  Stop collecting data by using **Ctrl+C** from keyboard.

To discover the source of the issue, you can check the two-sided traces: CLI, SRV, or somewhere in between.

#### Using netshell to collect data

This section provides the steps for using netshell to collect network trace.

> **NOTE**
> A Netsh trace creates an ETL file. ETL files can be opened only in Message Analyzer (MA) and Network Monitor 3.4 (set the parser to Network Monitor Parsers > Windows).

1. On both the SMB server and SMB client, create a **Temp** folder on drive **C**. Then, run the following command:

```
netsh trace start capture=yes report=yes scenario=NetConnection level=5 maxsize=1024
tracefile=c:\\Temp\\%computername%\_nettrace.etl**
```

If you are using PowerShell, run the following cmdlets:

```
New-NetEventSession -Name trace -LocalFilePath "C:\Temp\$env:computername`_netCap.etl" -MaxFileSize 1024

Add-NetEventPacketCaptureProvider -SessionName trace -TruncationLength 1500

Start-NetEventSession trace
```

2. Reproduce the issue.
3. Stop the trace by running the following command:

```
netsh trace stop
```

If you are using PowerShell, run the following cmdlets:

```
Stop-NetEventSession trace
Remove-NetEventSession trace
```

> **NOTE**
> You should trace only a minimum amount of the data that's transferred. For performance issues, always take both a good and bad trace, if the situation allows it.

**Analyze the traffic**

SMB is an application-level protocol that uses TCP/IP as the network transport protocol. Therefore, an SMB issue can also be caused by TCP/IP issues.

Check whether TCP/IP experiences any of these issues:

1. The TCP three-way handshake does not finish. This typically indicates that there is a firewall block, or that the Server service is not running.
2. Retransmits are occurring. These can cause slow file transfers because of compound TCP congestion throttling.
3. Five retransmits followed by a TCP reset could mean that the connection between systems was lost, or that one of the SMB services crashed or stopped responding.
4. The TCP receive window is diminishing. This can be caused by slow storage or some other issue that prevents data from being retrieved from the Ancillary Function Driver (AFD) Winsock buffer.

If there is no noticeable TCP/IP issue, look for SMB errors. To do this, follow these steps:

1. Always check SMB errors against the MS-SMB2 protocol specification. Many SMB errors are benign (not harmful). Refer to the following information to determine why SMB returned the error before you conclude that the error is related to any of the following issues:
   - The MS-SMB2 Message Syntax topic details each SMB command and its options.
   - The MS-SMB2 Client Processing topic details how the SMB client creates requests and responds to server messages.

- The MS-SMB2 Server Processing topic details how the SMB server creates requests and responds to client requests.

2. Check whether a TCP reset command is sent immediately after an FSCTL_VALIDATE_NEGOTIATE_INFO (validate negotiate) command. If so, refer to the following information:

   - The SMB session must be terminated (TCP reset) when the Validate Negotiate process fails on either the client or the server.
   - This process might fail because a WAN optimizer is modifying the SMB Negotiate packet.
   - If the connection ended prematurely, identify the last exchange communication between the client and server.

#### Analyze the protocol

Look at the actual SMB protocol details in the network trace to understand the exact commands and options that are used.

> **NOTE**
> Only Message Analyzer can parse SMBv3 and later version commands.

- Remember that SMB does only what it is told to do.
- You can learn a lot about what the application is trying to do by examining the SMB commands.

Compare the commands and operations to the protocol specification to make sure that everything is operating correctly. If it is not, collect data that is closer to or at a lower level to look for more information about the root cause. To do this, follow these steps:

1. Collect a standard packet capture.
2. Run the **netsh** command to trace and gather details about whether there are issues in the network stack or drops in Windows Filtering Platform (WFP) applications, such as firewall or antivirus program.
3. If all other options fail, collect a t.cmd if you suspect that the issue occurs within SMB itself, or if none of the other data is sufficient to identify a root cause.

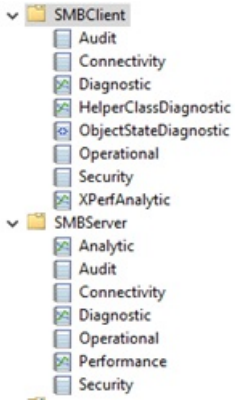
For example:

- You experience slow file transfers to a single file server.
- The two-sided traces show that the SRV responds slowly to a READ request.
- Removing an antivirus program resolves the slow file transfers.
- You contact the antivirus program manufactory to resolve the issue.

> **NOTE**
> Optionally, you might **also** temporarily uninstall the antivirus program during troubleshooting.

#### Event logs

Both SMB Client and SMB Server have a detailed event log structure, as shown in the following screenshot. Collect the event logs to help find the root cause of the issue.




## SMB-related system files

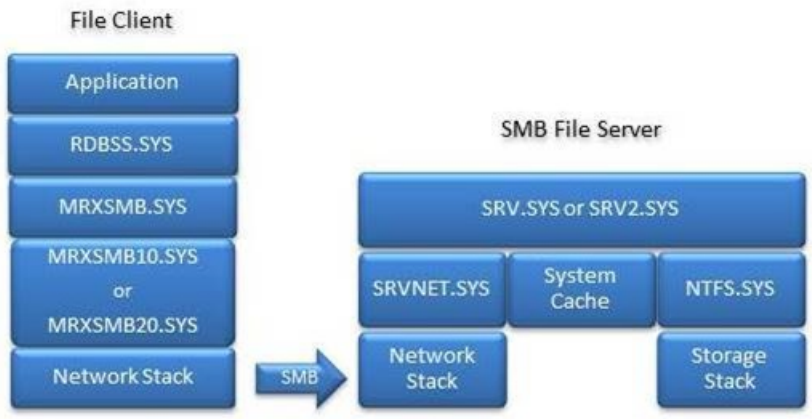
This section lists the SMB-related system files. To keep the system files updated, make sure that the latest update rollup is installed.

SMB Client binaries that are listed under **%windir%\system32\Drivers**:

- RDBSS.sys
- MRXSMB.sys
- MRXSMB10.sys
- MRXSMB20.sys
- MUP.sys
- SMBdirect.sys

SMB Server binaries that are listed under **%windir%\system32\Drivers**:

- SRVNET.sys
- SRV.sys
- SRV2.sys
- SMBdirect.sys
- Under **%windir%\system32**
- srvsvc.dll




**Update suggestions**

We recommend that you update the following components before you troubleshoot SMB issues:

- A file server requires file storage. If your storage has iSCSI component, update those components.
- Update the network components.
- For better performance and stability, update Windows Core.

## Reference

Microsoft SMB Protocol Packet Exchange Scenario

# How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows

12/16/2020 • 9 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This article describes how to enable and disable Server Message Block (SMB) version 1 (SMBv1), SMB version 2 (SMBv2), and SMB version 3 (SMBv3) on the SMB client and server components.

While disabling or removing SMBv1 might cause some compatibility issues with old computers or software, SMBv1 has significant security vulnerabilities and we strongly encourage you not to use it.

## Disabling SMBv2 or SMBv3 for troubleshooting

While we recommend that you keep SMBv2 and SMBv3 enabled, you might find it useful to disable one temporarily for troubleshooting, as described in How to detect status, enable, and disable SMB protocols on the SMB Server.

In Windows 10, Windows 8.1, and Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012, disabling SMBv3 deactivates the following functionality (and also the SMBv2 functionality that's described in the previous list):

- Transparent Failover - clients reconnect without interruption to cluster nodes during maintenance or failover
- Scale Out – concurrent access to shared data on all file cluster nodes
- Multichannel - aggregation of network bandwidth and fault tolerance if multiple paths are available between client and server
- SMB Direct – adds RDMA networking support for very high performance, with low latency and low CPU utilization
- Encryption – Provides end-to-end encryption and protects from eavesdropping on untrustworthy networks
- Directory Leasing - Improves application response times in branch offices through caching
- Performance Optimizations - optimizations for small random read/write I/O

In Windows 7 and Windows Server 2008 R2, disabling SMBv2 deactivates the following functionality:

- Request compounding - allows for sending multiple SMB 2 requests as a single network request
- Larger reads and writes - better use of faster networks
- Caching of folder and file properties - clients keep local copies of folders and files
- Durable handles - allow for connection to transparently reconnect to the server if there is a temporary disconnection
- Improved message signing - HMAC SHA-256 replaces MD5 as hashing algorithm
- Improved scalability for file sharing - number of users, shares, and open files per server greatly increased
- Support for symbolic links
- Client oplock leasing model - limits the data transferred between the client and server, improving performance on high-latency networks and increasing SMB server scalability
- Large MTU support - for full use of 10-gigabye (GB) Ethernet
- Improved energy efficiency - clients that have open files to a server can sleep

The SMBv2 protocol was introduced in Windows Vista and Windows Server 2008, while the SMBv3 protocol was introduced in Windows 8 and Windows Server 2012. For more information about the capabilities of SMBv2 and SMBv3 capabilities, see the following articles:

Server Message Block overview

What's New in SMB

# How to remove SMB v1

Here's how to remove SMBv1 in Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, and Windows 2012 R2.

**PowerShell methods**

SMB v1 (client and server)

- Detect:

```
Get-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

- Disable:

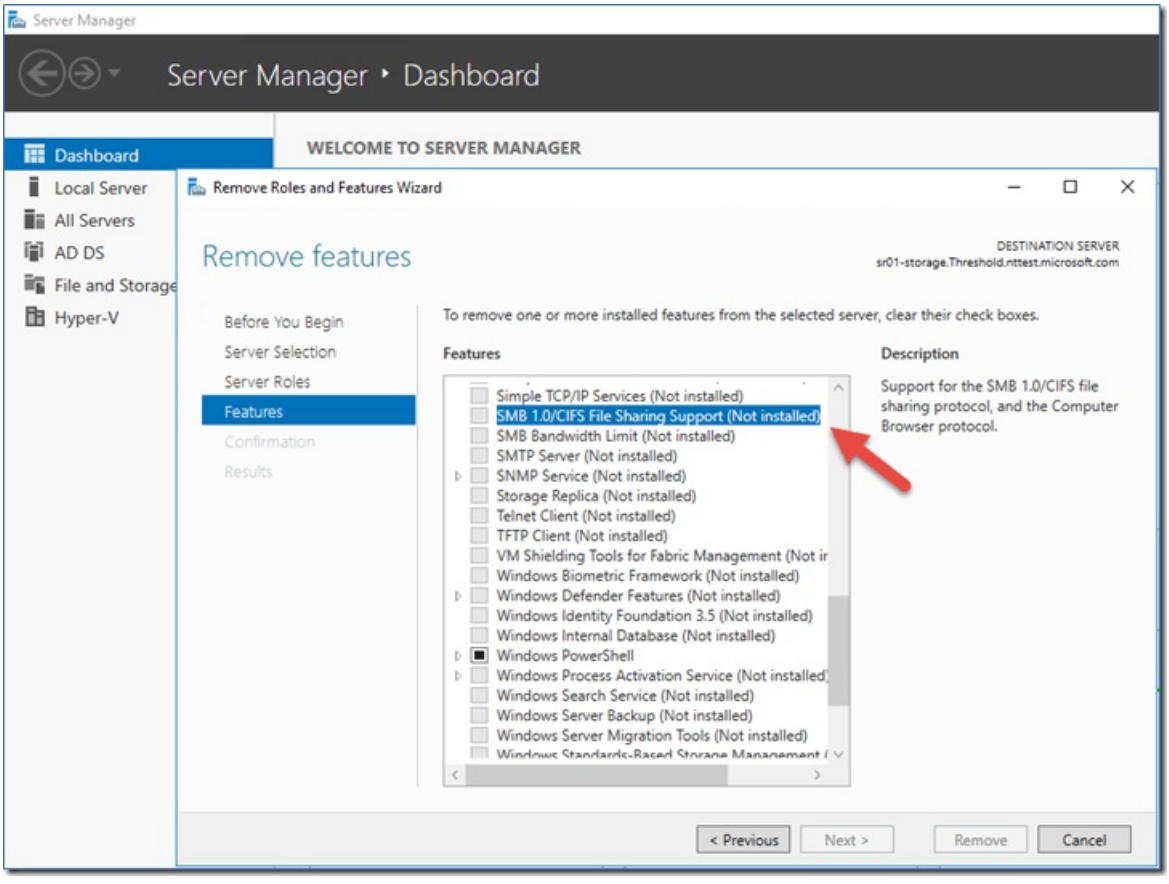
```
Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

- Enable:

```
Enable-WindowsOptionalFeature -Online -FeatureName smb1protocol
```

**Windows Server 2012 R2, Windows Server 2016, Windows Server 2019: Server Manager method for disabling SMB**

SMB v1




**Windows 8.1 and Windows 10: PowerShell method**

SMB v1 Protocol

- Detect:

```
Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

- Disable:

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

- Enable:

```
Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

##### SMB v2/v3 Protocol (only disables SMB v2/v3 Server)

- Detect:

```
Get-SmbServerConfiguration | Select EnableSMB2Protocol
```

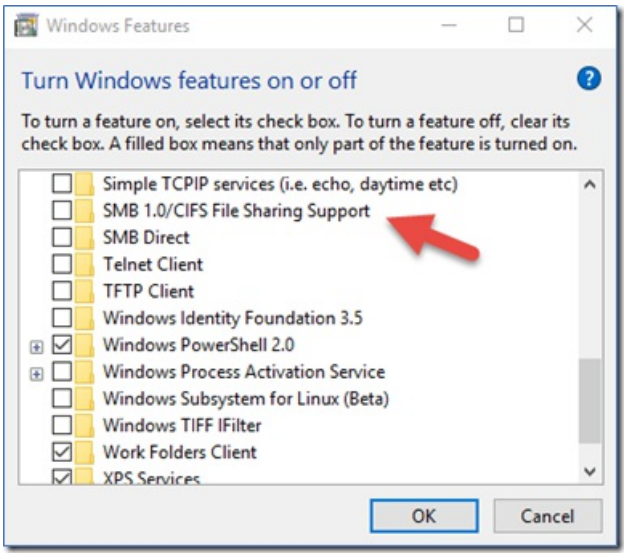
- Disable:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- Enable:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

**Windows 8.1 and Windows 10: Add or Remove Programs method**




## How to detect status, enable, and disable SMB protocols on the SMB Server

### For Windows 8 and Windows Server 2012

Windows 8 and Windows Server 2012 introduce the new **Set-SMBServerConfiguration** Windows PowerShell cmdlet. The cmdlet enables you to enable or disable the SMBv1, SMBv2, and SMBv3 protocols on the server component.

> **NOTE**
>
> When you enable or disable SMBv2 in Windows 8 or Windows Server 2012, SMBv3 is also enabled or disabled. This behavior occurs because these protocols share the same stack.

You do not have to restart the computer after you run the **Set-SMBServerConfiguration** cmdlet.

###### SMB v1 on SMB Server

- Detect:

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol
```

- Disable:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- Enable:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

For more information, see Server storage at Microsoft.

###### SMB v2/v3 on SMB Server

- Detect:

```
Get-SmbServerConfiguration | Select EnableSMB2Protocol
```

- Disable:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- Enable:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

### For Windows 7, Windows Server 2008 R2, Windows Vista, and Windows Server 2008

To enable or disable SMB protocols on an SMB Server that is running Windows 7, Windows Server 2008 R2, Windows Vista, or Windows Server 2008, use Windows PowerShell or Registry Editor.

#### PowerShell methods

> **NOTE**
>
> This method requires PowerShell 2.0 or later version of PowerShell.

###### SMB v1 on SMB Server

Detect:

```
Get-Item HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters | ForEach-Object {Get-ItemProperty
$_.pspath}
```

Default configuration = Enabled (No registry key is created), so no SMB1 value will be returned

Disable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -
Value 0 -Force
```

Enable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -
Value 1 -Force
```

**Note** You must restart the computer after you make these changes. For more information, see Server storage at Microsoft.

#### SMB v2/v3 on SMB Server

Detect:

```
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters | ForEach-Object {Get-
ItemProperty $_.pspath}
```

Disable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -
Value 0 -Force
```

Enable:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -Type DWORD -
Value 1 -Force
```

> **NOTE**
> You must restart the computer after you make these changes.

**Registry Editor**

> **IMPORTANT**
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, back up the registry for restoration in case problems occur.

To enable or disable SMBv1 on the SMB server, configure the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

```
Registry entry: SMB1
REG_DWORD: 0 = Disabled
REG_DWORD: 1 = Enabled
Default: 1 = Enabled (No registry key is created)
```

To enable or disable SMBv2 on the SMB server, configure the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

```
Registry entry: SMB2
REG_DWORD: 0 = Disabled
REG_DWORD: 1 = Enabled
Default: 1 = Enabled (No registry key is created)
```

> **NOTE**
>
> You must restart the computer after you make these changes.

# How to detect status, enable, and disable SMB protocols on the SMB Client

### For Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012

> **NOTE**
>
> When you enable or disable SMBv2 in Windows 8 or in Windows Server 2012, SMBv3 is also enabled or disabled. This behavior occurs because these protocols share the same stack.

#### SMB v1 on SMB Client

- Detect

```
sc.exe qc lanmanworkstation
```

- Disable:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

- Enable:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi
sc.exe config mrxsmb10 start= auto
```

For more information, see Server storage at Microsoft

#### SMB v2/v3 on SMB Client

- Detect:

```
sc.exe qc lanmanworkstation
```

- Disable:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc.exe config mrxsmb20 start= disabled
```

- Enable:

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi
sc.exe config mrxsmb20 start= auto
```

**NOTE**

- You must run these commands at an elevated command prompt.
- You must restart the computer after you make these changes.

## Disable SMBv1 Server with Group Policy

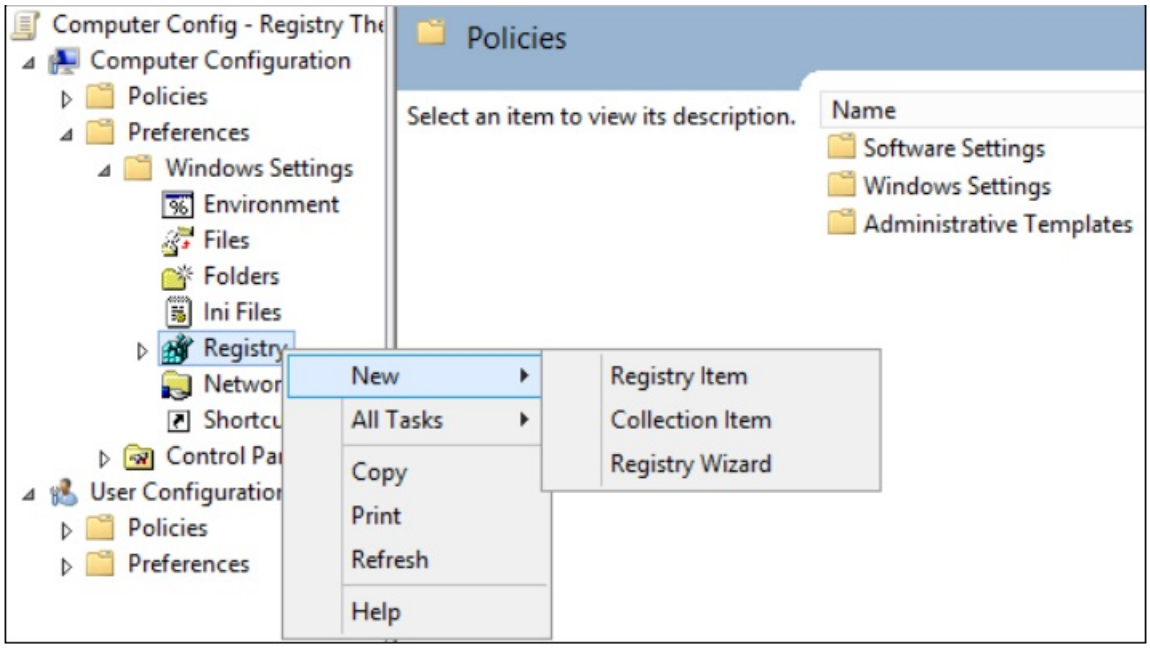
This procedure configures the following new item in the registry:

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**

- Registry entry: **SMB1**
- REG_DWORD: **0** = Disabled

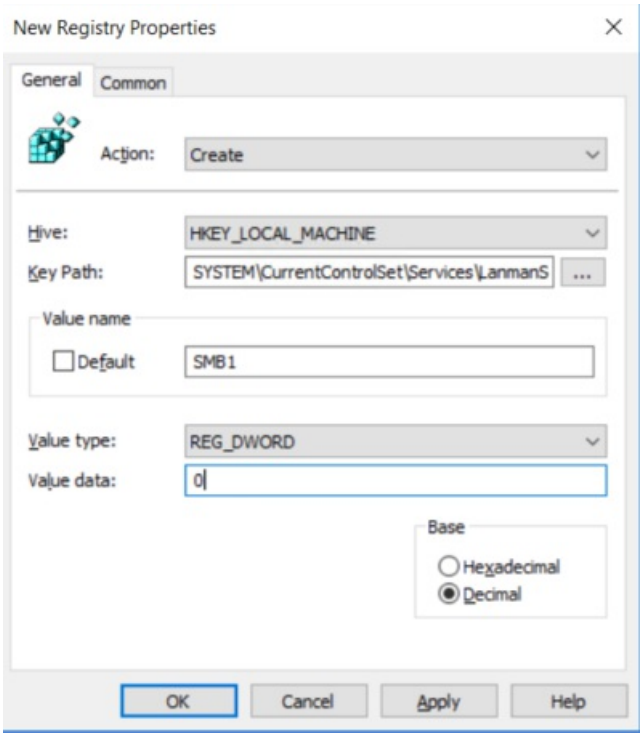
To configure this by using Group Policy, follow these steps:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.




In the **New Registry Properties** dialog box, select the following:

- **Action**: Create
- **Hive**: HKEY_LOCAL_MACHINE
- **Key Path**: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
- **Value name**: SMB1
- **Value type**: REG_DWORD
- **Value data**: 0




This disables the SMBv1 Server components. This Group Policy must be applied to all necessary workstations, servers, and domain controllers in the domain.

> **NOTE**
>
> WMI filters can also be set to exclude unsupported operating systems or selected exclusions, such as Windows XP.

> **IMPORTANT**
>
> Be careful when you make these changes on domain controllers on which legacy Windows XP or older Linux and third-party systems (that do not support SMBv2 or SMBv3) require access to SYSVOL or other file shares where SMB v1 is being disabled.

## Disable SMBv1 Client with Group Policy

To disable the SMBv1 client, the services registry key needs to be updated to disable the start of **MRxSMB10** and then the dependency on **MRxSMB10** needs to be removed from the entry for **LanmanWorkstation** so that it can start normally without requiring **MRxSMB10** to first start.

This will update and replace the default values in the following two items in the registry:

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsmb10**

Registry entry: **Start** REG_DWORD: **4** = Disabled

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation**

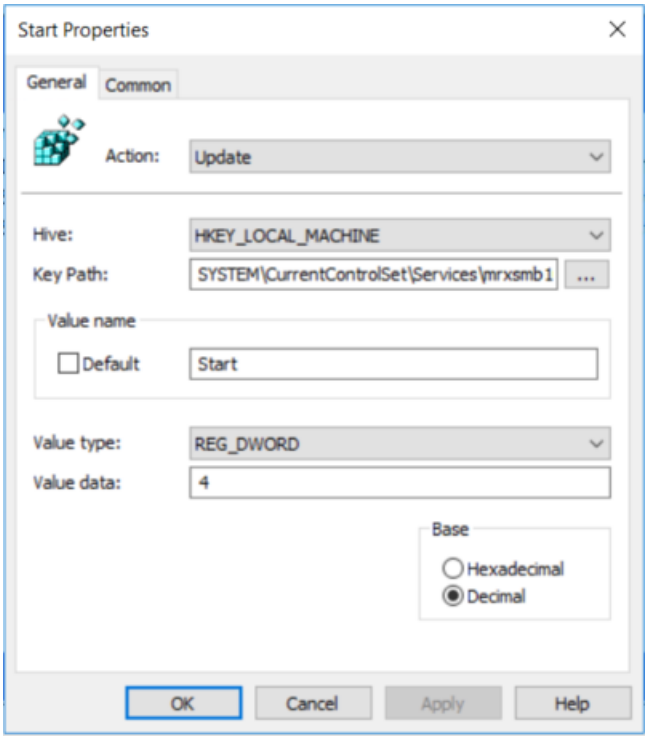
Registry entry: **DependOnService** REG_MULTI_SZ: **"Bowser","MRxSmb20”,"NSI"**

> **NOTE**
>
> The default included MRxSMB10 which is now removed as dependency.

To configure this by using Group Policy, follow these steps:

1. Open the **Group Policy Management Console**. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **Computer Configuration**, expand the **Preferences** folder, and then expand the **Windows Settings** folder.
3. Right-click the **Registry** node, point to **New**, and select **Registry Item**.
4. In the **New Registry Properties** dialog box, select the following:

   - **Action**: Update
   - **Hive**: HKEY_LOCAL_MACHINE
   - **Key Path**: SYSTEM\CurrentControlSet\services\mrxsmb10
   - **Value name**: Start
   - **Value type**: REG_DWORD
   - **Value data**: 4

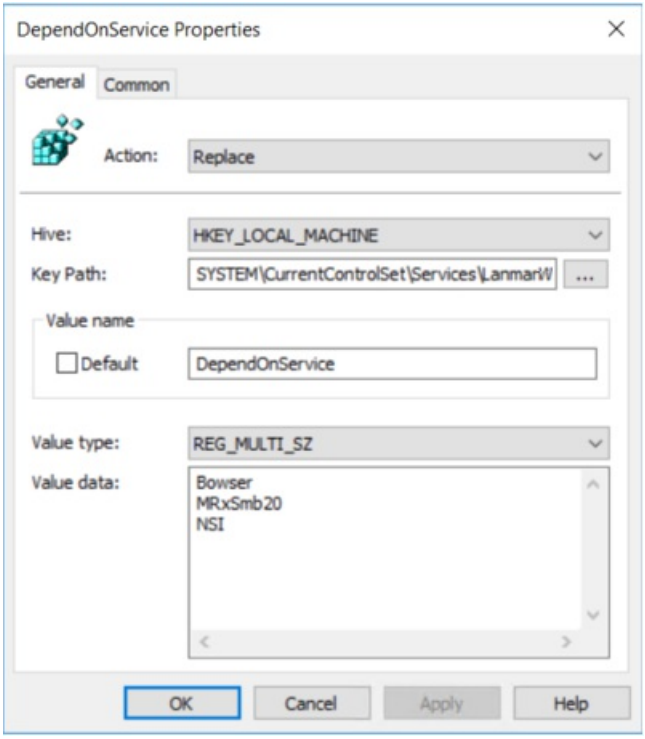



5. Then remove the dependency on the **MRxSMB10** that was just disabled.

   In the **New Registry Properties** dialog box, select the following:

   - **Action**: Replace
   - **Hive**: HKEY_LOCAL_MACHINE
   - **Key Path**: SYSTEM\CurrentControlSet\Services\LanmanWorkstation
   - **Value name**: DependOnService
   - **Value type**: REG_MULTI_SZ
   - **Value data**:
     - Bowser
     - MRxSmb20
     - NSI

> **NOTE**
>
> These three strings will not have bullets (see the following screen shot).




The default value includes **MRxSMB10** in many versions of Windows, so by replacing them with this multi-value string, it is in effect removing **MRxSMB10** as a dependency for **LanmanServer** and going from four default values down to just these three values above.

> **NOTE**
> When you use Group Policy Management Console, you don't have to use quotation marks or commas. Just type the each entry on individual lines.

6. Restart the targeted systems to finish disabling SMB v1.

**Auditing SMBv1 usage**

To determine which clients are attempting to connect to an SMB server with SMBv1, you can enable auditing on Windows Server 2016, Windows 10, and Windows Server 2019. You can also audit on Windows 7 and Windows Server 2008 R2 if they installed the May 2018 monthly update and on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 if they installed the July 2017 monthly update.

- Enable:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

- Disable:

```
Set-SmbServerConfiguration -AuditSmb1Access $false
```

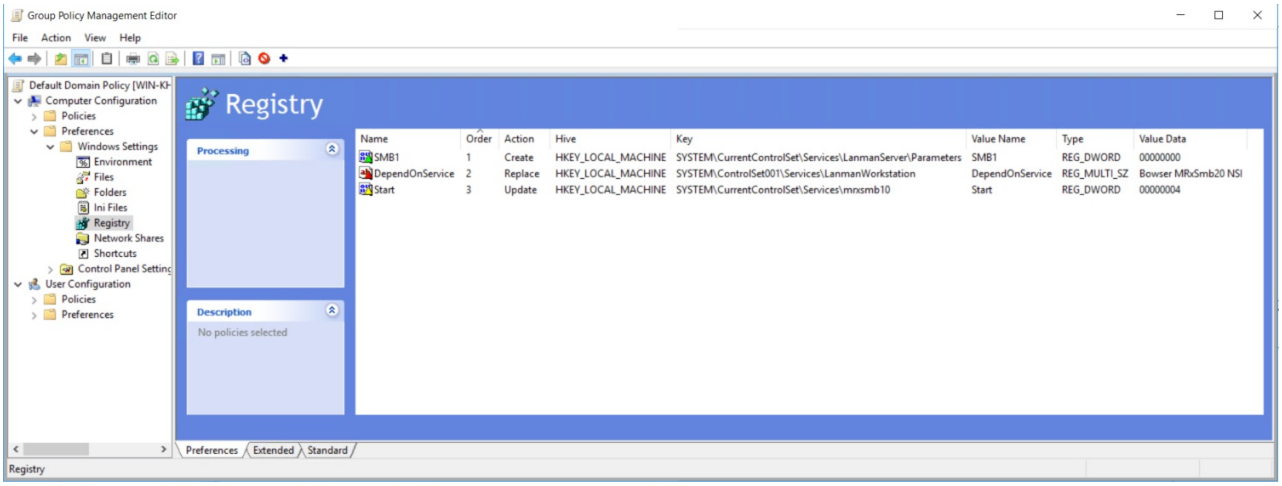
- Detect:

```
Get-SmbServerConfiguration | Select AuditSmb1Access
```

When SMBv1 auditing is enabled, event 3000 appears in the "Microsoft-Windows-SMBServer\Audit" event log, identifying each client that attempts to connect with SMBv1.

### Summary

If all the settings are in the same Group Policy Object (GPO), Group Policy Management displays the following settings.




### Testing and validation

After these are configured, allow the policy to replicate and update. As necessary for testing, run **gpupdate /force** at a command prompt, and then review the target computers to make sure that the registry settings are applied correctly. Make sure SMB v2 and SMB v3 is functioning for all other systems in the environment.

> **NOTE**
>
> Do not forget to restart the target systems.

# SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions

11/2/2020 • 7 minutes to read • Edit Online

## Summary

In Windows 10 Fall Creators Update and Windows Server, version 1709 (RS3) and later versions, the Server Message Block version 1 (SMBv1) network protocol is no longer installed by default. It was superseded by SMBv2 and later protocols starting in 2007. Microsoft publicly deprecated the SMBv1 protocol in 2014.

SMBv1 has the following behavior in Windows 10 and Windows Server starting in version 1709 (RS3):

- SMBv1 now has both client and server sub-features that can be uninstalled separately.
- Windows 10 Enterprise, Windows 10 Education, and Windows 10 Pro for Workstations no longer contain the SMBv1 client or server by default after a clean installation.
- Windows Server 2016 no longer contains the SMBv1 client or server by default after a clean installation.
- Windows 10 Home and Windows 10 Pro no longer contain the SMBv1 server by default after a clean installation.
- Windows 10 Home and Windows 10 Pro still contain the SMBv1 client by default after a clean installation. If the SMBv1 client is not used for 15 days in total (excluding the computer being turned off), it automatically uninstalls itself.
- In-place upgrades and Insider flights of Windows 10 Home and Windows 10 Pro do not automatically remove SMBv1 initially. If the SMBv1 client or server is not used for 15 days in total (excluding the time during which the computer is off), they each automatically uninstall themselves.
- In-place upgrades and Insider flights of the Windows 10 Enterprise, Windows 10 Education, and Windows 10 Pro for Workstations editions do not automatically remove SMBv1. An administrator must decide to uninstall SMBv1 in these managed environments.
- Automatic removal of SMBv1 after 15 days is a one-time operation. If an administrator re-installs SMBv1, no further attempts will be made to uninstall it.
- The SMB version 2.02, 2.1, 3.0, 3.02, and 3.1.1 features are still fully supported and included by default as part of the SMBv2 binaries.
- Because the Computer Browser service relies on SMBv1, the service is uninstalled if the SMBv1 client or server is uninstalled. This means that Explorer Network can no longer display Windows computers through the legacy NetBIOS datagram browsing method.
- SMBv1 can still be reinstalled in all editions of Windows 10 and Windows Server 2016.

SMBv1 has the following additional behaviors in Windows 10 starting in version 1809 (RS5). All other behaviors from version 1709 still apply:

- Windows 10 Pro no longer contains the SMBv1 client by default after a clean installation.
- In Windows 10 Enterprise, Windows 10 Education, and Windows 10 Pro for Workstations an administrator can activate automatic removal of SMBv1 by turning on the "SMB 1.0/CIFS Automatic Removal" feature.

> **NOTE**
>
> Windows 10, version 1803 (RS4) Pro handles SMBv1 in the same manner as Windows 10, version 1703 (RS2) and Windows 10, version 1607 (RS1). This issue was fixed in Windows 10, version 1809 (RS5). You can still uninstall SMBv1 manually. However, Windows will not automatically uninstall SMBv1 after 15 days in the following scenarios:

- You do a clean install of Windows 10, version 1803.
- You upgrade Windows 10, version 1607 or Windows 10, version 1703 to Windows 10, version 1803 directly without first upgrading to Windows 10, version 1709.

If you try to connect to devices that support only SMBv1, or if these devices try to connect to you, you may receive one of the following errors messages:

```
You can't connect to the file share because it's not secure. This share requires the obsolete SMB1 protocol,
which is unsafe and could expose your system to attack.
Your system requires SMB2 or higher. For more info on resolving this issue, see:
https://go.microsoft.com/fwlink/?linkid=852747
```

```
The specified network name is no longer available.
```

```
Unspecified error 0x80004005
```

```
System Error 64
```

```
The specified server cannot perform the requested operation.
```

```
Error 58
```

The following events appear when a remote server required an SMBv1 connection from this client, but SMBv1 is uninstalled or disabled on the client.

```
Log Name:      Microsoft-Windows-SmbClient/Security
 Source:        Microsoft-Windows-SMBClient
 Date:          Date/Time
 Event ID:      32002
 Task Category: None
 Level:         Info
 Keywords:      (128)
 User:          NETWORK SERVICE
 Computer:      junkle.contoso.com
 Description:
 The local computer received an SMB1 negotiate response.

Dialect:
SecurityMode
Server name:

Guidance:
SMB1 is deprecated and should not be installed nor enabled. For more information, see
https://go.microsoft.com/fwlink/?linkid=852747.
```

```
Log Name:      Microsoft-Windows-SmbClient/Security
 Source:        Microsoft-Windows-SMBClient
 Date:          Date/Time
 Event ID:      32000
 Task Category: None
 Level:         Info
 Keywords:      (128)
 User:          NETWORK SERVICE
 Computer:      junkle.contoso.com
 Description:
SMB1 negotiate response received from remote device when SMB1 cannot be negotiated by the local computer.
Dialect:
Server name:

Guidance:
The client has SMB1 disabled or uninstalled. For more information: https://go.microsoft.com/fwlink/?
linkid=852747.
```

These devices are not likely running Windows. They are more likely running older versions of Linux, Samba, or other types of third-party software to provide SMB services. Often, these versions of Linux and Samba are, themselves, no longer supported.

> **NOTE**
> Windows 10, version 1709 is also known as "Fall Creators Update."

# More Information

To work around this issue, contact the manufacturer of the product that supports only SMBv1, and request a software or firmware update that support SMBv2.02 or a later version. For a current list of known vendors and their SMBv1 requirements, see the following Windows and Windows Server Storage Engineering Team Blog article:

SMBv1 Product Clearinghouse

#### Leasing mode

If SMBv1 is required to provide application compatibility for legacy software behavior, such as a requirement to disable oplocks, Windows provides a new SMB share flag that's known as Leasing mode. This flag specifies whether a share disables modern SMB semantics such as leases and oplocks.

You can specify a share without using oplocks or leasing to allow a legacy application to work with SMBv2 or a later version. To do this, use the **New-SmbShare** or **Set-SmbShare** PowerShell cmdlets together with the **-LeasingMode None** parameter.

> **NOTE**
> You should use this option only on shares that are required by a third-party application for legacy support if the vendor states that it is required. Do not specify Leasing mode on user data shares or CA shares that are used by Scale-Out File Servers. This is because the removal of oplocks and leases causes instability and data corruption in most applications. Leasing mode works only in Share mode. It can be used by any client operating system.

#### Explorer Network Browsing

The Computer Browser service relies on the SMBv1 protocol to populate the Windows Explorer Network node (also known as "Network Neighborhood"). This legacy protocol is long deprecated, doesn't route, and has limited security. Because the service cannot function without SMBv1, it is removed at the same time.

However, if you still have to use the Explorer Network in home and small business workgroup environments to locate Windows-based computers, you can follow these steps on your Windows-based computers that no longer

use SMBv1:

1. Start the "Function Discovery Provider Host" and "Function Discovery Resource Publication" services, and then set them to **Automatic (Delayed Start)**.
2. When you open Explorer Network, enable network discovery when you are prompted.

All Windows devices within that subnet that have these settings will now appear in Network for browsing. This uses the WS-DISCOVERY protocol. Contact your other vendors and manufacturers if their devices still don't appear in this browse list after the Windows devices appear. It is possible they have this protocol disabled or that they support only SMBv1.

> **NOTE**
> We recommend that you map drives and printers instead of enabling this feature, which still requires searching and browsing for their devices. Mapped resources are easier to locate, require less training, and are safer to use. This is especially true if these resources are provided automatically through Group Policy. An administrator can configure printers for location by methods other than the legacy Computer Browser service by using IP addresses, Active Directory Domain Services (AD DS), Bonjour, mDNS, uPnP, and so on.

If you cannot use any of these workarounds, or if the application manufacturer cannot provide supported versions of SMB, you can re-enable SMBv1 manually by following the steps in How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows.

> **IMPORTANT**
> We strongly recommend that you don't reinstall SMBv1. This is because this older protocol has known security issues regarding ransomware and other malware.

#### Windows Server best practices analyzer messaging

Windows Server 2012 and later server operation systems contain a best practices analyzer (BPA) for file servers. If you have followed the correct online guidance to uninstall SMB1, running this BPA will return a contradictory warning message:

```
Title: The SMB 1.0 file sharing protocol should be enabled
Severity: Warning
Date: 3/25/2020 12:38:47 PM
Category: Configuration
Problem: The Server Message Block 1.0 (SMB 1.0) file sharing protocol is disabled on this file server.
Impact: SMB not in a default configuration, which could lead to less than optimal behavior.
Resolution: Use Registry Editor to enable the SMB 1.0 protocol.
```

You should ignore this specific BPA rule's guidance, it's deprecated. We repeat: don't enable SMB 1.0.

## Additional references

- Stop using SMB1

# SMB known issues

4/7/2020 • 2 minutes to read • Edit Online

The following topics describe some common troubleshooting issues that can occur when you use Server Message Block (SMB). These topics also provide possible solutions to those issues.

- TCP three-way handshake failure
- Negotiate, Session Setup, and Tree Connect Failures
- TCP connection is aborted during Validate Negotiate
- Slow files transfer speed
- High CPU usage issue on the SMB server
- Troubleshoot the Event ID 50 Error Message
- SMB Multichannel troubleshooting

# TCP three-way handshake failure during SMB connection

4/7/2020 • 2 minutes to read • Edit Online

When you analyze a network trace, you notice that there is a Transmission Control Protocol (TCP) three-way handshake failure that causes the SMB issue to occur. This article describes how to troubleshoot this situation.

## Troubleshooting

Generally, the cause is a local or infrastructure firewall that blocks the traffic. This issue can occur in either of the following scenarios.

## Scenario 1

The TCP SYN packet arrives on the SMB server, but the SMB server does not return a TCP SYN-ACK packet.

To troubleshoot this scenario, follow these steps.

**Step 1**

Run **netstat** or **Get-NetTcpConnection** to make sure that there is a listener on TCP port 445 that should be owned by the SYSTEM process.

```
netstat -ano | findstr :445
```

```
Get-NetTcpConnection -LocalPort 445
```

**Step 2**

Make sure that the Server service is started and running.

**Step 3**

Take a Windows Filtering Platform (WFP) capture to determine which rule or program is dropping the traffic. To do this, run the following command in a Command Prompt window:

```
netsh wfp capture start
```

Reproduce the issue, and then, run the following command:

```
netsh wfp capture stop
```

Run a scenario trace, and look for WFP drops in SMB traffic (on TCP port 445).

Optionally, you could remove the anti-virus programs because they are not always WFP-based.

**Step 4**

If Windows Firewall is enabled, enable firewall logging to determine whether it records a drop in traffic.

Make sure that the appropriate "File and Printer Sharing (SMB-In)" rules are enabled in **Windows Firewall with Advanced Security** > **Inbound Rules**.

> **NOTE**
>
> Depending on how your computer is set up, "Windows Firewall" might be called "Windows Defender Firewall."

## Scenario 2

The TCP SYN packet never arrives at the SMB server.

In this scenario, you have to investigate the devices along the network path. You may analyze network traces that are captured on each device to determine which device is blocking the traffic.

# Negotiate, Session Setup, and Tree Connect Failures

12/16/2020 • 2 minutes to read • Edit Online

This article describes how to troubleshoot the failures that occur during an SMB Negotiate, Session Setup, and Tree Connect request.

## Negotiate fails

The SMB server receives an SMB NEGOTIATE request from an SMB client. The connection times out and is reset after 60 seconds. There may be an ACK message after about 200 microseconds.

This problem is most often caused by antivirus program.

If you are using Windows Server 2008 R2, there are hotfixes for this problem. Make sure that the SMB client and the SMB server are up to date.

## Session Setup fails

The SMB server receives an SMB SESSION_SETUP request from a SMB client but failed to response.

If the fully qualified domain name (FQDN) or Network Basic Input/Output System (NetBIOS) name of the server is 'sed in the Universal Naming Convention (UNC) path, Windows will use Kerberos for authentication.

After the Negotiate response, there will be an attempt to get a Kerberos ticket for the Common Internet File System (CIFS) service principal name (SPN) of the server. Look at the Kerberos traffic on TCP port 88 to make sure that there are no Kerberos errors when the SMB client is gaining the token.

> **NOTE**
>
> The errors that occur during the Kerberos Pre-Authentication are OK. The errors that occur after the Kerberos Pre-Authentication (instances in which authentication does not work), are the errors that caused the SMB problem.

Additionally, make the following checks:

- Look at the security blob in the SMB SESSION_SETUP request to make sure the correct credentials are sent.
- Try to disable SMB server name hardening (**SmbServerNameHardeningLevel = 0**).
- Make sure that the SMB server has an SPN when it is accessed through a CNAME DNS record.
- Make sure that SMB signing is working. (This is especially important for older, third-party devices.)

## Tree Connect fails

Make sure that the user account credentials have both share and NT file system (NTFS) permissions to the folder.

The cause of common Tree Connect errors can be found in 3.3.5.7 Receiving an SMB2 TREE_CONNECT Request. The following are the solutions for two common status codes.

[STATUS_BAD_NETWORK_NAME]

Make sure that the share exists on the server, and that it is spelled correctly in the SMB client request.

[STATUS_ACCESS_DENIED]

Verify that the disk and folder that are used by the share exists and is accessible.

If you are using SMBv3 or later, check whether the server and the share require encryption, but the client doesn't support encryption. To do this, take the following actions:

- Check the server by running the following command.

  ```
  Get-SmbServerConfiguration | select Encrypt*
  ```

  If EncryptData and RejectUnencryptedAccess are true, the server requires encryption.

- Check the share by running the following command:

  ```
  Get-SmbShare | select name, EncryptData
  ```

  If EncryptData is true on the share, and RejectUnencryptedAccess is true on the server, encryption is required by the share

Follow these guidelines as you troubleshoot:

- Windows 8, Windows Server 2012, and later versions of Windows support client-side encryption (SMBv3 and later).
- Windows 7, Windows Server 2008 R2 and earlier versions of Windows do not support client-side encryption.
- Samba and third-party device may not support encryption. You may have to consult product documentation for more information.

## References

For more information, see the following articles.

3.3.5.4 Receiving an SMB2 NEGOTIATE Request

3.3.5.5 Receiving an SMB2 SESSION_SETUP Request

3.3.5.7 Receiving an SMB2 TREE_CONNECT Request

# TCP connection is aborted during Validate Negotiate

7/22/2020 • 2 minutes to read • Edit Online

In the network trace for the SMB issue, you notice that a TCP Reset abort occurred during the Validate Negotiate process. This article describes how to troubleshoot the situation.

## Cause

This issue can be caused by a failed negotiation validation. This typically occurs because a WAN accelerator modifies the original SMB NEGOTIATE packet.

Microsoft no longer allows modification of the Validate Negotiate packet for any reason. This is because this behavior creates a serious security risk.

The following requirements apply to the Validate Negotiate packet:

- The Validate Negotiate process uses the FSCTL_VALIDATE_NEGOTIATE_INFO command.
- The Validate Negotiate response must be signed. Otherwise, the connection is aborted.
- You should compare the FSCTL_VALIDATE_NEGOTIATE_INFO messages to the Negotiate messages to make sure that nothing was changed.

## Workaround

You can temporarily disable the Validate Negotiate process. To do this, locate the following registry subkey:

**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters**

Under the **Parameters** key, set **RequireSecureNegotiate** to **0**.

In Windows PowerShell, you can run the following command to set this value:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
RequireSecureNegotiate -Value 0 -Force
```

> **NOTE**
> The Validate Negotiate process cannot be disabled in Windows 10, Windows Server 2016, or later versions of Windows.

If either the client or server cannot support the Validate Negotiate command, you can work around this issue by setting SMB signing to be required. SMB signing is considered more secure than Validate Negotiate. However, there can also be performance degradation if signing is required.

## Reference

For more information, see the following articles:

3.3.5.15.12 Handling a Validate Negotiate Info Request

3.2.5.14.12 Handling a Validate Negotiate Info Response

# Slow SMB files transfer speed

7/22/2020 • 3 minutes to read • Edit Online

This article provides suggested troubleshooting procedures for slow file transfer speeds through SMB.

## Large file transfer is slow

If you observe slow transfers of large files, consider the following steps:

- Try the file copy command for unbuffered IO (**xcopy /J** or **robocopy /J**).
- Test the storage speed. This is because file copy speeds are limited by storage speed.
- File copies sometimes start fast and then slow down. Follow these guidelines to verify this situation:
  - This usually occurs when the initial copy is cached or buffered (either in memory or in the RAID controller's memory cache) and the cache runs out. This forces data to be written directly to disk (write-through). This is a slower process.
  - Use storage performance monitor counters to determine whether storage performance degrades over time. For more information, see Performance tuning for SMB file servers.
- Use RAMMap (SysInternals) to determine whether "Mapped File" usage in memory stops growing because of free memory exhaustion.
- Look for packet loss in the trace. This can cause throttling by the TCP congestion provider.
- For SMBv3 and later versions, make sure that SMB Multichannel is enabled and working.
- On the SMB client, enable large MTU in SMB, and disable bandwidth throttling. To do this, run the following command:

```
Set-SmbClientConfiguration -EnableBandwidthThrottling 0 -EnableLargeMtu 1
```

## Small file transfer is slow

Slow transfer of small files through SMB occurs most commonly if there are many files. This is an expected behavior.

During file transfer, file creation causes both high protocol overhead and high file system overhead. For large file transfers, these costs occur only one time. When a large number of small files are transferred, the cost is repetitive and causes slow transfers.

The following are technical details about this problem:

- SMB calls a create command to request that the file be created. Some code will check whether the file exists, and then create the file. Or some variation of the create command creates the actual file.
- Each create command generates activity on the file system.
- After the data is written, the file is closed.
- All some time, the process suffers from network latency and SMB server latency. This is because the SMB request is first translated to a file system command and then to the actual file system latency to complete

the operation.

- If any antivirus program is running, the transfer slows down even more. This is because the data is typically scanned one time by the packet sniffer and a second time when it is written to disk. In some scenarios, these actions are repeated thousands of time. You potentially observe speeds of less than 1 MB/s.

## Opening Office documents is slow

This problem generally occurs on a WAN connection. This is common and typically is caused by the manner in which Office apps (Microsoft Excel, in particular) access and read data.

We recommend that you make sure that the Office and SMB binaries are up-to-date, and then test by having leasing disabled on the SMB server. To do this, follow these steps:

1. Run the following PowerShell command in Windows 8 and Windows Server 2012 or later versions of Windows:

   ```
   Set-SmbServerConfiguration -EnableLeasing $false
   ```

   Or, run the following command in an elevated Command Prompt window:

   ```
   REG ADD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters /v DisableLeasing
   /t REG\_DWORD /d 1 /f
   ```

   > **NOTE**
   > After you set this registry key, SMB2 leases are no longer granted, but oplocks are still available. This setting is used primarily for troubleshooting.

2. Restart the file server or restart the **Server** service. To restart the service, run the following commands:

   ```
   NET STOP SERVER
   NET START SERVER
   ```

To avoid this issue, you can also replicate the file to a local file server. For more information, see aving Office documents to a network server is slow when using EFS.

# High CPU usage issue on the SMB server

4/7/2020 • 5 minutes to read • Edit Online

This article discusses how to troubleshoot the high CPU usage issue on the SMB server.

## High CPU usage because of storage performance issues

Storage performance issues can cause high CPU usage on SMB servers. Before you troubleshoot, make sure that the latest update rollup is installed on the SMB server to eliminate any known issues in srv2.sys.

In most cases, you will notice the issue of high CPU usage in the system process. Before you proceed, use Process Explorer to make sure that srv2.sys or ntfs.sys is consuming excessive CPU resources.

**Storage area network (SAN) scenario**

In aggregate levels, the overall SAN performance may appear to be fine. However, when you work with SMB issues, the individual request response time is what matters the most.

Generally, this issue can be caused by some form of command queuing in the SAN. You can use **Perfmon** to capture a **Microsoft-Windows-StorPort** tracing, and analyze it to accurately determine storage responsiveness.

**Disk IO latency**

Disk IO latency is a measure of the delay between the time that a disk IO request is created and completed.

The IO latency that is measured in Perfmon includes all the time that is spent in the hardware layers plus the time that is spent in the Microsoft Port Driver queue (Storport.sys for SCSI). If the running processes generate a large StorPort queue, the measured latency increases. This is because IO must wait before it is dispatched to the hardware layers.

In Perfmon, the following counters show physical disk latency:

- "Physical disk performance object" -> "Avg. Disk sec/Read counter" – This shows the average read latency.
- "Physical disk performance object" -> "Avg. Disk sec/Write counter" – This shows the average write latency.
- "Physical disk performance object" -> "Avg. Disk sec/Transfer counter" – This shows the combined averages for both reads and writes.

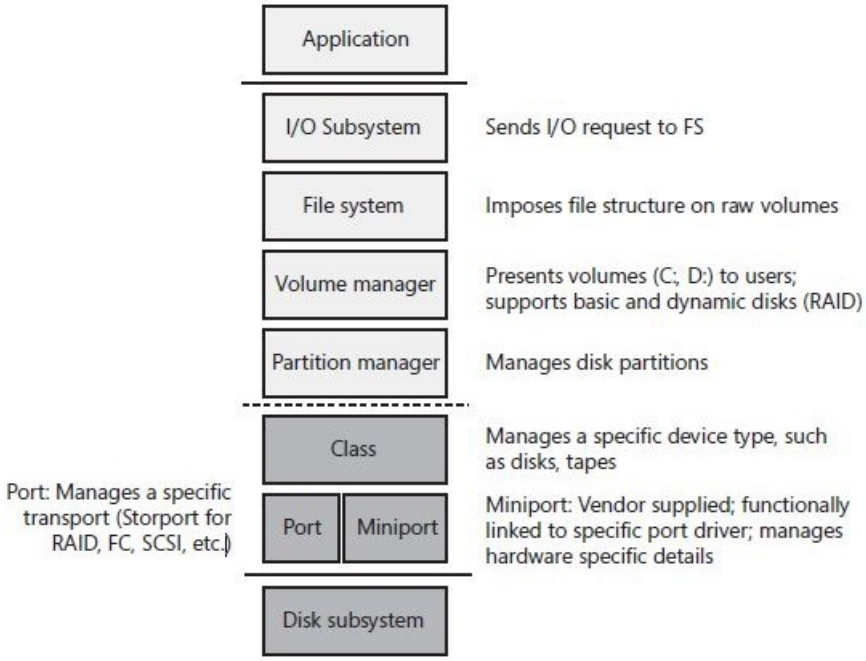
The "_Total" instance is an average of the latencies for all physical disks in the computer. Each of other instances represents an individual Physical Disk.

> **NOTE**
> Do not confuse these counters with Avg. Disk Transfers/sec. These are completely different counters.

**Windows Storage Stack follows**

This section gives a brief explanation on the Windows Storage Stack follows.

When an application creates an IO request, it sends the request to the Windows IO subsystem at the top of the stack. The IO then travels all the way down the stack to the hardware "Disk" subsystem. Then, the response travels all the way back up. During this process, each layer performs its function and then hands the IO to the next layer.




Perfmon does not create any performance data per second. Instead, it consumes data that is provided by other subsystems within Windows.

For the "physical disk performance object," the data is captured at the "Partition manager" level in the storage stack.

When we measure the counters that are mentioned in the previous section, we are measuring all the time that is spent by the request below the "Partition manager" level. When the IO request is sent by the partition manager down the stack, we time stamp it. When it returns, we time stamp it again and calculate the time difference. The time difference is the latency.

By doing this, we are accounting for the time that is spent in the following components:

- Class Driver - This manages the device type, such as disks, tapes, and so on.
- Port Driver - This manages the transport protocol, such as SCSI, FC, SATA, and so on.
- Device Miniport Driver - This is the device driver for the Storage Adapter. It is supplied by the manufacturer of the devices, such as Raid Controller, and FC HBA.
- Disk Subsystem - This includes everything that is below the Device Miniport Driver. This could be as simple as a cable that is connected to a single physical hard disk, or as complex as a Storage Area Network. If the issue is determined to be caused by this component, you can contact the hardware vendor for more information about troubleshooting.

**Disk queuing**

There is a limited amount of IO that a disk subsystem can accept at a given time. The excess IO gets queued until the disk can accept IO again. The time that IO spends in the queues below the "Partition manager" level is accounted for in the Perfmon physical disk latency measurements. As queues grow larger and IO must wait longer, the measured latency also grows.

There are multiple queues below the "Partition manager" level, as follows:

- Microsoft Port Driver Queue - SCSIport or Storport queue
- Manufacturer Supplied Device Driver Queue - OEM Device driver

- Hardware Queues – such as disk controller queue, SAN switches queue, array controller queue, and hard disk queue

We also account for the time that the hard disk spends actively servicing the IO and the travel time that is taken for the request to return to the "Partition manager" level to be marked as completed.

Finally, we have to pay special attention to the Port Driver Queue (for SCSI Storport.sys). The Port Driver is the last Microsoft component to touch an IO before we hand it off to the manufacturer-supplied Device Miniport Driver.

If the Device Miniport Driver can't accept any more IO because its queue or the hardware queues below it are saturated, we will start accumulating IO on the Port Driver Queue. The size of the Microsoft Port Driver queue is limited only by the available system memory (RAM), and it can grow very large. This causes large measured latency.

## High CPU caused by enumerating folders

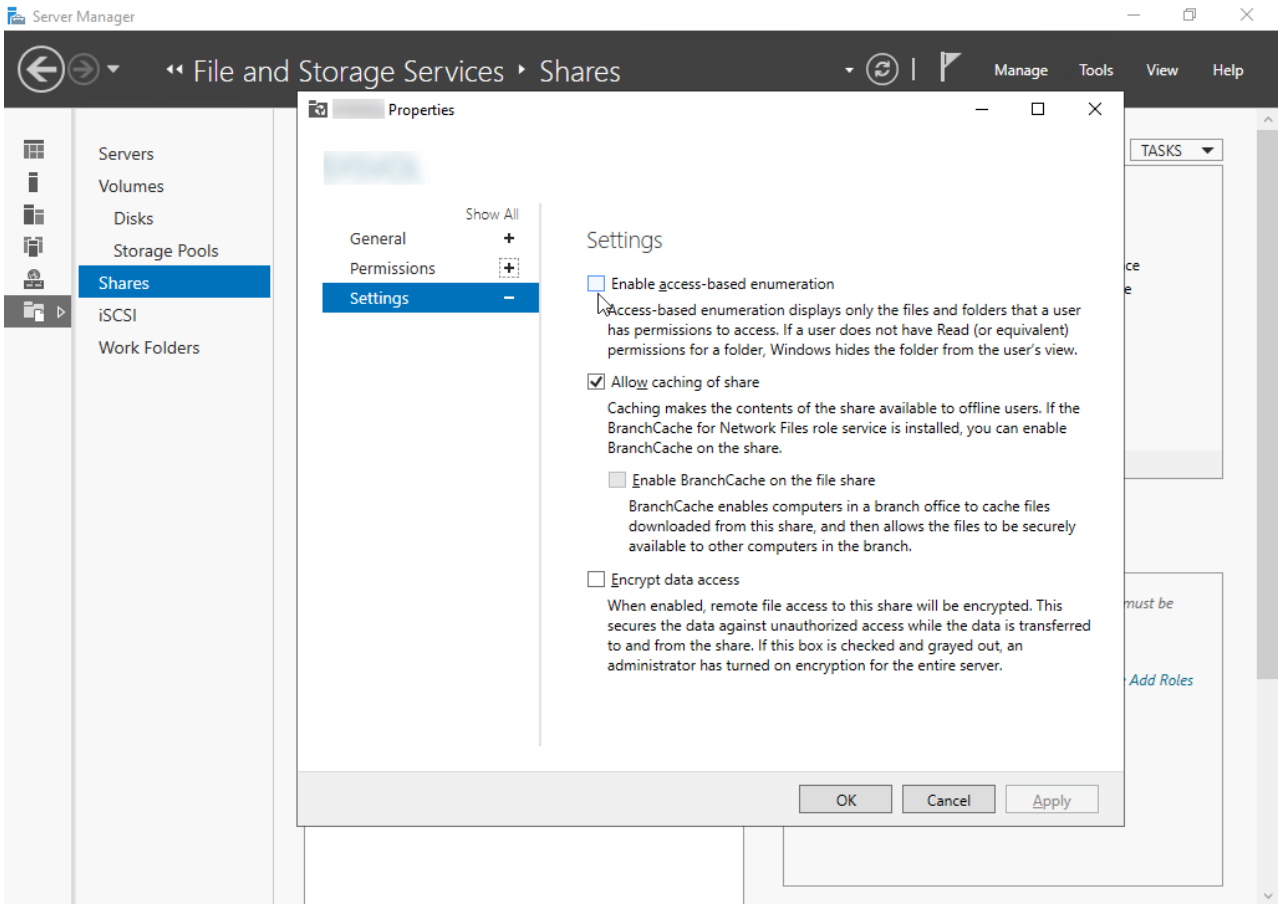
To troubleshoot this issue, disable the Access Based Enumeration (ABE) feature.

To determine which SMB shares have ABE enabled, run the following PowerShell command,

```
Get-SmbShare | Select Name, FolderEnumerationMode
```

Unrestricted = ABE disabled.
AccessBase = ABE enabled.

You can enable ABE in **Server Manager**. Navigatie to **File and Storage Services** > **Shares**, right-click the share, select **Properties**, go to **Settings** and then select **Enable access-based enumeration**.




Also, you can reduce **ABELevel** to a lower level (1 or 2) to improve performance.

You can check disk performance when enumeration is slow by opening the folder locally through a console or an

RDP session.

# Troubleshoot the Event ID 50 Error Message

12/16/2020 • 5 minutes to read • Edit Online

## Symptoms

When information is being written to the physical disk, the following two event messages may be logged in the system event log:

```
Event ID: 50
Event Type: Warning
Event Source: Ftdisk
Description: {Lost Delayed-Write Data} The system was attempting to transfer file data from buffers to
\Device\HarddiskVolume4. The write operation failed, and only some of the data may have been written to the
file.
Data:
0000: 00 00 04 00 02 00 56 00
0008: 00 00 00 00 32 00 04 80
0010: 00 00 00 00 00 00 00 00
0018: 00 00 00 00 00 00 00 00
0020: 00 00 00 00 00 00 00 00
0028: 11 00 00 80
```

```
Event ID: 26
Event Type: Information
Event Source: Application Popup
Description: Windows - Delayed Write Failed : Windows was unable to save all the data for the file
\Device\HarddiskVolume4\Program Files\Microsoft SQL Server\MSSQL$INSTANCETWO\LOG\ERRORLOG. The data has been
lost. This error may be caused by a failure of your computer hardware or network connection.

Please try to save this file elsewhere.
```

These event ID messages mean exactly the same thing and are generated for the same reasons. For the purposes of this article, only the event ID 50 message is described.

> **NOTE**
> The device and path in the description and the specific hexadecimal data will vary.

## More Information

An event ID 50 message is logged if a generic error occurs when Windows is trying to write information to the disk. This error occurs when Windows is trying to commit data from the file system Cache Manager (not hardware level cache) to the physical disk. This behavior is part of the memory management of Windows. For example, if a program sends a write request, the write request is cached by Cache Manager and the program is told the write is completed successfully. At a later point in time, Cache Manager tries to lazy write the data to the physical disk. When Cache Manager tries to commit the data to disk, an error occurs writing the data, and the data is flushed from the cache and discarded. Write-back caching improves system performance, but data loss and volume integrity loss can occur as a result of lost delayed-write failures.

It is important to remember that not all I/O is buffered I/O by Cache Manager. Programs can set a FILE_FLAG_NO_BUFFERING flag that bypasses Cache Manager. When SQL performs critical writes to a database, this flag is set to guarantee that the transaction is completed directly to disk. For example, non-critical writes to log

files perform buffered I/O to improve overall performance. An event ID 50 message never results from non-buffered I/O.

There are several different sources for an event ID 50 message. For example, an event ID 50 message logged from a MRxSmb source occurs if there is a network connectivity problem with the redirector. To avoid performing incorrect troubleshooting steps, make sure to review the event ID 50 message to confirm that it refers to a disk I/O issue and that this article applies.

An event ID 50 message is similar to an event ID 9 and an event ID 11 message. Although the error is not as serious as the error indicated by the event ID 9 and an event ID 11 message, you can use the same troubleshooting techniques for a event ID 50 message as you do for an event ID 9 and an event ID 11 message. However, remember that anything in the stack can cause lost-delay writes, such as filter drivers and mini-port drivers.

You can use the binary data that is associated with any accompanying "DISK" error (indicated by an event ID 9, 11, 51 error message or other messages) to help you in identifying the problem.

**How to Decode the Data Section of an Event ID 50 Event Message**

When you decode the data section in the example of an event ID 50 message that is included in the "Summary" section, you see that the attempt to perform a write operation failed because the device was busy and the data was lost. This section describes how to decode this event ID 50 message.

The following table describes what each offset of this message represents:

| OFFSETLENGTHVALUES | LENGTH | VALUES |
|---|---|---|
| 0x00 | 2 | Not Used |
| 0x02 | 2 | Dump Data Size = 0x0004 |
| 0x04 | 2 | Number of Strings = 0x0002 |
| 0x06 | 2 | Offset to the strings |
| 0x08 | 2 | Event Category |
| 0x0c | 4 | NTSTATUS Error Code = 0x80040032 = IO_LOST_DELAYED_WRITE |
| 0x10 | 8 | Not Used |
| 0x18 | 8 | Not Used |
| 0x20 | 8 | Not Used |
| 0x28 | 4 | NT Status error code |

**Key Sections to Decode**

### The Error Code

In the example in the "Summary" section, the error code is listed in the second line. This line starts with "0008:" and it includes the last four bytes in this line:0008: 00 00 00 00 32 00 04 80 In this case, the error code is 0x80040032. The following code is the code for error 50, and it is the same for all event ID 50 messages: IO_LOST_DELAYED_WRITEWARNINGNote When you are converting the hexadecimal data in the event ID message to the status code, remember that the values are represented in the little-endian format.

### The Target Disk

You can identify the disk that the write was being tried to by using the symbolic link that is listed to the drive in the "Description" section of the event ID message, for example: \Device\HarddiskVolume4.

### The Final Status Code

The final status code is the most important piece of information in an event ID 50 message. This is the error code that is return when the I/O request was made, and it is the key source of information. In the example in the "Summary" section, the final status code is listed at 0x28, the sixth line, that starts with "0028:" and includes the only four octets in this line:

```
0028: 11 00 00 80
```

In this case, the final status equals 0x80000011.This status code maps to STATUS_DEVICE_BUSY and implies that the device is currently busy.

> **NOTE**
> When you are converting the hexadecimal data in the event ID 50 message to the status code, remember that the values are represented in the little-endian format. Because the status code is the only piece of information that you are interested in, it may be easier to view the data in WORDS format instead of BYTES. If you do so, the bytes will be in the correct format and the data may be easier to interpret quickly.

To do so, click **Words** in the **Event Properties** window. In the Data Words view, the example in the "Symptoms" section would read as follows: Data:

```
() Bytes (.)
Words 0000: 00040000 00560002 00000000 80040032 0010: 00000000 00000000 00000000 00000000 0020: 00000000
00000000 80000011
```

To obtain a list of Windows NT status codes, see NTSTATUS.H in the Windows Software Developers Kit (SDK).

# SMB Multichannel troubleshooting

7/22/2020 • 2 minutes to read • Edit Online

This article describes how to troubleshoot issues that are related to SMB Multichannel.

## Check the network interface status

Make sure that the binding for the network interface is set to **True** on the SMB client (MS_client) and SMB server (MS_server). When you run the following command, the output should show **True** under **Enabled** for both network interfaces:

```
Get-NetAdapterBinding -ComponentID ms_server,ms_msclient
```

After that, make sure the network interface is listed in the output of the following commands:

```
Get-SmbServerNetworkInterface
```

```
Get-SmbClientNetworkInterface
```

You can also run the **Get-NetAdapter** command to view the interface index to verify the result. The interface index shows all the active SMB adapters that are actively bound to the appropriate interface.

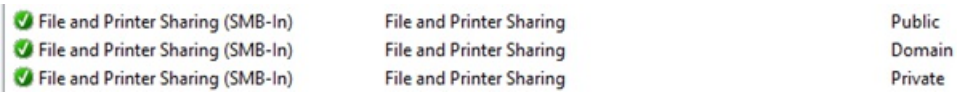
## Check the firewall

If there is only a link-local IP address, and no publicly routable address, the network profile is likely set to **Public**. This means that SMB is blocked at the firewall by default.

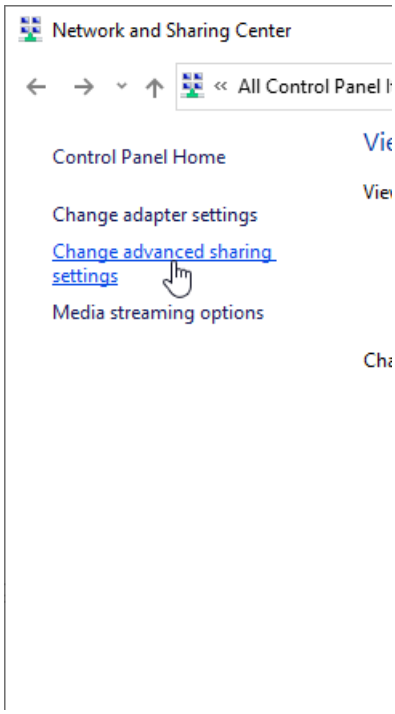
The following command reveals which connection profile is being used. You can also use the Network and Sharing Center to retrieve this information.

**Get-NetConnectionProfile**

Under the **File and Printer Sharing** group, check the firewall inbound rules to make sure that "SMB-In" is enabled for the correct profile.




You can also enable **File and Printer Sharing** in the **Network and Sharing Center** window. To do this, select **Change advanced sharing settings** in the menu on the left, and then select **Turn on file and printer sharing** for the profile. This option enables the File and Printer Sharing firewall rules.




## Capture client and server sided traffic for troubleshooting

You need the SMB connection tracing information that starts from the TCP three-way handshake. We recommend that you close all applications (especially Windows Explorer) before you start the capture. Restart the **Workstation** service on the SMB client, start the packet capture, and then reproduce the issue.

Make sure that the SMBv3.*x* connection is being negotiated, and that nothing in between the server and the client is affecting dialect negotiation. SMBv2 and earlier versions don't support multichannel.

Look for the NETWORK_INTERFACE_INFO packets. This is where the SMB client requests a list of adapters from the SMB server. If these packets aren't exchanged, multichannel doesn't work.

The server responds by returning a list of valid network interfaces. Then, the SMB client adds those to the list of available adapters for multichannel. At this point, multichannel should start and, at least, try to start the connection.

For more information, see the following articles:

- 3.2.4.20.10 Application Requests Querying Server's Network Interfaces
- 2.2.32.5 NETWORK_INTERFACE_INFO Response
- 3.2.5.14.11 Handling a Network Interfaces Response

In the following scenarios, an adapter cannot be used:

- There is a routing issue on the client. This is typically caused by an incorrect routing table that forces traffic over the wrong interface.
- Multichannel constraints have been set. For more information, see New-SmbMultichannelConstraint.
- Something blocked the network interface request and response packets.
- The client and server can't communicate over the extra network interface. For example, the TCP three-way handshake failed, the connection is blocked by a firewall, session setup failed, and so on.

If the adapter and its IPv6 address are on the list that is sent by the server, the next step is to see whether communications are tried over that interface. Filter the trace by the link-local address and SMB traffic, and look for a connection attempt. If this is a NetConnection trace, you can also examine Windows Filtering Platform (WFP) events to see whether the connection is being blocked.

# File Server Resource Manager (FSRM) overview

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server (Semi-Annual Channel),

File Server Resource Manager (FSRM) is a role service in Windows Server that enables you to manage and classify data stored on file servers. You can use File Server Resource Manager to automatically classify files, perform tasks based on these classifications, set quotas on folders, and create reports monitoring storage usage.

It's a small point, but we also added the ability to disable change journals in Windows Server, version 1803.

## Features

File Server Resource Manager includes the following features:

- Quota management allows you to limit the space that is allowed for a volume or folder, and they can be automatically applied to new folders that are created on a volume. You can also define quota templates that can be applied to new volumes or folders.
- File Classification Infrastructure provides insight into your data by automating classification processes so that you can manage your data more effectively. You can classify files and apply policies based on this classification. Example policies include dynamic access control for restricting access to files, file encryption, and file expiration. Files can be classified automatically by using file classification rules or manually by modifying the properties of a selected file or folder.
- File Management Tasks enables you to apply a conditional policy or action to files based on their classification. The conditions of a file management task include the file location, the classification properties, the date the file was created, the last modified date of the file, or the last time the file was accessed. The actions that a file management task can take include the ability to expire files, encrypt files, or run a custom command.
- File screening management helps you control the types of files that user can store on a file server. You can limit the extension that can be stored on your shared files. For example, you can create a file screen that does not allow files with an MP3 extension to be stored in personal shared folders on a file server.
- Storage reports help you identify trends in disk usage and how your data is classified. You can also monitor a selected group of users for attempts to save unauthorized files.

The features included with File Server Resource Manager can be configured and managed by using the File Server Resource Manager app or by using Windows PowerShell.

> **IMPORTANT**
> File Server Resource Manager supports volumes formatted with the NTFS file system only. The Resilient File System isn't supported.

## Practical applications

Some practical applications for File Server Resource Manager include:

- Use File Classification Infrastructure with the Dynamic Access Control scenario to create a policy that grants access to files and folders based on the way files are classified on the file server.
- Create a file classification rule that tags any file that contains at least 10 social security numbers as having

personally identifiable information.

- Expire any file that has not been modified in the last 10 years.
- Create a 200 megabyte quota for each user's home directory and notify them when they are using 180 megabytes.
- Do not allow any music files to be stored in personal shared folders.
- Schedule a report that runs every Sunday night at midnight that generates a list of the most recently accessed files from the previous two days. This can help you determine the weekend storage activity and plan your server downtime accordingly.

## What's new - prevent FSRM from creating change journals

Starting with Windows Server, version 1803, you can now prevent the File Server Resource Manager service from creating a change journal (also known as a USN journal) on volumes when the service starts. This can conserve a little bit of space on each volume, but will disable real-time file classification.

For older new features, see What's New in File Server Resource Manager.

To prevent File Server Resource Manager from creating a change journal on some or all volumes when the service starts, use the following steps:

1. Stop the SRMSVC service. For example, open a PowerShell session as an administrator and enter `Stop-Service SrmSvc`.
2. Delete the USN journal for the volumes you want to conserve space on by using the fsutil command:

   ```
   fsutil usn deletejournal /d <VolumeName>
   ```

   For example: `fsutil usn deletejournal /d c:`
3. Open Registry Editor, for example, by typing `regedit` in the same PowerShell session.
4. Navigate to the following key:
   **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SrmSvc\Settings**
5. To optionally skip change journal creation for the entire server (skip this step if you want to disable it only on specific volumes):
   a. Right-click the **Settings** key and then select **New** > **DWORD (32-bit) Value**.
   b. Name the value `SkipUSNCreationForSystem`.
   c. Set the value to **1** (in hexidecimal).
6. To optionally skip change journal creation for specific volumes:
   a. Get the volume paths you want to skip by using the `fsutil volume list` command or the following PowerShell command:

      ```
      Get-Volume | Format-Table DriveLetter,FileSystemLabel,Path
      ```

      Here's an example output:

```
DriveLetter FileSystemLabel Path
----------- --------------- ----
            System Reserved \\?\Volume{8d3c9e8a-0000-0000-0000-100000000000}\
C                           \\?\Volume{8d3c9e8a-0000-0000-0000-501f00000000}\
```

b. Back in Registry Editor, right-click the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SrmSvc\Settings** key and then select **New** > **Multi-String Value**.

c. Name the value `SkipUSNCreationForVolumes`.

d. Enter the path of each volume on which you skip creating a change journal, placing each path on a separate line. For example:

```
\\?\Volume{8d3c9e8a-0000-0000-0000-100000000000}\
\\?\Volume{8d3c9e8a-0000-0000-0000-501f00000000}\
```

> **NOTE**
>
> Registry Editor might tell you that it removed empty strings, displaying this warning that you can safely disregard: *Data of type REG_MULTI_SZ cannot contain empty strings. Registry Editor will remove all empty strings found.*

7. Start the SRMSVC service. For example, in a PowerShell session enter `Start-Service SrmSvc`.

## Additional References

- Dynamic Access Control

# Checklist: Apply a Quota to a volume or folder

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server (Semi-Annual Channel)

1. Configure e-mail settings if you plan to send threshold notifications or storage reports by e-mail. Configure E-Mail Notifications
2. Assess storage requirements on the volume or folder. You can use reports on the **Storage Reports Management** node to provide data. (For example, run a Files by Owner report on demand to identify users who use large amounts of disk space.) Generate Reports on Demand
3. Review available pre-configured quota templates. (In **Quota Management**, click the **Quota Templates** node.) Edit Quota Template Properties
   -Or-
   Create a new quota template to enforce a storage policy in your organization. Create a Quota Template
4. Create a quota based on the template on the volume or folder. Create a Quota
   -Or-
   Create an auto apply quota to automatically generate quotas for subfolders on the volume or folder. Create an Auto Apply Quota
5. Schedule a report task that contains a Quota Usage report to monitor quota usage periodically. Schedule a Set of Reports

**NOTE**

If you want to screen files on a volume or folder, see Checklist: Apply a File Screen to a Volume or Folder.

# Checklist - Apply a file screen to a volume or folder

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

To apply a file screen to a volume or folder, use the following list:

1. Configure e-mail settings if you plan to send file screening notifications or storage reports by e-mail by following the instructions in Configure E-Mail Notifications.
2. Enable recording of file screening events in the auditing database if you plan to generate File Screening Audit reports. Configure File Screen Audit
3. Assess stored file types that are candidates for screening rules. You can use reports at the **Storage Reports Management** node to provide data. (For example, run a Files by File Group report or a Large Files report on demand to identify files that occupy large amounts of disk space.) Generate Reports on Demand
4. Review the preconfigured file groups, or create a new file group to enforce a specific screening policy in your organization. Define File Groups for Screening
5. Review the properties of available file screen templates. (In **File Screening Management**, click the **File Screen Templates** node.) Edit File Screen Template Properties
   -Or-
   Create a new file screen template to enforce a storage policy in your organization. Create a File Screen Template
6. Create a file screen based on the template on a volume or folder. Create a File Screen
7. Configure file screen exceptions in subfolders of the volume or folder. Create a File Screen Exception
8. Schedule a report task containing a File Screening Audit report to monitor screening activity periodically. Schedule a Set of Reports

> **NOTE**
> To limit storage on a volume or folder, see Checklist: Apply a Quota to a Volume or Folder

# Setting File Server Resource Manager Options

11/2/2020 • 2 minutes to read • Edit Online

> Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

The general File Server Resource Manager options can be set in the **File Server Resource Manager Options** dialog box. These settings are used throughout the nodes, and some of them can be modified when you work with quotas, screen files, or generate storage reports.

This section includes the following topics:

- Configure E-Mail Notifications
- Configure Notification Limits
- Configure Storage Reports
- Configure File Screen Audit

# Configure E-Mail Notifications

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

When you create quotas and file screens, you have the option of sending e-mail notifications to users when their quota limit is approaching or after they have attempted to save files that have been blocked. When you generate storage reports, you have the option of sending the reports to specific recipients by e-mail. If you want to routinely notify certain administrators about quota and file screening events, or send storage reports, you can configure one or more default recipients.

To send these notifications and storage reports, you must specify the SMTP server to be used for forwarding the e-mail messages.

## To configure e-mail options

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. On the **E-mail Notifications** tab, under **SMTP server name or IP address**, type the host name or the IP address of the SMTP server that will forward e-mail notifications and storage reports.
3. If you want to routinely notify certain administrators about quota or file screening events or e-mail storage reports, under **Default administrator recipients**, type each e-mail address.

   Use the format *account@domain*. Use semicolons to separate multiple accounts.
4. To specify a different "From" address for e-mail notifications and storage reports sent from File Server Resource Manager, under the **Default "From" e-mail address**, type the e-mail address that you want to appear in your message.
5. To test your settings, click **Send Test E-mail**.
6. Click **OK**.

## Additional References

- Setting File Server Resource Manager Options

# Configure Notification Limits

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

To reduce the number of notifications that accumulate for repeatedly exceeding a quota threshold or attempting to save an unauthorized file, File Server Resource Manager applies time limits to the following notification types:

- E-mail
- Event log
- Command
- Report

Each limit specifies a period of time before another configured notification of the same type is generated for an identical issue.

A default 60-minute limit is set for each notification type, but you can change these limits. The limit applies to all the notifications of a given type, whether they are generated by quota thresholds or by file screening events.

## To specify a standard notification limit for each notification type

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. On the **Notification Limits** tab, enter a value in minutes for each notification type that is shown.
3. Click **OK**.

> **NOTE**
> To customize time limits that are associated with notifications for a specific quota or file screen, you can use the File Server Resource Manager command-line tools **Dirquota.exe** and **Filescrn.exe**, or use the File Server Resource Manager cmdlets.

## Additional References

- Setting File Server Resource Manager Options
- Command-Line Tools

# Configure Storage Reports

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

You can configure the default parameters for storage reports. These default parameters are used for the incident reports that are generated when a quota or file screening event occurs. They are also used for scheduled and on-demand reports, and you can override the default parameters when you define the specific properties of these reports.

> **IMPORTANT**
> When you change the default parameters for a type of report, changes affect all incident reports and any existing scheduled report tasks that use the defaults.

## To configure the default parameters for Storage Reports

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. On the **Storage Reports** tab, under **Configure default parameters**, select the type of report that you want to modify.
3. Click **Edit Parameters**.
4. Depending on the type of report that you select, different report parameters will be available for editing. Perform all necessary modifications, and then click **OK** to save them as the default parameters for that type of report.
5. Repeat steps 2 through 4 for each type of report that you want to edit.
6. To see a list of the default parameters for all reports, click **Review Reports**. Then click **Close**.
7. Click **OK**.

## Additional References

- Setting File Server Resource Manager Options
- Storage Reports Management

# Configure File Screen Audit

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

By using File Server Resource Manager, you can record file screening activity in an auditing database. The information saved in this database is used to generate the File Screening Audit report.

**IMPORTANT**

If the **Record file screening activity in the auditing database** check box is cleared, the File Screening Audit Reports will not contain any information.

## To configure file screen audit

1. In the console tree, right-click **File Server Resource Manager**, and then click **Configure Options**. The **File Server Resource Manager Options** dialog box opens.
2. On the **File Screen Audit** tab, select the **Record file screening activity in the auditing database** check box.
3. Click **OK**. All file screening activity will now be stored in the auditing database, and it can be viewed by running a File Screening Audit report.

## Additional References

- Setting File Server Resource Manager Options
- Storage Reports Management

# Quota Management

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

On the **Quota Management** node of the File Server Resource Manager Microsoft® Management Console (MMC) snap-in, you can perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder, and generate notifications when the quota limits are approached or exceeded.
- Generate auto apply quotas that apply to all existing subfolders in a volume or folder and to any subfolders that are created in the future.
- Define quota templates that can be easily applied to new volumes or folders and then used across an organization.

For example, you can:

- Place a 200 megabyte (MB) limit on users' personal server folders, with an email notification sent to you and the user when 180 MB of storage has been exceeded.
- Set a flexible 500 MB quota on a group's shared folder. When this storage limit is reached, all users in the group are notified by e-mail that the storage quota has been temporarily extended to 520 MB so that they can delete unnecessary files and comply with the preset 500 MB quota policy.
- Receive a notification when a temporary folder reaches 2 gigabytes (GB) of usage, yet not limit that folder's quota because it is necessary for a service running on your server.

This section includes the following topics:

- Create a Quota
- Create an Auto Apply Quota
- Create a Quota Template
- Edit Quota Template Properties
- Edit Auto Apply Quota Properties

> **NOTE**
> To set e-mail notifications and reporting capabilities, you must first configure the general File Server Resource Manager options.

## Additional References

- Setting File Server Resource Manager Options

# Create a Quota

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Quotas can be created from a template or with custom properties. The following procedure describes how to create a quota that is based on a template (recommended). If you need to create a quota with custom properties, you can save these properties as a template to re-use at a later date.

When you create a quota, you choose a quota path, which is a volume or folder that the storage limit applies to. On a given quota path, you can use a template to create one of the following types of quota:

- A single quota that limits the space for an entire volume or folder.
- An auto apply quota, which assigns the quota template to a folder or volume. Quotas based on this template are automatically generated and applied to all subfolders. For more information about creating auto apply quotas, see Create an Auto Apply Quota.

> **NOTE**
> By creating quotas exclusively from templates, you can centrally manage your quotas by updating the templates instead of the individual quotas. Then, you can apply changes to all quotas based on the modified template. This feature simplifies the implementation of storage policy changes by providing one central point where all updates can be made.

## To create a quota that is based on a template

1. In **Quota Management**, click the **Quota Templates** node.
2. In the Results pane, select the template on which you will base your new quota.
3. Right-click the template and click **Create Quota from Template** (or select **Create Quota from Template** from the **Actions** pane). This opens the **Create Quota** dialog box with the summary properties of the quota template displayed.
4. Under **Quota path**, type or browse to the folder that the quota will apply to.
5. Click the **Create quota on path** option. Note that the quota properties will apply to the entire folder.

   > **NOTE**
   > To create an auto apply quota, click the **Auto apply template and create quotas on existing and new subfolders** option. For more information about auto apply quotas, see Create an Auto Apply Quota

6. Under **Derive properties from this quota template**, the template you used in step 2 to create your new quota is pre-selected (or you can select another template from the list). Note that the template's properties are displayed under **Summary of quota properties**.
7. Click **Create**.

## Additional References

- Quota Management
- Create an Auto Apply Quota
- Create a Quota Template

# Create an Auto Apply Quota

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

By using auto apply quotas, you can assign a quota template to a parent volume or folder. Then File Server Resource Manager automatically generates quotas that are based on that template. Quotas are generated for each of the existing subfolders and for subfolders that you create in the future.

For example, you can define an auto apply quota for subfolders that are created on demand, for roaming profile users, or for new users. Every time a subfolder is created, a new quota entry is automatically generated by using the template from the parent folder. These automatically generated quota entries can then be viewed as individual quotas under the **Quotas** node. Each quota entry can be maintained separately.

## To create an Auto Apply Quota

1. In **Quota Management**, click the **Quotas** node.
2. Right-click **Quotas**, and then click **Create Quota** (or select **Create Quota** from the **Actions** pane). This opens the **Create Quota** dialog box.
3. Under **Quota path**, type the name of or browse to the parent folder that the quota profile will apply to. The auto apply quota will be applied to each of the subfolders (current and future) in this folder.
4. Click **Auto apply template and create quotas on existing and new subfolders**.
5. Under **Derive properties from this quota template**, select the quota template that you want to apply from the drop-down list. Note that each template's properties are displayed under **Summary of quota properties**.
6. Click **Create**.

> **NOTE**
> You can verify all automatically generated quotas by selecting the **Quotas** node and then selecting **Refresh**. An individual quota for each subfolder and the auto apply quota profile in the parent volume or folder are listed.

## Additional References

- Quota Management
- Edit Auto Apply Quota Properties

# Create a Quota Template

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

A *quota template* defines a space limit, the type of quota (hard or soft) and optionally, a set of notifications that will be generated automatically when quota usage reaches defined threshold levels.

By creating quotas exclusively from templates, you can centrally manage your quotas by updating the templates instead of replicating changes in each quota. This feature simplifies the implementation of storage policy changes by providing one central point where you can make all updates.

## To create a Quota Template

1. In **Quota Management**, click the **Quota Templates** node.
2. Right-click **Quota Templates**, and then click **Create Quota Template** (or select **Create Quota Template** from the **Actions** pane). This opens the **Create Quota Template** dialog box.
3. If you want to copy the properties of an existing template to use as a base for your new template, select a template from the **Copy properties from quota template** drop-down list. Then click **Copy**.

   Whether you have chosen to use the properties of an existing template or you are creating a new template, modify or set the following values on the **Settings** tab:
4. In the **Template Name** text box, enter a name for the new template.
5. In the **Label** text box, enter an optional descriptive label that will appear next to any quotas derived from the template.
6. Under **Space Limit**:
   - In the **Limit** text box, enter a number and choose a unit (KB, MB, GB, or TB) to specify the space limit for the quota.
   - Click the **Hard quota** or **Soft quota** option. (A hard quota prevents users from saving files after the space limit is reached and generates notifications when the volume of data reaches each configured threshold. A soft quota does not enforce the quota limit, but it generates all configured notifications.)
7. You can configure one or more optional threshold notifications for your quota template, as described in the procedure that follows. After you have selected all the quota template properties that you want to use, click **OK** to save the template.

## Setting optional notification thresholds

When storage in a volume or folder reaches a threshold level that you define, File Server Resource Manager can send e-mail messages to administrators or specific users, log an event, execute a command or a script, or generate reports. You can configure more than one type of notification for each threshold, and you can define multiple thresholds for any quota (or quota template). By default, no notifications are generated.

For example, you could configure thresholds to send an e-mail message to the administrator and the users who would be interested to know when a folder reaches 85 percent of its quota limit, and then send another notification when the quota limit is reached. Additionally, you might want to run a script that uses the

**dirquota.exe** command to raise the quota limit automatically when a threshold is reached.

> **IMPORTANT**
> To send e-mail notifications and configure the storage reports with parameters that are appropriate for your server environment, you must first set the general File Server Resource Manager options. For more information, see Setting File Server Resource Manager Options

**To configure notifications that File Server Resource Manager will generate at a quota threshold**

1. In the **Create Quota Template** dialog box, under **Notification thresholds**, click **Add**. The **Add Threshold** dialog box appears.
2. To set a quota limit percentage that will generate a notification:

   In the **Generate notifications when usage reaches (%)** text box, enter a percentage of the quota limit for the notification threshold. (The default percentage for the first notification threshold is 85 percent.)
3. To configure e-mail notifications:

   On the **E-mail Message** tab, set the following options:

   - To notify administrators when a threshold is reached, select the **Send e-mail to the following administrators** check box, and then enter the names of the administrative accounts that will receive the notifications. Use the format *account@domain*, and use semicolons to separate multiple accounts.
   - To send e-mail to the person who saved the file that reached the quota threshold, select the **Send e-mail to the user who exceeded the threshold** check box.
   - To configure the message, edit the default subject line and message body that are provided. The text that is in brackets inserts variable information about the quota event that caused the notification. For example, the **[Source Io Owner]** variable inserts the name of the user who saved the file that reached the quota threshold. To insert additional variables in the text, click **Insert Variable**.
   - To configure additional headers (including From, Cc, Bcc, and Reply-to), click **Additional E-mail Headers**.
4. To log an event:

   On the **Event Log** tab, select the **Send warning to event log** check box, and edit the default log entry.
5. To run a command or script:

   On the **Command** tab, select the **Run this command or script** check box. Then type the command, or click **Browse** to search for the location where the script is stored. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.
6. To generate one or more storage reports:

   On the **Report** tab, select the **Generate reports** check box, and then select which reports to generate. (You can choose one or more administrative e-mail recipients for the report or e-mail the report to the user who reached the threshold.)

   The report is saved in the default location for incident reports, which you can modify in the **File Server Resource Manager Options** dialog box.
7. Click **OK** to save your notification threshold.
8. Repeat these steps if you want to configure additional notification thresholds for the quota template.

## Additional References

- Quota Management
- Setting File Server Resource Manager Options
- Edit Quota Template Properties
- Command-Line Tools

# Edit Quota Template Properties

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

When you make changes to a quota template, you have the option of extending those changes to quotas that were created from the original quota template. You can choose to modify only those quotas that still match the original template or all quotas that were derived from the original template, regardless of any modifications that were made to the quotas since they were created. This feature simplifies the process of updating the properties of your quotas by providing one central point where you can make all the changes.

> **NOTE**
> If you choose to apply the changes to all quotas that were derived from the original template, you will overwrite any custom quota properties that you created.

## To edit Quota Template Properties

1. In **Quota Templates**, select the template that you want to modify.
2. Right-click the quota template, and then click **Edit Template Properties** (or in the **Actions** pane, under **Selected Quota Templates,** select **Edit Template Properties**). This opens the **Quota Template Properties** dialog box.
3. Perform all necessary changes. The settings and notification options are identical to those that you can set when you create a quota template. Optionally, you can copy the properties from a different template and modify them for this one.
4. When you are finished editing the template properties, click **OK**. This will open the **Update Quotas Derived from Template** dialog box.
5. Select the type of update that you want to apply:
   - If you have quotas that have been modified since they were created with the original template, and you do not want to change them, select **Apply template only to derived quotas that match the original template**. This option will update only those quotas that have not been edited since they were created with the original template.
   - If you want to modify all existing quotas that were created from the original template, select **Apply template to all derived quotas**.
   - If you want to keep the existing quotas unchanged, select **Do not apply template to derived quotas**.
6. Click **OK**.

## Additional References

- Quota Management
- Create a Quota Template

# Edit Auto Apply Quota Properties

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

When you make changes to an auto apply quota, you have the option of extending those changes to existing quotas in the auto apply quota path. You can choose to modify only those quotas that still match the original auto apply quota or all quotas in the auto apply quota path, regardless of any modifications that were made to the quotas since they were created. This feature simplifies the process of updating the properties of quotas that were derived from an auto apply quota by providing one central point where you can make all the changes.

> **NOTE**
> If you choose to apply the changes to all quotas in the auto apply quota path, you will overwrite any custom quota properties that you have created.

## To edit an Auto Apply Quota

1. In **Quotas**, select the auto apply quota that you want to modify. You can filter the quotas to show only auto apply quotas.
2. Right-click the quota entry, and then click **Edit Quota Properties** (or in the **Actions** pane, under **Selected Quotas,** select **Edit Quota Properties**). This opens the **Edit Auto Apply Quota** dialog box.
3. Under **Derive properties from this quota template**, select the quota template that you want to apply. You can review the properties of each quota template in the summary list box.
4. Click **OK**. This will open the **Update Quotas Derived from Auto Apply Quota** dialog box.
5. Select the type of update that you want to apply:
   - If you have quotas that have been modified since they were automatically generated, and you do not want to change them, select **Apply auto apply quota only to derived quotas that match the original auto apply quota**. This option will update only those quotas in the auto apply quota path that have not been edited since they were automatically generated.
   - If you want to modify all existing quotas in the auto apply quota path, select **Apply auto apply quota to all derived quotas**.
   - If you want to keep the existing quotas unchanged but make the modified auto apply quota effective for new subfolders in the auto apply quota path, select **Do not apply auto apply quota to derived quotas**.
6. Click **OK**.

## Additional References

- Quota Management
- Create an Auto Apply Quota

# File Screening Management

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

On the **File Screening Management** node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:

- Create file screens to control the types of files that users can save, and generate notifications when users attempt to save unauthorized files.
- Define file screening templates that can be applied to new volumes or folders and that can be used across an organization.
- Create file screening exceptions that extend the flexibility of the file screening rules.

For example, you can:

- Ensure that no music files are stored on personal folders on a server, yet you could allow storage of specific types of media files that support legal rights management or comply with company policies. In the same scenario, you might want to give a vice president in the company special privileges to store any type of files in his personal folder.
- Implement a screening process to notify you by e-mail when an executable file is stored on a shared folder, including information about the user who stored the file and the file's exact location, so that you can take the appropriate precautionary steps.

This section includes the following topics:

- Define File Groups for Screening
- Create a File Screen
- Create a File Screen Exception
- Create a File Screen Template
- Edit File Screen Template Properties

> **NOTE**
> To set e-mail notifications and certain reporting capabilities, you must first configure the general File Server Resource Manager options.

## Additional References

- Setting File Server Resource Manager Options

# Define File Groups for Screening

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

A *file group* is used to define a namespace for a file screen, file screen exception, or **Files by File Group** storage report. It consists of a set of file name patterns, which are grouped by the following:

- **Files to include**: files that belong in the group
- **Files to exclude**: files that do not belong in the group

> **NOTE**
> For convenience, you can create and edit file groups while you edit the properties of file screens, file screen exceptions, file screen templates, and **Files by File Group** reports. Any file group changes that you make from these property sheets are not limited to the current item that you are working on.

## To create a File Group

1. In **File Screening Management**, click the **File Groups** node.
2. On the **Actions** pane, click **Create File Group**. This opens the **Create File Group Properties** dialog box.

   (Alternatively, while you edit the properties of a file screen, file screen exception, file screen template, or **Files by File Group** report, under **Maintain file groups**, click **Create**.)
3. In the **Create File Group Properties** dialog box, type a name for the file group.
4. Add files to include and files to exclude:
   - For each set of files that you want to include in the file group, in the **Files to include** box, enter a file name pattern, and then click **Add**.
   - For each set of files that you want to exclude from the file group, in the **Files to exclude** box, enter a file name pattern, and then click **Add**. Note that standard wildcard rules apply, for example, ***.exe** selects all executable files.
5. Click **OK**.

## Additional References

- File Screening Management
- Create a File Screen
- Create a File Screen Exception
- Create a File Screen Template
- Storage Reports Management

# Create a File Screen

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

When creating a new file screen, you can choose to save a file screen template that is based on the custom file screen properties that you define. The advantage of this is that a link is maintained between file screens and the template that is used to create them, so that in the future, changes to the template can be applied to all file screens that derive from it. This is a feature that simplifies the implementation of storage policy changes by providing one central point where you can make all updates.

## To create a File Screen with custom properties

1. In **File Screening Management**, click the **File Screens** node.
2. Right-click **File Screens,** and click **Create File Screen** (or select **Create File Screen** from the **Actions** pane). This opens the **Create File Screen** dialog box.
3. Under **File screen path**, type the name of or browse to the folder that the file screen will apply to. The file screen will apply to the selected folder and all of its subfolders.
4. Under **How do you want to configure file screen properties**, click **Define custom file screen properties**, and then click **Custom Properties**. This opens the **File Screen Properties** dialog box.
5. If you want to copy the properties of an existing template to use as a base for your file screen, select a template from the **Copy properties from template** drop-down list. Then click **Copy**.

   In the **File Screen Properties** dialog box, modify or set the following values on the **Settings** tab:
6. Under **Screening type**, click the **Active screening** or **Passive screening** option. (Active screening prevents users from saving files that are members of blocked file groups and generates notifications when users try to save unauthorized files. Passive screening sends configured notifications, but it does not prevent users from saving files.)
7. Under **File groups**, select each file group that you want to include in your file screen. (To select the check box for the file group, double-click the file group label.)

   If you want to view the file types that a file group includes and excludes, click the file group label, and then click **Edit**. To create a new file group, click **Create**.
8. Additionally, you can configure **File Server Resource Manager** to generate one or more notifications by setting options on the **E-mail Message**, **Event Log**, **Command**, and **Report** tabs. For more information about file screen notification options, see Create a File Screen Template.
9. After you have selected all the file screen properties that you want to use, click **OK** to close the **File Screen Properties** dialog box.
10. In the **Create File Screen** dialog box, click **Create** to save the file screen. This opens the **Save Custom Properties as a Template** dialog box.
11. Select the type of custom file screen you want to create:

    - To save a template that is based on these customized properties (recommended), click **Save the**

**custom properties as a template** and enter a name for the template. This option will apply the template to the new file screen, and you can use the template to create additional file screens in the future. This will enable you to later update the file screens automatically by updating the template.

- If you do not want to save a template when you save the file screen, click **Save the custom file screen without creating a template**.

12. Click **OK**.

## Additional References

- File Screening Management
- Define File Groups for Screening
- Create a File Screen Template
- Edit File Screen Template Properties

# Create a File Screen Exception

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Occasionally, you need to allow exceptions to file screening. For example, you might want to block video files from a file server, but you need to allow your training group to save the video files for their computer-based training. To allow files that other file screens are blocking, create a *file screen exception*.

A file screen exception is a special type of file screen that over-rides any file screening that would otherwise apply to a folder and all its subfolders in a designated exception path. That is, it creates an exception to any rules derived from a parent folder.

> **NOTE**
> You cannot create a file screen exception on a parent folder where a file screen is already defined. You must assign the exception to a subfolder or make changes to the existing file screen.

You assign file groups to determine which file types will be allowed in the file screen exception.

## To create a File Screen Exception

1. In **File Screening Management**, click the **File Screens** node.
2. Right-click **File Screens**, and click **Create File Screen Exception** (or select **Create File Screen Exception** from the **Actions** pane). This opens the **Create File Screen Exception** dialog box.
3. In the **Exception path** text box, type or select the path that the exception will apply to. The exception will apply to the selected folder and all of its subfolders.
4. To specify which files to exclude from file screening:
   - Under **File groups**, select each file group that you want to exclude from file screening. (To select the check box for the file group, double-click the file group label.)
   - If you want to view the file types that a file group includes and excludes, click the file group label, and click **Edit**.
   - To create a new file group, click **Create**.
5. Click **OK**.

## Additional References

- File Screening Management
- Define File Groups for Screening

# Create a File Screen Template

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

A *file screen template* defines a set of file groups to screen, the type of screening to perform (active or passive), and optionally, a set of notifications that will be generated automatically when a user saves, or attempts to save, an unauthorized file.

File Server Resource Manager can send e-mail messages to administrators or specific users, log an event, execute a command or a script, or generate reports. You can configure more than one type of notification for a file screen event.

By creating file screens exclusively from templates, you can centrally manage your file screens by updating the templates instead of replicating changes in each file screen. This feature simplifies the implementation of storage policy changes by providing one central point where you can make all updates.

**IMPORTANT**

To send e-mail notifications and to configure the storage reports with parameters that are appropriate for your server environment, you must first set the general File Server Resource Manager options. For more information, see Setting File Server Resource Manager Options.

## To create a File Screen Template

1. In **File Screening Management**, click the **File Screen Templates** node.
2. Right-click **File Screen Templates**, and then click **Create File Screen Template** (or select **Create File Screen Template** from the **Actions** pane). This opens the **Create File Screen Template** dialog box.
3. If you want to copy the properties of an existing template to use as a base for your new template, select a template from the **Copy properties from template** drop-down list and then click **Copy**.

   Whether you have chosen to use the properties of an existing template or you are creating a new template, modify or set the following values on the **Settings** tab:
4. In the **Template name** text box, enter a name for the new template.
5. Under **Screening type**, click the **Active screening** or **Passive screening** option. (Active screening prevents users from saving files that are members of blocked file groups and generates notifications when users try to save unauthorized files. Passive screening sends configured notifications, but it does not prevent users from saving files).
6. To specify which file groups to screen:

   Under **File groups**, select each file group that you want to include. (To select the check box for the file group, double-click the file group label.)

   If you want to view the file types that a file group includes and excludes, click the file group label, and then click **Edit**. To create a new file group, click **Create**.

   Additionally, you can configure File Server Resource Manager to generate one or more notifications by

setting the following options on the **E-mail Message**, **Event Log**, **Command**, and **Report** tabs.

7. To configure e-mail notifications:

   On the **E-mail Message** tab, set the following options:

   - To notify administrators when a user or application attempts to save an unauthorized file, select the **Send e-mail to the following administrators** check box, and then enter the names of the administrative accounts that will receive the notifications. Use the format *account@domain*, and use semicolons to separate multiple accounts.
   - To send e-mail to the user who attempted to save the file, select the **Send e-mail to the user who attempted to save an unauthorized file** check box.
   - To configure the message, edit the default subject line and message body that are provided. The text that is in brackets inserts variable information about the file screen event that caused the notification. For example, the [**Source Io Owner**] variable inserts the name of the user who attempted to save an unauthorized file. To insert additional variables in the text, click **Insert Variable**.
   - To configure additional headers (including From, Cc, Bcc, and Reply-to), click **Additional E-mail Headers**.

8. To log an error to the event log when a user tries to save an unauthorized file:

   On the **Event Log** tab, select the **Send warning to event log** check box, and edit the default log entry.

9. To run a command or script when a user tries to save an unauthorized file:

   On the **Command** tab, select the **Run this command or script** check box. Then type the command, or click **Browse** to search for the location where the script is stored. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.

10. To generate one or more storage reports when a user tries to save an unauthorized file:

    On the **Report** tab, select the **Generate reports** check box, and then select which reports to generate. (You can choose one or more administrative e-mail recipients for the report or e-mail the report to the user who attempted to save the file.)

    The report is saved in the default location for incident reports, which you can modify in the **File Server Resource Manager Options** dialog box.

11. After you have selected all the file template properties that you want to use, click **OK** to save the template.

## Additional References

- File Screening Management
- Setting File Server Resource Manager Options
- Edit File Screen Template Properties

# Edit File Screen Template Properties

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

When you make changes to a file screen template, you have the option of extending those changes to file screens that were created with the original file screen template. You can choose to modify only those file screens that match the original template or all file screens that derive from the original template, regardless of any modifications that you made to the file screens since they were created. This feature simplifies the process of updating the properties of file screens by providing one central point where you make all the changes.

> **NOTE**
> If you apply the changes to all file screens that derive from the original template, you will overwrite any custom file screen properties that you created.

## To edit File Screen Template Properties

1. In **File Screen Templates**, select the template that you want to modify.
2. Right-click the file screen template and click **Edit Template Properties** (or in the **Actions** pane, under **Selected File Screen Templates**, select **Edit Template Properties**.) This opens the **File Screen Template Properties** dialog box.
3. If you want to copy the properties of another template as a base for your modified template, select a template from the **Copy properties from template** drop-down list. Then click **Copy**.
4. Perform all necessary changes. The settings and notification options are identical to those that are available when you create a file screen template.
5. When you are finished editing the template properties, click **OK**. This will open the **Update File Screens Derived from Template** dialog box.
6. Select the type of update that you want to apply:
   - If you have file screens that have been modified since they were created using the original template, and you do not want to change them, click **Apply template only to derived file screens that match the original template**. This option will update only those file screens that have not been edited since they were created with the original template properties.
   - If you want to modify all existing file screens that were created using the original template, click **Apply template to all derived file screens**.
   - If you want to keep the existing file screens unchanged, click **Do not apply template to derived file screens**.
7. Click **OK**.

## Additional References

- File Screening Management
- Create a File Screen Template

# Storage Reports Management

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

On the **Storage Reports Management** node of the File Server Resource Manager Microsoft® Management Console (MMC) snap-in, you can perform the following tasks:

- Schedule periodic storage reports that allow you to identify trends in disk usage.
- Monitor attempts to save unauthorized files for all users or a selected group of users.
- Generate storage reports instantly.

For example, you can:

- Schedule a report that will run every Sunday at midnight, generating a list that includes the most recently accessed files from the previous two days. With this information, you can monitor weekend storage activity and plan server down-time that will have less impact on users who are connecting from home over the weekend.
- Run a report at any time to identify all duplicate files in a volume on a server so that disk space can be quickly reclaimed without losing any data.
- Run a Files by File Group report to identify how storage resources are segmented across different file groups
- Run a Files by Owner report to analyze how individual users are using shared storage resources.

This section includes the following topics:

- Schedule a Set of Reports
- Generate Reports on Demand

> **NOTE**
>
> To set e-mail notifications and certain reporting capabilities, you must first configure the general File Server Resource Manager options.

## Additional References

- Setting File Server Resource Manager Options

# Schedule a Set of Reports

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

To generate a set of reports on a regular schedule, you schedule a *report task.* The report task specifies which reports to generate and what parameters to use; which volumes and folders to report on; how often to generate the reports and which file formats to save them in.

Scheduled reports are saved in a default location, which you can specify in the **File Server Resource Manager Options** dialog box. You also have the option of delivering the reports by e-mail to a group of administrators.

> **NOTE**
>
> To minimize the impact of report processing on performance, generate multiple reports on the same schedule so that the data is only gathered once. To quickly add reports to existing report tasks, you can use the **Add or Remove Reports for a Report Task** action. This allows you to add or remove reports from multiple report tasks and to edit the report parameters. To change schedules or delivery addresses, you must edit individual report tasks.

## To schedule a Report Task

1. Click the **Storage Reports Management** node.
2. Right-click **Storage Reports Management**, and then click **Schedule a New Report Task** (or select **Schedule a New Report Task** from the **Actions** pane). This opens the **Storage Reports Task Properties** dialog box.
3. To select volumes or folders on which to generate reports:
   - Under **Scope**, click **Add**.
   - Browse to the volume or folder on which you want to generate the reports, select it, and then click **OK** to add the path to the list.
   - Add as many volumes or folders as you want to include in the reports. (To remove a volume or folder, click the path and then click **Remove**).
4. To specify which reports to generate:
   - Under **Report data**, select each report that you want to include. By default, all reports are generated for a scheduled report task.

   To edit the parameters of a report:
   - Click the report label, and then click **Edit Parameters**.
   - In the **Report Parameters** dialog box, edit the parameters as needed, and then click **OK**.
   - To see a list of parameters for all the selected reports, click **Review Selected Reports**. Then click **Close**.
5. To specify the formats for saving the reports:
   - Under **Report formats**, select one or more formats for the scheduled reports. By default, reports are generated in Dynamic HTML (DHTML). You can also select HTML, XML, CSV, and text formats. The reports

are saved to the default location for scheduled reports.

6. To deliver copies of the reports to administrators by e-mail:

   - On the **Delivery** tab, select the **Send reports to the following administrators** check box, and then enter the names of the administrative accounts that will receive reports.
   - Use the format *account@domain*, and use semicolons to separate multiple accounts.

7. To schedule the reports:

   On the **Schedule** tab, click **Create Schedule**, and then in the **Schedule** dialog box, click **New**. This displays a default schedule set for 9:00 A.M. daily, but you can modify the default schedule.

   - To specify a frequency for generating the reports, select an interval from the **Schedule Task** drop-down list. You can schedule daily, weekly, or monthly reports, or generate the reports only once. You can also generate reports at system startup or logon, or when the computer has been idle for a specified time.
   - To provide additional scheduling information for the chosen interval, modify or set the values in the **Schedule Task** options. These options change based on the interval that you choose. For example, for a weekly report, you can specify the number of weeks between reports and on which days of the week to generate reports.
   - To specify the time of day when you want to generate the report, type or select the value in the **Start time** box.
   - To access additional scheduling options (including a start date and end date for the task), click **Advanced**.
   - To save the schedule, click **OK**.
   - To create an additional schedule for a task (or modify an existing schedule), on the **Schedule** tab, click **Edit Schedule**.

8. To save the report task, click **OK**.

The report task is added to the **Storage Reports Management** node. Tasks are identified by the reports to be generated, the namespace to be reported on, and the report schedule.

In addition, you can view the current status of the report (whether or not the report is running), the last run time and the result of that run, and the next scheduled run time.

## Additional References

- Storage Reports Management
- Setting File Server Resource Manager Options

# Generate Reports on Demand

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

During daily operations, you can use the **Generate Reports Now** option to generate one or more reports on demand. With these reports, you can analyze the different aspects of current disk usage on the server. Current data is gathered before the reports are generated.

When you generate reports on demand, the reports are saved in a default location that you specify in the **File Server Resource Manager Option** dialog box, but no report task is created for later use. You can view the reports immediately after they are generated or e-mail the reports to a group of administrators.

> **NOTE**
> If you choose to open the reports immediately, you must wait while the reports are generated. Processing time varies, depending on the types of reports and the scope of the data.

## To generate Reports immediately

1. Click the **Storage Reports Management** node.
2. Right-click **Storage Reports Management**, and then click **Generate Reports Now** (or select **Generate Reports Now** from the **Actions** pane). This opens the **Storage Reports Task Properties** dialog box.
3. To select volumes or folders on which to generate reports:
   - Under **Scope**, click **Add**.
   - Browse to the volume or folder on which you want to generate the reports, select it, and then click **OK** to add the path to the list.
   - Add as many volumes or folders as you want to include in the reports. (To remove a volume or folder, click the path and then click **Remove**).
4. To specify which reports to generate:
   - Under **Report data**, select each report that you want to include.

   To edit the parameters of a report:
   - Click the report label, and then click **Edit Parameters**.
   - In the **Report Parameters** dialog box, edit the parameters as needed, and then click **OK**.
   - To see a list of parameters for all the selected reports, click **Review Selected Reports** and then click **Close**.
5. To specify the formats for saving the reports:
   - Under **Report formats**, select one or more formats for the scheduled reports. By default, reports are generated in Dynamic HTML (DHTML). You can also select HTML, XML, CSV, and text formats. The reports are saved to the default location for on-demand reports.
6. To deliver copies of the reports to administrators by e-mail:
   - On the **Delivery** tab, select the **Send reports to the following administrators** check box, and then

enter the names of the administrative accounts that will receive reports.

- Use the format *account@domain*, and use semicolons to separate multiple accounts.

7. To gather the data and generate the reports, click **OK**. This opens the **Generate Storage Reports** dialog box.
8. Select how you want to generate the on-demand reports:

   - If you want to view the reports immediately after they are generated, click **Wait for reports to be generated and then display them**. Each report opens in its own window.
   - To view the reports later, click **Generate reports in the background**.

   Both options save the reports, and if you enabled delivery by e-mail, send the reports to administrators in the formats that you selected.

## Additional References

- Storage Reports Management
- Setting File Server Resource Manager Options

# Classification Management

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Classification properties are used to categorize files and can be used to select files for scheduled file management tasks.

There are many ways to classify a file. One way is to create a classification property that assigns a value to all files within a specified directory. Another way is to create rules to decide what value to set for a given property.

This section includes the following topics:

- Create a Classification Property
- Create an Automatic Classification Rule

**NOTE**

To set e-mail notifications and certain reporting capabilities, you must first configure the general File Server Resource Manager options.

## Additional References

Setting File Server Resource Manager Options

# Create an Automatic Classification Rule

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

The following procedure guides you through the process of creating a classification rule. Each rule sets the value for a single property. By default, a rule is run only once and ignores files that already have a property value assigned. However, you can configure a rule to evaluate files regardless of whether a value is already assigned to the property.

## To create a Classification Rule

1. In **Classification Management**, click the **Classification Rules** node.
2. Right-click **Classification Rules**, and then click **Create a New Rule** (or click **Create a New Rule** in the **Actions** pane). This opens the **Classification Rule Definitions** dialog box.
3. On the **Rule Settings** tab, enter the following information:
   - **Rule name**. Type a name for the rule.
   - **Enabled**. This rule will only be applied if the Enabled check box is selected. To disable the rule, clear this box.
   - **Description**. Type an optional description for this rule.
   - **Scope**. Click **Add** to select a location where this rule will apply. You can add multiple locations, or remove a location by clicking **Remove**. The classification rule will apply to all folders and their subfolders in this list.
4. On the **Classification** tab, enter the following information:
   - **Classification mechanism**. Choose a method for assigning the property value.
   - **Property name**. Select the property that this rule will assign.
   - **Property value**. Select the property value that this rule will assign.
5. Optionally, click the **Advanced** button to select further options. On the **Evaluation Type** tab, the check box to **Re-evaluate files** is unchecked by default. The options that can be selected here are as follows:
   - **Re-evaluate files** unchecked: A rule is applied to a file if, and only if, the property specified by the rule has not been set to any value on the file.
   - **Re-evaluate files** checked and the **Overwrite the existing value** option selected: the rule will be applied to the files every time the automatic classification process runs. For example, if a file has a Boolean property that is set to **Yes**, a rule using the folder classifier to set all files to **No** with this option set will leave the property set to **No**.
   - **Re-evaluate files** checked and the **Aggregate the values** option selected: The rule will be applied to the files every time the automatic classification process runs. However, when the rule has decided what value to set the property file to, it aggregates that value with the one already in the file. For example, if a file has a Boolean property that is set to **Yes**, a rule using the folder classifier to set all files to **No** with this option set will leave the property set to **Yes**.

   On the **Additional Classification Parameters** tab, you can specify additional parameters that are recognized by the selected classification method by entering the name and value and clicking the **Insert** button.

6. Click **OK** or **Cancel** to close the **Advanced** dialog box.
7. Click **OK**.

## Additional References

- Create a Classification Property
- Classification Management

# Create a Classification Property

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Classification properties are used to assign values to files within a specified folder or volume. There are many property types that you can choose from, depending on your needs. The following table defines the available property types.

| PROPERTY | DESCRIPTION |
| --- | --- |
| Yes/No | A Boolean property that can be **Yes** or **No**. When combining multiple values during classification or from file content, a **No** value will be overridden by a **Yes** value. |
| Date-time | A simple date/time property. When combining multiple values during classification or from file content, conflicting values will prevent re-classification. |
| Number | A simple number property. When combining multiple values during classification or from file content, conflicting values will prevent re-classification. |
| Ordered List | A list of fixed values. Only one value can be assigned to a property at a time. When combining multiple values during classification or from file content, the value highest in the list will be used. |
| String | A simple string property. When combining multiple values during classification or from file content conflicting values will prevent re-classification. |
| Multi-choice | A list of values that can be assigned to a property. More than one value can be assigned to a property at a time. When combining multiple values during classification or from file content, each value in the list will be used. |
| Multi-string | A list of strings that can be assigned to a property. More than one value can be assigned to a property at a time. When combining multiple values during classification or from file content, each value in the list will be used. |

The following procedure guides you through the process of creating a classification property.

## To create a Classification Property

1. In **Classification Management**, click the **Classification Properties** node.
2. Right-click **Classification Properties**, and then click **Create property** (or click **Create property** in the **Actions** pane). This opens the **Classification Property Definitions** dialog box.

3. In the **Property Name** text box, type a name for the property.
4. In the **Description** text box, add an optional description for the property.
5. In the **Property Type** drop-down menu, select a property type from the list.
6. Click **OK**.

## Additional References

- Create an Automatic Classification Rule
- Classification Management

# File Management Tasks

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

File management tasks automate the process of finding subsets of files on a server and applying simple commands. These tasks can be scheduled to occur periodically to reduce repetitive costs. Files that will be processed by a file management task can be defined through any of the following properties:

- Location
- Classification properties
- Creation time
- Modification time
- Last accessed time

File management tasks can also be configured to notify file owners of any impending policy that will be applied to their files.

> **NOTE**
> Individual File Management tasks are run on independent schedules.

This section includes the following topics:

- Create a File Expiration Task
- Create a Custom File Management Task

> **NOTE**
> To set e-mail notifications and certain reporting capabilities, you must first configure the general File Server Resource Manager options.

## Additional References

- Setting File Server Resource Manager Options

# Create a File Expiration Task

11/2/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

The following procedure guides you through the process of creating a file management task for expiring files. File expiration tasks are used to automatically move all files that match certain criteria to a specified expiration directory, where an administrator can then back those files up and delete them.

When a file expiration task is run, a new directory is created within the expiration directory, grouped by the server name on which the task was run.

The new directory name is based on the name of the file management task and the time it was run. When an expired file is found it is moved into the new directory, while preserving its original directory structure.

## To create a file expiration task

1. Click the **File Management Tasks** node.
2. Right-click **File Management Tasks**, and then click **Create File Management Task** (or click **Create File Management Task** in the **Actions** pane). This opens the **Create File Management Task** dialog box.
3. On the **General** tab, enter the following information:
   - **Name**. Enter a name for the new task.
   - **Description**. Enter an optional descriptive label for this task.
   - **Scope**. Add the directories that this task should operate on by using the **Add** button. Optionally, directories can be removed from the list using the **Remove** button. The file management task will apply to all folders and their subfolders in this list.
4. On the **Action** tab, enter the following information:
   - **Type**. Select **File Expiration** from the drop-down box.
   - **Expiration Directory**. Select a directory where files will be expired to.

     **WARNING**
     Do not select a directory that is within the scope of the task, as defined in the previous step. Doing so could cause an iterative loop that could lead to system instability and data loss.
5. Optionally, on the **Notification** tab, click **Add** to send e-mail notifications, log an event, or run a command or script a specified minimum number of days before the task performs an action on a file.
   - In the **Number of days before task is executed to send notification** combo box, type or select a value to specify the minimum number of days prior to a file being acted on that a notification will be sent.

> **NOTE**
> Notifications are sent only when a task is run. If the specified minimum number of days to send a notification does not coincide with a scheduled task, the notification will be sent on the day of the previous scheduled task.

- To configure e-mail notifications, click the **E-mail Message** tab and enter the following information:
  - To notify administrators when a threshold is reached, select the **Send e-mail to the following administrators** check box, and then enter the names of the administrative accounts that will receive the notifications. Use the format *account@domain*, and use semicolons to separate multiple accounts.
  - To send e-mail to the person whose files are about to expire, select the **Send e-mail to the user whose files are about to expire** check box.
  - To configure the message, edit the default subject line and message body that are provided. The text that is in brackets inserts variable information about the quota event that caused the notification. For example, the **[Source File Owner]** variable inserts the name of the user whose file is about to expire. To insert additional variables in the text, click **Insert Variable**.
  - To attach a list of the files that are about to expire, click **Attach to the e-mail list of files on which action will be performed**, and type or select a value for **Maximum number of files in the list**.
  - To configure additional headers (including From, Cc, Bcc, and Reply-to), click **Additional E-mail Headers**.
- To log an event, click the **Event Log** tab and select the **Send warning to event log** check box, and then edit the default log entry.
- To run a command or script, click the **Command** tab and select the **Run this command or script** check box. Then type the command, or click **Browse** to search for the location where the script is stored. You can also enter command arguments, select a working directory for the command or script, or modify the command security setting.

6. Optionally, use the **Report** tab to generate one or more logs or storage reports.
   - To generate logs, select the **Generate log** check box and then select one or more available logs.
   - To generate reports, select the **Generate a report** check box and then select one or more available report formats.
   - To create e-mail generated logs or storage reports, select the **Send reports to the following administrators** check box and type one or more administrative e-mail recipients using the format *account@domain*. Use a semicolon to separate multiple addresses.

   > **NOTE**
   > The report is saved in the default location for incident reports, which you can modify in the **File Server Resource Manager Options** dialog box.

7. Optionally, use the **Condition** tab to run this task only on files that match a defined set of conditions. The following settings are available:
   - **Property conditions**. Click **Add** to create a new condition based on the file's classification. This will open the **Property Condition** dialog box, which allows you to select a property, an operator to

perform on the property, and the value to compare the property against. After clicking **OK**, you can then create additional conditions, or edit or remove an existing condition.

- **Days since file was last modified**. Click the check box and then enter a number of days into the spin box. This will result in the file management task only being applied to files that have not been modified for more than the specified number of days.
- **Days since file was last accessed**. Click the check box and then enter a number of days into the spin box. If the server is configured to track timestamps for when files were last accessed, this will result in the file management task only being applied to files that have not been accessed for more than the specified number of days. If the server is not configured to track accessed times, this condition will be ineffective.
- **Days since file was created**. Click the check box and then enter a number of days into the spin box. This will result in the task only being applied to files that were created at least the specified number of days ago.
- **Effective starting**. Set a date when this file management task should start processing files. This option is useful for delaying the task until you have had a chance to notify users or make other preparations in advance.

8. On the **Schedule** tab, click **Create Schedule**, and then in the **Schedule** dialog box, click **New**. This displays a default schedule set for 9:00 A.M. daily, but you can modify the default schedule. When you have finished configuring the schedule, click **OK** and then click **OK** again.

## Additional References

- Classification Management
- File Management Tasks

# Create a Custom File Management Task

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Expiration is not always a desired action to be performed on files. File management tasks allow you to run custom commands as well.

> **NOTE**
> This procedure assumes that you are familiar with file management tasks, and therefore only covers the **Action** tab where custom settings are configured.

## To create a custom task

1. Click the **File Management Tasks** node.
2. Right-click **File Management Tasks**, and then click **Create File Management Task** (or click **Create File Management Task** in the **Actions** pane). This opens the **Create File Management Task** dialog box.
3. On the **Action** tab, enter the following information:
   - **Type**. Select **Custom** from the drop-down menu.
   - **Executable**. Type or browse to a command to run when the file management task processes files. This executable must be set to be writable by Administrators and System only. If any other users have write access to the executable, it will not run correctly.
   - **Command settings**. To configure the arguments passed to the executable when a file management job processes files, edit the text box labeled **Arguments**. To insert additional variables in the text, place the cursor in the location in the text box where you want to insert the variable, select the variable that you want to insert, and then click **Insert Variable**. The text that is in brackets inserts variable information that the executable can receive. For example, the [Source File Path] variable inserts the name of the file that should be processed by the executable. Optionally, click the **Working directory** button to specify the location of the custom executable.
   - **Command Security**. Configure the security settings for this executable. By default, the command is run as Local Service, which is the most restrictive account available.
4. Click **OK**.

## Additional References

- Classification Management
- File Management Tasks

# Managing Remote Storage Resources

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

To manage storage resources on a remote computer, you have two options:

- Connect to the remote computer from the File Server Resource Manager Microsoft® Management Console (MMC) snap-in (which you can then use to manage the remote resources).
- Use the command-line tools that are installed with File Server Resource Manager.

Either option allows you to work with quotas, screen files, manage classifications, schedule file management tasks, and generate reports with those remote resources.

> **NOTE**
> File Server Resource Manager can manage resources on either the local computer or a remote computer, but not both at the same time.

For example, you can:

- Connect to another computer in the domain using the File Server Resource Manager MMC snap-in and review storage utilization on a volume or folder located on the remote computer.
- Create quota and file screen templates on a local server and then use the command-line tools to import those templates into a file server located in a branch office.

This section includes the following topics:

- Connect to a Remote Computer
- Command-Line Tools

# Connect to a Remote Computer

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

To manage storage resources on a remote computer, you can connect to the computer from File Server Resource Manager. While you are connected, File Server Resource Manager allows you to manage quotas, screen files, manage classifications, schedule file management tasks, and generate reports with those remote resources.

> **NOTE**
> File Server Resource Manager can manage resources on either the local computer or a remote computer, but not both at the same time.

## To connect to a remote computer from File Server Resource Manager

1. In **Administrative Tools**, click **File Server Resource Manager**.
2. In the console tree, right-click **File Server Resource Manager**, and then click **Connect to Another Computer**.
3. In the **Connect to Another Computer** dialog box, click **Another computer**. Then type the name of the server you want to connect to (or click **Browse** to search for a remote computer).
4. Click **OK**.

> **IMPORTANT**
> The **Connect to Another Computer** command is available only when you open File Server Resource Manager from **Administrative Tools**. When you access File Server Resource Manager from Server Manager, the command is not available.

## Additional considerations

To manage remote resources with File Server Resource Manager:

- You must be logged on to the local computer with a domain account that is a member of the **Administrators** group on the remote computer.
- The remote computer must be running Windows Server, and File Server Resource Manager must be installed.
- The **Remote File Server Resource Manager Management** exception on the remote computer must be enabled. Enable this exception by using Windows Firewall in Control Panel.

## Additional References

- Managing Remote Storage Resources

# File Server Resource Manager command-line tools

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

File Server Resource Manager installs the FileServerResourceManager PowerShell cmdlets as well as the following command-line tools:

- **Dirquota.exe**. Use to create and manage quotas, auto apply quotas, and quota templates.
- **Filescrn.exe**. Use to create and manage file screens, file screen templates, file screen exceptions, and file groups.
- **Storrept.exe**. Use to configure report parameters and generate storage reports on demand. Also use to create report tasks, which you can schedule by using **schtasks.exe**.

You can use these tools to manage storage resources on a local computer or a remote computer. For more information about these command-line tools, see the following references:

- **Dirquota**: https://go.microsoft.com/fwlink/?LinkId=92741
- **Filescrn**: https://go.microsoft.com/fwlink/?LinkId=92742
- **Storrept**: https://go.microsoft.com/fwlink/?LinkId=92743

> **NOTE**
> To see command syntax and the available parameters for a command, run the command with the **/?** parameter.

## Remote management using the command-line tools

Each tool has several options for performing actions similar to those that are available in the File Server Resource Manager MMC snap-in. To have a command perform an action on a remote computer instead of the local computer, use the **/remote**:*ComputerName* parameter.

For example,**Dirquota.exe** includes a **template export** parameter to write quota template settings to an XML file, and a **template import** parameter to import template settings from the XML file. Adding the **/remote**:*ComputerName* parameter to the **Dirquota.exe template import** command will import the templates from the XML file on the local computer to the remote computer.

> **NOTE**
> When you run the command-line tools with the **/remote**:*ComputerName* parameter to perform a template export (or import) on a remote computer, the templates are written to (or copied from) an XML file on the local computer.

## Additional considerations

To manage remote resources with the command-line tools:

- You must be logged on with a domain account that is a member of the **Administrators** group on the local computer and on the remote computer.

- You must run the command-line tools from an elevated Command Prompt window. To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- The remote computer must be running Windows Server, and File Server Resource Manager must be installed.
- The **Remote File Server Resource Manager Management** exception on the remote computer must be enabled. Enable this exception by using Windows Firewall in Control Panel.

## Additional References

- Managing Remote Storage Resources

# Troubleshooting File Server Resource Manager

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

This section lists common issues that you might encounter when using File Server Resource Manager.

> **NOTE**
> A good troubleshooting option is to look for event logs that have been generated by File Server Resource Manager. All event log entries for File Server Resource Manager can be found in the **Application** event log under the source **SRMSVC**

## I am not receiving e-mail notifications.

- **Cause**: The e-mail options have not been configured or have been configured incorrectly.
- **Solution**: On the **E-mail Notifications** tab, in the **File Server Resource Manager Options** dialog box, verify that the SMTP server and default e-mail recipients have been specified and are valid. Send a test e-mail to confirm that the information is correct and that the SMTP server that is used to send the notifications is working properly. For more information see Configure E-Mail Notifications.

## I am only receiving one e-mail notification, even though the event that triggered that notification happened several times in a row.

- **Cause**: When a user attempts several times to save a file that is blocked or to save a file that exceeds a quota threshold, and there is an e-mail notification configured for that file screening or quota event, only one e-mail is sent to the administrator over a 60-minute period by default. This prevents an abundance of redundant messages in the administrator's e-mail account.
- **Solution**: On the **Notification Limits** tab, in the **File Server Resource Manager Options** dialog box, you can set a time limit for each of the notification types: e-mail, event log, command, and report. Each limit specifies a time period that must pass before another notification of the same type is generated for the same issue. For more information see Configure Notification Limits.

## My storage reports keep failing and little or no information is available in the Event Log regarding the source of the failure.

- **Cause**: The volume where the reports are being saved may be corrupted.
- **Solution**: Run **chkdsk** on the volume and try generating the reports again.

## My File Screening Audit reports do not contain any information.

- **Cause**: One or more of the following may be the cause:
  - The auditing database is not configured to record file screening activity.
  - The auditing database is empty (that is, no file screening activity has been recorded).
  - The parameters for the File Screening Audit report are not selecting data from the auditing database.
- **Solution**: On the **File Screen Audit** tab, in the **File Server Resource Manager Options** dialog box,

verify that the **Record file screening activity in the auditing database** check box is selected.

- For more information about recording file screening activity, see Configure File Screen Audit.
- To configure default parameters for the File Screening Audit report, see Configure Storage Reports.
- To edit report parameters for scheduled report tasks or on-demand reports, see Storage Reports Management.

## The "Used" and "Available" values for some of the quotas I have created do not correspond to the actual "Limit" setting.

- **Cause**: You may have a nested quota, where the quota of a subfolder derives a more restrictive limit from the quota of its parent folder. For example, you might have a quota limit of 100 megabytes (MB) applied to a parent folder and a quota of 200 MB applied separately to each of its subfolders. If the parent folder has a total of 50 MB of data stored in it (the sum of the data stored in its subfolders), each of the subfolders will list only 50 MB of available space.
- **Solution**: Under **Quota Management**, click **Quotas**. In the **Results** pane, select the quota entry that you are troubleshooting. In the **Actions** pane, click **View Quotas Affecting Folder**, and then look for quotas that are applied to the parent folders. This will allow you to identify which parent folder quotas have a lower storage limit setting than the quota you have selected.

# Folder Redirection, Offline Files, and Roaming User Profiles overview

11/2/2020 • 9 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2

This topic discusses the Folder Redirection, Offline Files (client-side caching or CSC), and Roaming User Profiles (sometimes known as RUP) technologies, including what's new and where to find additional information.

## Technology description

Folder Redirection and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location. These features used to be referred to as Intellimirror.

- **Folder Redirection** enables users and administrators to redirect the path of a known folder to a new location, manually or by using Group Policy. The new location can be a folder on the local computer or a directory on a file share. Users interact with files in the redirected folder as if it still existed on the local drive. For example, you can redirect the Documents folder, which is usually stored on a local drive, to a network location. The files in the folder are then available to the user from any computer on the network.
- **Offline Files** makes network files available to a user, even if the network connection to the server is unavailable or slow. When working online, file access performance is at the speed of the network and server. When working offline, files are retrieved from the Offline Files folder at local access speeds. A computer switches to Offline Mode when:
  - **Always Offline** mode has been enabled
  - The server is unavailable
  - The network connection is slower than a configurable threshold
  - The user manually switches to Offline Mode by using the **Work offline** button in Windows Explorer
- **Roaming User Profiles** redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers. When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile. Typically, a network administrator enables Roaming User Profiles on domain accounts.

## Practical applications

Administrators can use Folder Redirection, Offline Files, and Roaming User Profiles to centralize storage for user data and settings and to provide users with the ability to access their data while offline or in the event of a network or server outage. Some specific applications include:

- Centralize data from client computers for administrative tasks, such as using a server-based backup tool to back up user folders and settings.
- Enable users to continue accessing network files, even if there is a network or server outage.
- Optimize bandwidth usage and enhance the experience of users in branch offices who access files and folders that are hosted by corporate servers located offsite.

- Enable mobile users to access network files while working offline or over slow networks.

## New and changed functionality

The following table describes some of the major changes in Folder Redirection, Offline Files, and Roaming User Profiles that are available in this release.

| FEATURE/FUNCTIONALITY | NEW OR UPDATED? | DESCRIPTION |
|---|---|---|
| Always Offline mode | New | Provides faster access to files and lower bandwidth usage by always working offline, even when connected through a high-speed network connection. |
| Cost-aware synchronization | New | Helps users avoid high data usage costs from synchronization while using metered connections that have usage limits, or while roaming on another provider's network. |
| Primary Computer support | New | Enables you to limit the use of Folder Redirection, Roaming User Profiles, or both to only a user's primary computers. |

## Always Offline mode

Starting with Windows 8 and Windows Server 2012, administrators can configure the experience for users of Offline Files to always work offline, even when they are connected through a high-speed network connection. Windows updates files in the Offline Files cache by synchronizing hourly in the background, by default.

**What value does Always Offline mode add?**

The Always Offline mode provides the following benefits:

- Users experience faster access to files in redirected folders, such as the Documents folder.
- Network bandwidth is reduced, decreasing costs on expensive WAN connections or metered connections such as a 4G mobile network.

**How has Always Offline mode changed things?**

Prior to Windows 8, Windows Server 2012, users would transition between the Online and Offline modes, depending on network availability and conditions, even when the Slow-Link mode (also known as the Slow Connection mode) was enabled and set to a 1 millisecond latency threshold.

With Always Offline mode, computers never transition to Online mode when the **Configure slow-link mode** Group Policy setting is configured and the **Latency** threshold parameter is set to 1 millisecond. Changes are synced in the background every 120 minutes, by default, but synchronization is configurable by using the **Configure Background Sync** Group Policy setting.

For more information, see Enable the Always Offline Mode to Provide Faster Access to Files.

## Cost-aware synchronization

With cost-aware synchronization, Windows disables background synchronization when the user is using a metered network connection, such as a 4G mobile network, and the subscriber is near or over their bandwidth limit, or roaming on another provider's network.

> **NOTE**
>
> Metered network connections usually have round-trip network latencies that are slower than the default 35 millisecond latency value for transitioning to Offline (Slow Connection) mode in Windows 8, Windows Server 2019, Windows Server 2016, and Windows Server 2012. Therefore, these connections usually transition to Offline (Slow Connection) mode automatically.

**What value does cost-aware synchronization add?**

Cost-aware synchronization helps users avoid unexpectedly high data usage costs while using metered connections that have usage limits, or while roaming on another provider's network.

**How has cost-aware synchronization changed things?**

Prior to Windows 8 and Windows Server 2012, users who wanted to minimize fees while using Offline Files on metered network connections had to track their data usage by using tools from the mobile network provider. The users could then manually switch to Offline mode when they were roaming, near their bandwidth limit, or over their limit.

With cost-aware sync, Windows automatically tracks roaming and bandwidth usage limits while on metered connections. When the user is roaming, near their bandwidth limit, or over their limit, Windows switches to Offline mode and prevents all synchronization. Users can still manually initiate synchronization, and administrators can override cost-aware synchronization for specific users, such as executives.

For more information, see Enable Background File Synchronization on Metered Networks.

## Primary computers for Folder Redirection and Roaming User Profiles

You can now designate a set of computers, known as primary computers, for each domain user, which enables you to control which computers use Folder Redirection, Roaming User Profiles, or both. Designating primary computers is a simple and powerful method to associate user data and settings with particular computers or devices, simplify administrator oversight, improve data security, and help protect user profiles from corruption.

**What value do primary computers add?**

There are four major benefits to designating primary computers for users:

- The administrator can specify which computers users can use to access their redirected data and settings. For example, the administrator can choose to roam user data and settings between a user's desktop and laptop, and to not roam the information when that user logs on to any other computer, such as a conference room computer.
- Designating primary computers reduces the security and privacy risk of leaving residual personal or corporate data on computers where the user has logged on. For example, a general manager who logs on to an employee's computer for temporary access does not leave behind any personal or corporate data.
- Primary computers enable the administrator to mitigate the risk of an improperly configured or otherwise corrupt profile, which could result from roaming between differently configured systems, such as between x86-based and x64-based computers.
- The amount of time required for a user's first sign-in on a non-primary computer, such as a server, is faster because the user's roaming user profile and/or redirected folders are not downloaded. Sign-out times are also reduced, because changes to the user profile do not need to be uploaded to the file share.

**How have primary computers changed things?**

To limit downloading private user data to primary computers, the Folder Redirection and Roaming User Profiles technologies perform the following logic checks when a user signs in to a computer:

1. The Windows operating system checks the new Group Policy settings (**Download roaming profiles on primary computers only** and **Redirect folders on primary computers only**) to determine if the **msDS-**

**Primary-Computer** attribute in Active Directory Domain Services (AD DS) should influence the decision to roam the user's profile or apply Folder Redirection.

2. If the policy setting enables primary computer support, Windows verifies that the AD DS schema supports the **msDS-Primary-Computer** attribute. If it does, Windows determines if the computer that the user is logging on to is designated as a primary computer for the user as follows:
   a. If the computer is one of the user's primary computers, Windows applies the Roaming User Profiles and Folder Redirection settings.
   b. If the computer is not one of the user's primary computers, Windows loads the user's cached local profile, if present, or it creates a new local profile. Windows also removes any existing redirected folders according to the removal action that was specified by the previously applied Group Policy setting, which is retained in the local Folder Redirection configuration.

For more information, see Deploy Primary Computers for Folder Redirection and Roaming User Profiles

## Hardware requirements

Folder Redirection, Offline Files, and Roaming User Profiles require an x64-based or x86-based computer, and they are not supported by Windows on ARM (WOA)-based computers.

## Software requirements

To designate primary computers, your environment must meet the following requirements:

- The Active Directory Domain Services (AD DS) schema must be updated to include Windows Server 2012 schema and conditions (installing a Windows Server 2012 or later domain controller automatically updates the schema). For more information about upgrading the AD DS schema, see Upgrade Domain Controllers to Windows Server 2016.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 and be joined to the Active Directory domain that you are managing.

## More information

For additional related information, see the following resources.

| CONTENT TYPE | REFERENCES |
| --- | --- |
| Product evaluation | Supporting Information Workers with Reliable File Services and Storage<br>What's New in Offline Files (Windows 7 and Windows Server 2008 R2)<br>What's New in Offline Files for Windows Vista<br>Changes to Offline Files in Windows Vista (TechNet Magazine) |
| Deployment | Deploy Folder Redirection, Offline Files, and Roaming User Profiles<br>Implementing an End-User Data Centralization Solution: Folder Redirection and Offline Files Technology Validation and Deployment<br>Managing Roaming User Data Deployment Guide<br>Configuring New Offline Files Features for Windows 7 Computers Step-by-Step Guide<br>Using Folder Redirection<br>Implementing Folder Redirection (Windows Server 2003) |

| CONTENT TYPE | REFERENCES |
| --- | --- |
| Tools and settings | Offline files on MSDN<br>Offline Files Group Policy Reference (Windows 2000) |
| Community resources | File Services and Storage Forum<br>Hey, Scripting Guy! How Can I Work with the Offline Files Feature in Windows?<br>Hey, Scripting Guy! How Can I Enable and Disable Offline Files? |
| Related technologies | Identity and Access in Windows Server<br>Storage in Windows Server<br>Remote access and server management |

# Deploying Roaming User Profiles

12/16/2020 • 23 minutes to read • Edit Online

Applies to: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server (Semi-annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

This topic describes how to use Windows Server to deploy Roaming User Profiles to Windows client computers. Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers.

For a list of recent changes to this topic, see the Change history section of this topic.

**IMPORTANT**

Due to the security changes made in MS16-072, we updated Step 4: Optionally create a GPO for Roaming User Profiles in this topic so that Windows can properly apply the Roaming User Profiles policy (and not revert to local policies on affected PCs).

**IMPORTANT**

User customizations to Start is lost after an OS in-place upgrade in the following configuration:

- Users are configured for a roaming profile
- Users are allowed to make changes to Start

As a result, the Start menu is reset to the default of the new OS version after the OS in-place upgrade. For workarounds, see Appendix C: Working around reset Start menu layouts after upgrades.

## Prerequisites

### Hardware requirements

Roaming User Profiles requires an x64-based or x86-based computer; it isn't supported by Windows RT.

### Software requirements

Roaming User Profiles has the following software requirements:

- If you are deploying Roaming User Profiles with Folder Redirection in an environment with existing local user profiles, deploy Folder Redirection before Roaming User Profiles to minimize the size of roaming profiles. After the existing user folders have been successfully redirected, you can deploy Roaming User Profiles.
- To administer Roaming User Profiles, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.
- Client computers must be joined to the Active Directory Domain Services (AD DS) that you are managing.

- A computer must be available with Group Policy Management and Active Directory Administration Center installed.
- A file server must be available to host roaming user profiles.
  - If the file share uses DFS Namespaces, the DFS folders (links) must have a single target to prevent users from making conflicting edits on different servers.
  - If the file share uses DFS Replication to replicate the contents with another server, users must be able to access only the source server to prevent users from making conflicting edits on different servers.
  - If the file share is clustered, disable continuous availability on the file share to avoid performance issues.
- To use primary computer support in Roaming User Profiles, there are additional client computer and Active Directory schema requirements. For more information, see Deploy Primary Computers for Folder Redirection and Roaming User Profiles.
- The layout of a user's Start menu won't roam on Windows 10, Windows Server 2019, or Windows Server 2016 if they're using more than one PC, Remote Desktop Session Host, or Virtualized Desktop Infrastructure (VDI) server. As a workaround, you can specify a Start layout as described in this topic. Or you can make use of user profile disks, which properly roam Start menu settings when used with Remote Desktop Session Host servers or VDI servers. For more info, see Easier User Data Management with User Profile Disks in Windows Server 2012.

**Considerations when using Roaming User Profiles on multiple versions of Windows**

If you decide to use Roaming User Profiles across multiple versions of Windows, we recommend taking the following actions:

- Configure Windows to maintain separate profile versions for each operating system version. This helps prevent undesirable and unpredictable issues such as profile corruption.
- Use Folder Redirection to store user files such as documents and pictures outside of user profiles. This enables the same files to be available to users across operating system versions. It also keeps profiles small and sign-ins quick.
- Allocate sufficient storage for Roaming User Profiles. If you support two operating system versions, profiles will double in number (and thus total space consumed) because a separate profile is maintained for each operating system version.
- Don't use Roaming User Profiles across computers running Windows Vista/Windows Server 2008 and Windows 7/Windows Server 2008 R2. Roaming between these operating system versions isn't supported due to incompatibilities in their profile versions.
- Inform your users that changes made on one operating system version won't roam to another operating system version.
- When moving your environment to a version of Windows that uses a different profile version (such as from Windows 10 to Windows 10, version 1607—see Appendix B: Profile version reference information for a list), users receive a new, empty roaming user profile. You can minimize the impact of getting a new profile by using Folder Redirection to redirect common folders. There isn't a supported method of migrating roaming user profiles from one profile version to another.

## Step 1: Enable the use of separate profile versions

If you are deploying Roaming User Profiles on computers running Windows 8.1, Windows 8, Windows Server 2012 R2, or Windows Server 2012, we recommend making a couple of changes to your Windows environment prior to deploying. These changes help ensure that future operating system upgrades go smoothly, and facilitate the ability to simultaneously run multiple versions of Windows with Roaming User Profiles.

To make these changes, use the following procedure.

1. Download and install the appropriate software update on all computers on which you're going to use

roaming, mandatory, super-mandatory, or domain default profiles:

- Windows 8.1, or Windows Server 2012 R2: install the software update described in article 2887595 in the Microsoft Knowledge Base (when released).
- Windows 8 or Windows Server 2012: install the software update described in article 2887239 in the Microsoft Knowledge Base.

2. On all computers running Windows 8.1, Windows 8, Windows Server 2012 R2, or Windows Server 2012 on which you will use Roaming User Profiles, use Registry Editor or Group Policy to create the following registry key DWORD Value and set it to `1`. For information about creating registry keys by using Group Policy, see Configure a Registry Item.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ProfSvc\Parameters\UseProfilePathExtensionVersion
```

> **WARNING**
> Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

3. Restart the computers.

## Step 2: Create a Roaming User Profiles security group

If your environment is not already set up with Roaming User Profiles, the first step is to create a security group that contains all users and/or computers to which you want to apply Roaming User Profiles policy settings.

- Administrators of general-purpose roaming user profiles deployments typically create a security group for users.
- Administrators of Remote Desktop Services or virtualized desktop deployments typically use a security group for users and the shared computers.

Here's how to create a security group for Roaming User Profiles:

1. Open Server Manager on a computer with Active Directory Administration Center installed.
2. On the **Tools** menu, select **Active Directory Administration Center**. Active Directory Administration Center appears.
3. Right-click the appropriate domain or OU, select **New**, and then select **Group**.
4. In the **Create Group** window, in the **Group** section, specify the following settings:
   - In **Group name**, type the name of the security group, for example: **Roaming User Profiles Users and Computers**.
   - In **Group scope**, select **Security**, and then select **Global**.
5. In the **Members** section, select **Add**. The Select Users, Contacts, Computers, Service Accounts or Groups dialog box appears.
6. If you want to include computer accounts in the security group, select **Object Types**, select the **Computers** check box and then select **OK**.
7. Type the names of the users, groups, and/or computers to which you want to deploy Roaming User Profiles, select **OK**, and then select **OK** again.

## Step 3: Create a file share for roaming user profiles

If you do not already have a separate file share for roaming user profiles (independent from any shares for redirected folders to prevent inadvertent caching of the roaming profile folder), use the following procedure to create a file share on a server running Windows Server.

> **NOTE**
> Some functionality might differ or be unavailable depending on the version of Windows Server you're using.

Here's how to create a file share on Windows Server:

1. In the Server Manager navigation pane, select **File and Storage Services**, and then select **Shares** to display the Shares page.
2. In the Shares tile, select **Tasks**, and then select **New Share**. The New Share Wizard appears.
3. On the **Select Profile** page, select **SMB Share – Quick**. If you have File Server Resource Manager installed and are using folder management properties, instead select **SMB Share - Advanced**.
4. On the **Share Location** page, select the server and volume on which you want to create the share.
5. On the **Share Name** page, type a name for the share (for example, **User Profiles$**) in the **Share name** box.

   > **TIP**
   > When creating the share, hide the share by putting a `$` after the share name. This hides the share from casual browsers.

6. On the **Other Settings** page, clear the **Enable continuous availability** checkbox, if present, and optionally select the **Enable access-based enumeration** and **Encrypt data access** checkboxes.
7. On the **Permissions** page, select **Customize permissions...**. The Advanced Security Settings dialog box appears.
8. Select **Disable inheritance**, and then select **Convert inherited permissions into explicit permission on this object**.
9. Set the permissions as described in Required permissions for the file share hosting roaming user profiles and shown in the following screen shot, removing permissions for unlisted groups and accounts, and adding special permissions to the Roaming User Profiles Users and Computers group that you created in Step 1.

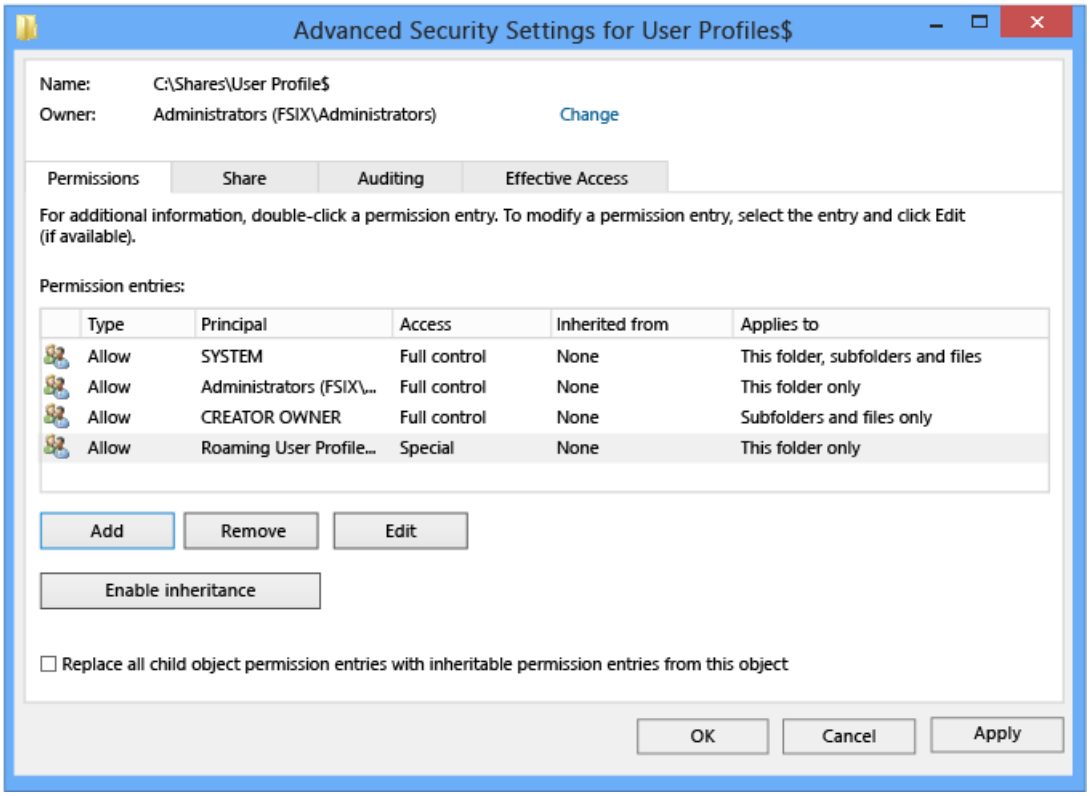



**Figure 1** Setting the permissions for the roaming user profiles share

10. If you chose the **SMB Share - Advanced** profile, on the **Management Properties** page, select the **User Files** Folder Usage value.
11. If you chose the **SMB Share - Advanced** profile, on the **Quota** page, optionally select a quota to apply to users of the share.
12. On the **Confirmation** page, select **Create.**

**Required permissions for the file share hosting roaming user profiles**

| USER ACCOUNT | ACCESS | APPLIES TO |
|---|---|---|
| System | Full control | This folder, subfolders and files |
| Administrators | Full Control | This folder only |
| Creator/Owner | Full Control | Subfolders and files only |
| Security group of users needing to put data on share (Roaming User Profiles Users and Computers) | List folder / read data *(Advanced permissions)*<br>Create folders / append data *(Advanced permissions)* | This folder only |
| Other groups and accounts | None (remove) | |

## Step 4: Optionally create a GPO for Roaming User Profiles

If you do not already have a GPO created for Roaming User Profiles settings, use the following procedure to create an empty GPO for use with Roaming User Profiles. This GPO allows you to configure Roaming User Profiles settings (such as primary computer support, which is discussed separately), and can also be used to enable Roaming User Profiles on computers, as is typically done when deploying in virtualized desktop environments or with Remote Desktop Services.

Here's how to create a GPO for Roaming User Profiles:

1. Open Server Manager on a computer with Group Policy Management installed.
2. From the **Tools** menu select **Group Policy Management**. Group Policy Management appears.
3. Right-click the domain or OU in which you want to setup Roaming User Profiles, then select **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, type a name for the GPO (for example, **Roaming User Profile Settings**), and then select **OK**.
5. Right-click the newly created GPO and then clear the **Link Enabled** checkbox. This prevents the GPO from being applied until you finish configuring it.
6. Select the GPO. In the **Security Filtering** section of the **Scope** tab, select **Authenticated Users**, and then select **Remove** to prevent the GPO from being applied to everyone.
7. In the **Security Filtering** section, select **Add**.
8. In the **Select User, Computer, or Group** dialog box, type the name of the security group you created in Step 1 (for example, **Roaming User Profiles Users and Computers**), and then select **OK**.
9. Select the **Delegation** tab, select **Add**, type **Authenticated Users**, select **OK**, and then select **OK** again to accept the default Read permissions.

   This step is necessary due to security changes made in MS16-072.

> **IMPORTANT**
> Due to the security changes made in MS16-072A, you now must give the Authenticated Users group delegated Read permissions to the GPO - otherwise the GPO won't get applied to users, or if it's already applied, the GPO is removed, redirecting user profiles back to the local PC. For more info, see Deploying Group Policy Security Update MS16-072.

## Step 5: Optionally set up Roaming User Profiles on user accounts

If you are deploying Roaming User Profiles to user accounts, use the following procedure to specify roaming user profiles for user accounts in Active Directory Domain Services. If you are deploying Roaming User Profiles to computers, as is typically done for Remote Desktop Services or virtualized desktop deployments, instead use the procedure documented in Step 6: Optionally set up Roaming User Profiles on computers.

> **NOTE**
> If you set up Roaming User Profiles on user accounts by using Active Directory and on computers by using Group Policy, the computer-based policy setting takes precedence.

Here's how to set up Roaming User Profiles on user accounts:

1. In Active Directory Administration Center, navigate to the **Users** container (or OU) in the appropriate domain.
2. Select all users to which you want to assign a roaming user profile, right-click the users and then select **Properties**.
3. In the **Profile** section, select the **Profile path:** checkbox and then enter the path to the file share where you want to store the user's roaming user profile, followed by `%username%` (which is automatically replaced with the user name the first time the user signs in). For example:

`\\fs1.corp.contoso.com\User Profiles$\%username%`

To specify a mandatory roaming user profile, specify the path to the NTuser.man file that you created previously, for example, `fs1.corp.contoso.comUser Profiles$default`. For more information, see Create mandatory user profiles.

4. Select **OK**.

> **NOTE**
>
> By default, deployment of all Windows® Runtime-based (Windows Store) apps is allowed when using Roaming User Profiles. However, when using a special profile, apps are not deployed by default. Special profiles are user profiles where changes are discarded after the user signs out:
>
> To remove restrictions on app deployment for special profiles, enable the **Allow deployment operations in special profiles** policy setting (located in Computer Configuration\Policies\Administrative Templates\Windows Components\App Package Deployment). However, deployed apps in this scenario will leave some data stored on the computer, which could accumulate, for example, if there are hundreds of users of a single computer. To clean up apps, locate or develop a tool that uses the CleanupPackageForUserAsync API to clean up app packages for users who no longer have a profile on the computer.
>
> For additional background information about Windows Store apps, see Manage Client Access to the Windows Store.

## Step 6: Optionally set up Roaming User Profiles on computers

If you are deploying Roaming User Profiles to computers, as is typically done for Remote Desktop Services or virtualized desktop deployments, use the following procedure. If you are deploying Roaming User Profiles to user accounts, instead use the procedure described in Step 5: Optionally set up Roaming User Profiles on user accounts.

You can use Group Policy to apply Roaming User Profiles to computers running Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.

> **NOTE**
>
> If you set up Roaming User Profiles on computers by using Group Policy and on user accounts by using Active Directory, the computer-based policy setting takes precedence.

Here's how to set up Roaming User Profiles on computers:

1. Open Server Manager on a computer with Group Policy Management installed.
2. From the **Tools** menu, select **Group Policy Management**. Group Policy Management will appear.
3. In Group Policy Management, right-click the GPO you created in Step 3 (for example, **Roaming User Profiles Settings**), and then select **Edit**.
4. In the Group Policy Management Editor window, navigate to **Computer Configuration**, then **Policies**, then **Administrative Templates**, then **System**, and then **User Profiles**.
5. Right-click **Set roaming profile path for all users logging onto this computer** and then select **Edit**.

> **TIP**
> A user's home folder, if configured, is the default folder used by some programs such as Windows PowerShell. You can configure an alternative local or network location on a per-user basis by using the **Home folder** section of the user account properties in AD DS. To configure the home folder location for all users of a computer running Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 in a virtual desktop environment, enable the **Set user home folder** policy setting, and then specify the file share and drive letter to map (or specify a local folder). Do not use environment variables or ellipses. The user's alias is appended to the end of the path specified during user sign on.

6. In the **Properties** dialog box, select **Enabled**
7. In the **Users logging onto this computer should use this roaming profile path** box, enter the path to the file share where you want to store the user's roaming user profile, followed by `%username%` (which is automatically replaced with the user name the first time the user signs in). For example:

   ```
   \\fs1.corp.contoso.com\User Profiles$\%username%
   ```

   To specify a mandatory roaming user profile, which is a preconfigured profile to which users cannot make permanent changes (changes are reset when the user signs out), specify the path to the NTuser.man file that you created previously, for example, `\\fs1.corp.contoso.com\User Profiles$\default`. For more information, see Creating a Mandatory User Profile.
8. Select **OK**.

## Step 7: Optionally specify a Start layout for Windows 10 PCs

You can use Group Policy to apply a specific Start menu layout so that users see the same Start layout on all PCs. If users sign in to more than one PC and you want them to have a consistent Start layout across PCs, make sure that the GPO applies to all of their PCs.

To specify a Start layout, do the following:

1. Update your Windows 10 PCs to Windows 10 version 1607 (also known as the Anniversary Update) or newer, and install the March 14th, 2017 cumulative update (KB4013429) or newer.
2. Create a full or partial Start menu layout XML file. To do so, see Customize and export Start layout.
   - If you specify a *full* Start layout, a user can't customize any part of the Start menu. If you specify a *partial* Start layout, users can customize everything but the locked groups of tiles you specify. However, with a partial Start layout, user customizations to the Start menu won't roam to other PCs.
3. Use Group Policy to apply the customized Start layout to the GPO you created for Roaming User Profiles. To do so, see Use Group Policy to apply a customized Start layout in a domain.
4. Use Group Policy to set the following registry value on your Windows 10 PCs. To do so, see Configure a Registry Item.

| ACTION | UPDATE |
|---|---|
| Hive | **HKEY_LOCAL_MACHINE** |
| Key path | **Software\Microsoft\Windows\CurrentVersion\Explorer** |
| Value name | **SpecialRoamingOverrideAllowed** |
| Value type | **REG_DWORD** |

| ACTION | UPDATE |
| --- | --- |
| Value data | **1** (or **0** to disable) |
| Base | **Decimal** |

5. (Optional) Enable first-time logon optimizations to make signing in faster for users. To do so, see Apply policies to improve sign-in time.
6. (Optional) Further decrease sign-in times by removing unnecessary apps from the Windows 10 base image you use to deploy client PCs. Windows Server 2019 and Windows Server 2016 don't have any pre-provisioned apps, so you can skip this step on server images.
   - To remove apps, use the Remove-AppxProvisionedPackage cmdlet in Windows PowerShell to uninstall the following applications. If your PCs are already deployed you can script the removal of these apps using the Remove-AppxPackage.
     - Microsoft.windowscommunicationsapps_8wekyb3d8bbwe
     - Microsoft.BingWeather_8wekyb3d8bbwe
     - Microsoft.DesktopAppInstaller_8wekyb3d8bbwe
     - Microsoft.Getstarted_8wekyb3d8bbwe
     - Microsoft.Windows.Photos_8wekyb3d8bbwe
     - Microsoft.WindowsCamera_8wekyb3d8bbwe
     - Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe
     - Microsoft.WindowsStore_8wekyb3d8bbwe
     - Microsoft.XboxApp_8wekyb3d8bbwe
     - Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
     - Microsoft.ZuneMusic_8wekyb3d8bbwe

> **NOTE**
> Uninstalling these apps decreases sign-in times, but you can leave them installed if your deployment needs any of them.

## Step 8: Enable the Roaming User Profiles GPO

If you set up Roaming User Profiles on computers by using Group Policy, or if you customized other Roaming User Profiles settings by using Group Policy, the next step is to enable the GPO, permitting it to be applied to affected users.

> **TIP**
> If you plan to implement primary computer support, do so now, before you enable the GPO. This prevents user data from being copied to non-primary computers before primary computer support is enabled. For the specific policy settings, see Deploy Primary Computers for Folder Redirection and Roaming User Profiles.

Here's how to enable the Roaming User Profile GPO:

1. Open Group Policy Management.
2. Right-click the GPO that you created and then select **Link Enabled**. A checkbox appears next to the menu item.

## Step 9: Test Roaming User Profiles

To test Roaming User Profiles, sign in to a computer with a user account configured for Roaming User Profiles, or

sign in to a computer configured for Roaming User Profiles. Then confirm that the profile is redirected.

Here's how to test Roaming User Profiles:

1. Sign in to a primary computer (if you enabled primary computer support) with a user account for which you have enabled Roaming User Profiles enabled. If you enabled Roaming User Profiles on specific computers, sign in to one of these computers.
2. If the user has previously signed in to the computer, open an elevated command prompt, and then type the following command to ensure that the latest Group Policy settings are applied to the client computer:

   ```
   GpUpdate /Force
   ```

3. To confirm that the user profile is roaming, open **Control Panel**, select **System and Security**, select **System**, select **Advanced System Settings**, select **Settings** in the User Profiles section and then look for **Roaming** in the **Type** column.

# Appendix A: Checklist for deploying Roaming User Profiles

| STATUS | ACTION |
| --- | --- |
| ☐<br>☐<br>☐<br>☐<br>☐ | 1. Prepare domain<br>- Join computers to domain<br>- Enable the use of separate profile versions<br>- Create user accounts<br>- (Optional) Deploy Folder Redirection |
| ☐ | 2. Create security group for Roaming User Profiles<br>- Group name:<br>- Members: |
| ☐ | 3. Create a file share for Roaming User Profiles<br>- File share name: |
| ☐ | 4. Create a GPO for Roaming User Profiles<br>- GPO name: |
| ☐ | 5. Configure Roaming User Profiles policy settings |
| ☐<br>☐<br>☐ | 6. Enable Roaming User Profiles<br>- Enabled in AD DS on user accounts?<br>- Enabled in Group Policy on computer accounts? |
| ☐ | 7. (Optional) Specify a mandatory Start layout for Windows 10 PCs |
| ☐<br>☐<br>☐<br>☐ | 8. (Optional) Enable primary computer support<br>- Designate primary computers for users<br>- Location of user and primary computer mappings:<br>- (Optional) Enable primary computer support for Folder Redirection<br>- Computer-based or User-based?<br>- (Optional) Enable primary computer support for Roaming User Profiles |
| ☐ | 9. Enable the Roaming User Profiles GPO |

| STATUS | ACTION |
| --- | --- |
| ☐ | 10. Test Roaming User Profiles |

## Appendix B: Profile version reference information

Each profile has a profile version that corresponds roughly to the version of Windows on which the profile is used. For example, Windows 10, version 1703 and version 1607 both use the .V6 profile version. Microsoft creates a new profile version only when necessary to maintain compatibility, which is why not every version of Windows includes a new profile version.

The following table lists the location of Roaming User Profiles on various versions of Windows.

| OPERATING SYSTEM VERSION | ROAMING USER PROFILE LOCATION |
| --- | --- |
| Windows XP and Windows Server 2003 | `\\<servername>\<fileshare>\<username>` |
| Windows Vista and Windows Server 2008 | `\\<servername>\<fileshare>\<username>.V2` |
| Windows 7 and Windows Server 2008 R2 | `\\<servername>\<fileshare>\<username>.V2` |
| Windows 8 and Windows Server 2012 | `\\<servername>\<fileshare>\<username>.V3` (after the software update and registry key are applied)<br>`\\<servername>\<fileshare>\<username>.V2` (before the software update and registry key are applied) |
| Windows 8.1 and Windows Server 2012 R2 | `\\<servername>\<fileshare>\<username>.V4` (after the software update and registry key are applied)<br>`\\<servername>\<fileshare>\<username>.V2` (before the software update and registry key are applied) |
| Windows 10 | `\\<servername>\<fileshare>\<username>.V5` |
| Windows 10, version 1703 and version 1607 | `\\<servername>\<fileshare>\<username>.V6` |

## Appendix C: Working around reset Start menu layouts after upgrades

Here are some ways to work around Start menu layouts getting reset after an in-place upgrade:

- If only one user ever uses the device and the IT Admin uses a managed OS deployment strategy such as Configuration Manager they can do the following:

  1. Export the Start menu layout with Export-Startlayout before the upgrade
  2. Import the Start menu layout with Import-StartLayout after OOBE but before the user signs in

  > **NOTE**
  > Importing a StartLayout modifies the Default User profile. All user profiles created after the import has occurred will get the imported Start-Layout.

- IT Admins can opt to manage Start's Layout with Group Policy. Using Group Policy provides a centralized management solution to apply a standardized Start Layout to users. There are 2 modes to modes to using Group Policy for Start management. Full Lockdown and Partial Lockdown. The full lockdown scenario

prevents the user from making any changes to Start's layout. The partial lockdown scenario allows user to make changes to a specific area of Start. For more info, see Customize and export Start layout.

> **NOTE**
> User made changes in the partial lockdown scenario will still be lost during upgrade.

- Let the Start layout reset occur and allow end users to reconfigure Start. A notification email or other notification can be sent to end users to expect their Start layouts to be reset after the OS upgrade to minimized impact.

## Change history

The following table summarizes some of the most important changes to this topic.

| DATE | DESCRIPTION | REASON |
|---|---|---|
| May 1st, 2019 | Added updates for Windows Server 2019 | |
| April 10th, 2018 | Added discussion of when user customizations to Start are lost after an OS in-place upgrade | Callout known issue. |
| March 13th, 2018 | Updated for Windows Server 2016 | Moved out of Previous Versions library and updated for current version of Windows Server. |
| April 13th, 2017 | Added profile information for Windows 10, version 1703, and clarified how roaming profile versions work when upgrading operating systems—see Considerations when using Roaming User Profiles on multiple versions of Windows. | Customer feedback. |
| March 14th, 2017 | Added optional step for specifying a mandatory Start layout for Windows 10 PCs in Appendix A: Checklist for deploying Roaming User Profiles. | Feature changes in latest Windows update. |
| January 23rd, 2017 | Added a step to Step 4: Optionally create a GPO for Roaming User Profiles to delegate Read permissions to Authenticated Users, which is now required because of a Group Policy security update. | Security changes to Group Policy processing. |
| December 29th, 2016 | Added a link in Step 8: Enable the Roaming User Profiles GPO to make it easier to get info on how to set Group Policy for primary computers. Also fixed a couple references to steps 5 and 6 that had the numbers wrong. | Customer feedback. |
| December 5th, 2016 | Added info explaining a Start menu settings roaming issue. | Customer feedback. |

| DATE | DESCRIPTION | REASON |
| --- | --- | --- |
| July 6th, 2016 | Added Windows 10 profile version suffixes in Appendix B: Profile version reference information. Also removed Windows XP and Windows Server 2003 from the list of supported operating systems. | Updates for the new versions of Windows, and removed info about versions of Windows that are no longer supported. |
| July 7th, 2015 | Added requirement and step to disable continuous availability when using a clustered file server. | Clustered file shares have better performance for small writes (which are typical with roaming user profiles) when continuous availability is disabled. |
| March 19th, 2014 | Capitalized profile version suffixes (.V2, .V3, .V4) in Appendix B: Profile version reference information. | Although Windows is case insensitive, if you use NFS with the file share, it's important to have the correct (uppercase) capitalization for the profile suffix. |
| October 9th, 2013 | Revised for Windows Server 2012 R2 and Windows 8.1, clarified a few things, and added the Considerations when using Roaming User Profiles on multiple versions of Windows and Appendix B: Profile version reference information sections. | Updates for new version; customer feedback. |

## More information

- Deploy Folder Redirection, Offline Files, and Roaming User Profiles
- Deploy Primary Computers for Folder Redirection and Roaming User Profiles
- Implementing User State Management
- Microsoft's Support Statement Around Replicated User Profile Data
- Sideload Apps with DISM
- Troubleshooting packaging, deployment, and query of Windows Runtime-based apps

# Deploy Folder Redirection with Offline Files

11/2/2020 • 10 minutes to read • Edit Online

Applies to: Windows 10, Windows 7, Windows 8, Windows 8.1, Windows Vista, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server (Semi-annual Channel)

This topic describes how to use Windows Server to deploy Folder Redirection with Offline Files to Windows client computers.

For a list of recent changes to this topic, see Change history.

**IMPORTANT**

Due to the security changes made in MS16-072, we updated Step 3: Create a GPO for Folder Redirection of this topic so that Windows can properly apply the Folder Redirection policy (and not revert redirected folders on affected PCs).

## Prerequisites

### Hardware requirements

Folder Redirection requires an x64-based or x86-based computer; it is not supported by Windows® RT.

### Software requirements

Folder Redirection has the following software requirements:

- To administer Folder Redirection, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server (Semi-annual Channel), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.
- Client computers must be joined to the Active Directory Domain Services (AD DS) that you are managing.
- A computer must be available with Group Policy Management and Active Directory Administration Center installed.
- A file server must be available to host redirected folders.
  - If the file share uses DFS Namespaces, the DFS folders (links) must have a single target to prevent users from making conflicting edits on different servers.
  - If the file share uses DFS Replication to replicate the contents with another server, users must be able to access only the source server to prevent users from making conflicting edits on different servers.
  - When using a clustered file share, disable continuous availability on the file share to avoid performance issues with Folder Redirection and Offline Files. Additionally, Offline Files might not transition to offline mode for 3-6 minutes after a user loses access to a continuously available file share, which could frustrate users who aren't yet using the Always Offline mode of Offline Files.

> **NOTE**
> Some newer features in Folder Redirection have additional client computer and Active Directory schema requirements. For more info, see Deploy primary computers, Disable Offline Files on folders, Enable Always Offline mode, and Enable optimized folder moving.

## Step 1: Create a folder redirection security group

If your environment is not already set up with Folder Redirection, the first step is to create a security group that contains all users to which you want to apply Folder Redirection policy settings.

Here's how to create a security group for Folder Redirection:

1. Open Server Manager on a computer with Active Directory Administration Center installed.
2. On the **Tools** menu, select **Active Directory Administration Center**. Active Directory Administration Center appears.
3. Right-click the appropriate domain or OU, select **New**, and then select **Group**.
4. In the **Create Group** window, in the **Group** section, specify the following settings:
   - In **Group name**, type the name of the security group, for example: **Folder Redirection Users**.
   - In **Group scope**, select **Security**, and then select **Global**.
5. In the **Members** section, select **Add**. The Select Users, Contacts, Computers, Service Accounts or Groups dialog box appears.
6. Type the names of the users or groups to which you want to deploy Folder Redirection, select **OK**, and then select **OK** again.

## Step 2: Create a file share for redirected folders

If you do not already have a file share for redirected folders, use the following procedure to create a file share on a server running Windows Server 2012.

> **NOTE**
> Some functionality might differ or be unavailable if you create the file share on a server running another version of Windows Server.

Here's how to create a file share on Windows Server 2019, Windows Server 2016, and Windows Server 2012:

1. In the Server Manager navigation pane, select **File and Storage Services**, and then select **Shares** to display the Shares page.
2. In the **Shares** tile, select **Tasks**, and then select **New Share**. The New Share Wizard appears.
3. On the **Select Profile** page, select **SMB Share – Quick**. If you have File Server Resource Manager installed and are using folder management properties, instead select **SMB Share - Advanced**.
4. On the **Share Location** page, select the server and volume on which you want to create the share.
5. On the **Share Name** page, type a name for the share (for example, **Users$**) in the **Share name** box.

> **TIP**
> When creating the share, hide the share by putting a `$` after the share name. This will hide the share from casual browsers.

6. On the **Other Settings** page, clear the Enable continuous availability checkbox, if present, and optionally select the **Enable access-based enumeration** and **Encrypt data access** checkboxes.
7. On the **Permissions** page, select **Customize permissions...**. The Advanced Security Settings dialog box appears.
8. Select **Disable inheritance**, and then select **Convert inherited permissions into explicit permission on this object**.
9. Set the permissions as described Table 1 and shown in Figure 1, removing permissions for unlisted groups and accounts, and adding special permissions to the Folder Redirection Users group that you created in Step 1.

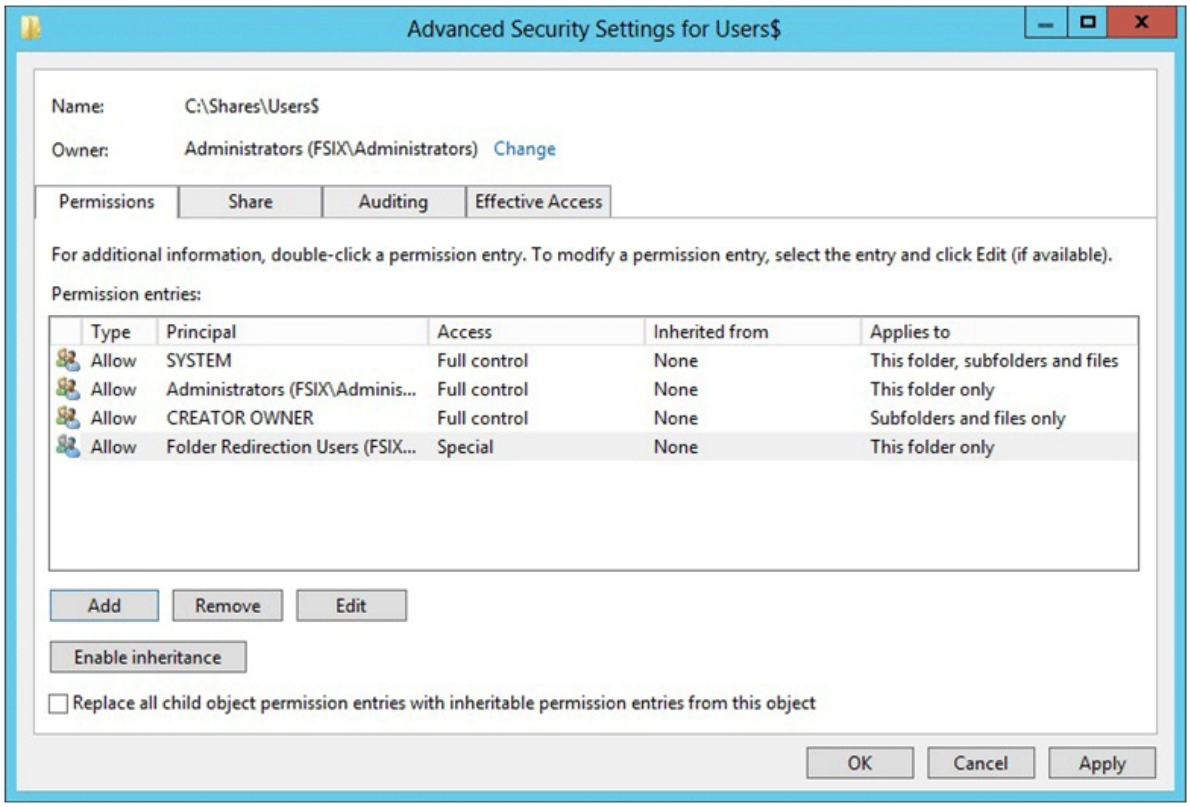



**Figure 1** Setting the permissions for the redirected folders share

10. If you chose the **SMB Share - Advanced** profile, on the **Management Properties** page, select the **User Files** Folder Usage value.
11. If you chose the **SMB Share - Advanced** profile, on the **Quota** page, optionally select a quota to apply to users of the share.
12. On the **Confirmation** page, select **Create.**

**Required permissions for the file share hosting redirected folders**

| USER ACCOUNT | ACCESS | APPLIES TO |
|---|---|---|
| System | Full control | This folder, subfolders and files |
| Administrators | Full Control | This folder only |
| Creator/Owner | Full Control | Subfolders and files only |

| USER ACCOUNT | ACCESS | APPLIES TO |
| --- | --- | --- |
| Security group of users needing to put data on share (Folder Redirection Users) | List folder / read data *(Advanced permissions)*<br>Create folders / append data *(Advanced permissions)*<br>Read attributes *(Advanced permissions)*<br>Read extended attributes *(Advanced permissions)*<br>Read permissions *(Advanced permissions)* | This folder only |
| Other groups and accounts | None (remove) | |

## Step 3: Create a GPO for Folder Redirection

If you do not already have a GPO created for Folder Redirection settings, use the following procedure to create one.

Here's how to create a GPO for Folder Redirection:

1. Open Server Manager on a computer with Group Policy Management installed.
2. From the **Tools** menu, select **Group Policy Management**.
3. Right-click the domain or OU in which you want to setup Folder Redirection, then select **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, type a name for the GPO (for example, **Folder Redirection Settings**), and then select **OK**.
5. Right-click the newly created GPO and then clear the **Link Enabled** checkbox. This prevents the GPO from being applied until you finish configuring it.
6. Select the GPO. In the **Security Filtering** section of the **Scope** tab, select **Authenticated Users**, and then select **Remove** to prevent the GPO from being applied to everyone.
7. In the **Security Filtering** section, select **Add**.
8. In the **Select User, Computer, or Group** dialog box, type the name of the security group you created in Step 1 (for example, **Folder Redirection Users**), and then select **OK**.
9. Select the **Delegation** tab, select **Add**, type **Authenticated Users**, select **OK**, and then select **OK** again to accept the default Read permissions.

   This step is necessary due to security changes made in MS16-072.

> **IMPORTANT**
>
> Due to the security changes made in MS16-072, you now must give the Authenticated Users group delegated Read permissions to the Folder Redirection GPO - otherwise the GPO won't get applied to users, or if it's already applied, the GPO is removed, redirecting folders back to the local PC. For more info, see Deploying Group Policy Security Update MS16-072.

## Step 4: Configure folder redirection with Offline Files

After creating a GPO for Folder Redirection settings, edit the Group Policy settings to enable and configure Folder Redirection, as discussed in the following procedure.

> **NOTE**
>
> Offline Files is enabled by default for redirected folders on Windows client computers, and disabled on computers running Windows Server, unless changed by the user. To use Group Policy to control whether Offline Files is enabled, use the **Allow or disallow use of the Offline Files feature** policy setting. For information about some of the other Offline Files Group Policy settings, see Enable Advanced Offline Files Functionality, and Configuring Group Policy for Offline Files.

Here's how to configure Folder Redirection in Group Policy:

1. In Group Policy Management, right-click the GPO you created (for example, **Folder Redirection Settings**), and then select **Edit**.
2. In the Group Policy Management Editor window, navigate to **User Configuration**, then **Policies**, then **Windows Settings**, and then **Folder Redirection**.
3. Right-click a folder that you want to redirect (for example, **Documents**), and then select **Properties**.
4. In the **Properties** dialog box, from the **Setting** box, select **Basic - Redirect everyone's folder to the same location**.

   > **NOTE**
   >
   > To apply Folder Redirection to client computers running Windows XP or Windows Server 2003, select the **Settings** tab and select the **Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems** checkbox.

5. In the **Target folder location** section, select **Create a folder for each user under the root path** and then in the **Root Path** box, type the path to the file share storing redirected folders, for example: **\\fs1.corp.contoso.com\users$**
6. Select the **Settings** tab, and in the **Policy Removal** section, optionally select **Redirect the folder back to the local userprofile location when the policy is removed** (this setting can help make Folder Redirection behave more predictably for administrators and users).
7. Select **OK**, and then select **Yes** in the Warning dialog box.

## Step 5: Enable the Folder Redirection GPO

Once you have completed configuring the Folder Redirection Group Policy settings, the next step is to enable the GPO, permitting it to be applied to affected users.

> **TIP**
>
> If you plan to implement primary computer support or other policy settings, do so now, before you enable the GPO. This prevents user data from being copied to non-primary computers before primary computer support is enabled.

Here's how to enable the Folder Redirection GPO:

1. Open Group Policy Management.
2. Right-click the GPO that you created, and then select **Link Enabled**. A checkbox will appear next to the menu

item.

## Step 6: Test Folder Redirection

To test Folder Redirection, sign in to a computer with a user account configured for Folder Redirection. Then confirm that the folders and profiles are redirected.

Here's how to test Folder Redirection:

1. Sign in to a primary computer (if you enabled primary computer support) with a user account for which you have enabled Folder Redirection.
2. If the user has previously signed in to the computer, open an elevated command prompt, and then type the following command to ensure that the latest Group Policy settings are applied to the client computer:

   ```
   gpupdate /force
   ```

3. Open File Explorer.
4. Right-click a redirected folder (for example, the My Documents folder in the Documents library), and then select **Properties**.
5. Select the **Location** tab, and confirm that the path displays the file share you specified instead of a local path.

## Appendix A: Checklist for deploying Folder Redirection

| STATUS | ACTION |
| --- | --- |
| ☐<br>☐<br>☐ | 1. Prepare domain<br>- Join computers to domain<br>- Create user accounts |
| ☐ | 2. Create security group for Folder Redirection<br>- Group name:<br>- Members: |
| ☐ | 3. Create a file share for redirected folders<br>- File share name: |
| ☐ | 4. Create a GPO for Folder Redirection<br>- GPO name: |
| ☐<br><br>☐<br>☐<br>☐<br>☐<br>☐ | 5. Configure Folder Redirection and Offline Files policy settings<br>- Redirected folders:<br>- Windows 2000, Windows XP, and Windows Server 2003 support enabled?<br>- Offline Files enabled? (enabled by default on Windows client computers)<br>- Always Offline Mode enabled?<br>- Background file synchronization enabled?<br>- Optimized Move of redirected folders enabled? |

| STATUS | ACTION |
| --- | --- |
| ☐<br><br>☐<br><br>☐<br>☐ | 6. (Optional) Enable primary computer support<br>- Computer-based or User-based?<br>- Designate primary computers for users<br>- Location of user and primary computer mappings:<br>- (Optional) Enable primary computer support for Folder Redirection<br>- (Optional) Enable primary computer support for Roaming User Profiles |
| ☐ | 7. Enable the Folder Redirection GPO |
| ☐ | 8. Test Folder Redirection |

## Change history

The following table summarizes some of the most important changes to this topic.

| DATE | DESCRIPTION | REASON |
| --- | --- | --- |
| January 18, 2017 | Added a step to Step 3: Create a GPO for Folder Redirection to delegate Read permissions to Authenticated Users, which is now required because of a Group Policy security update. | Customer feedback |

## More information

- Folder Redirection, Offline Files, and Roaming User Profiles
- Deploy Primary Computers for Folder Redirection and Roaming User Profiles
- Enable Advanced Offline Files Functionality
- Microsoft's Support Statement Around Replicated User Profile Data
- Sideload Apps with DISM
- Troubleshooting packaging, deployment, and query of Windows Runtime-based apps

# Deploy primary computers for Folder Redirection and Roaming User Profiles

11/2/2020 • 6 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2

This topic describes how to enable primary computer support and designate primary computers for users. Doing so enables you to control which computers use Folder Redirection and Roaming User Profiles.

**IMPORTANT**

When enabling primary computer support for Roaming User Profiles, always enable primary computer support for Folder Redirection as well. This keeps documents and other user files out of the user profiles, which helps profiles remain small and sign on times stay fast.

## Prerequisites

## Software requirements

Primary computer support has the following requirements:

- The Active Directory Domain Services (AD DS) schema must be updated to include Windows Server 2012 schema additions (installing a Windows Server 2012 domain controller automatically updates the schema). For information about updating the AD DS schema, see Adprep.exe integration and Running Adprep.exe.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012.

**TIP**

Although primary computer support requires Folder Redirection and/or Roaming User Profiles, if you are deploying these technologies for the first time, it is best to set up primary computer support before enabling the GPOs that configure Folder Redirection and Roaming User Profiles. This prevents user data from being copied to non-primary computers before primary computer support is enabled. For configuration information, see Deploy Folder Redirection and Deploy Roaming User Profiles.

## Step 1: Designate primary computers for users

The first step in deploying primary computers support is designating the primary computers for each user. To do so, use Active Directory Administration Center to obtain the distinguished name of the relevant computers and then set the **msDs-PrimaryComputer** attribute.

**TIP**

To use Windows PowerShell to work with primary computers, see the blog post Digging a little deeper into Windows 8 Primary Computer.

Here's how to specify the primary computers for users:

1. Open Server Manager on a computer with Active Directory Administration Tools installed.
2. On the **Tools** menu, select **Active Directory Administration Center**. Active Directory Administration Center appears.
3. Navigate to the **Computers** container in the appropriate domain.
4. Right-click a computer that you want to designate as a primary computer and then select **Properties**.
5. In the Navigation pane, select **Extensions**.
6. Select the **Attribute Editor** tab, scroll to **distinguishedName**, select **View**, right-click the value listed, select **Copy**, select **OK**, and then select **Cancel**.
7. Navigate to the **Users** container in the appropriate domain, right-click the user to which you want to assign the computer, and then select **Properties**.
8. In the Navigation pane, select **Extensions**.
9. Select the **Attribute Editor** tab, select **msDs-PrimaryComputer** and then select **Edit**. The Multi-valued String Editor dialog box appears.
10. Right-click the text box, select **Paste**, select **Add**, select **OK**, and then select **OK** again.

## Step 2: Optionally enable primary computers for Folder Redirection in Group Policy

The next step is to optionally configure Group Policy to enable primary computer support for Folder Redirection. Doing so enables a user's folders to be redirected on computers designated as the user's primary computers, but not on any other computers. You can control primary computers for Folder Redirection on a per-computer basis, or a per-user basis.

Here's how to enable primary computers for Folder Redirection:

1. In Group Policy Management, right-click the GPO you created when doing the initial configuration of Folder Redirection and/or Roaming User Profiles (for example, **Folder Redirection Settings** or **Roaming User Profiles Settings**), and then select **Edit**.
2. To enable primary computers support using computer-based Group Policy, navigate to **Computer Configuration**. For user-based Group Policy, navigate to **User Configuration**.
   - Computer-based Group Policy applies primary computer processing to all computers to which the GPO applies, affecting all users of the computers.
   - User-based Group Policy to applies primary computer processing to all user accounts to which the GPO applies, affecting all computers to which the users sign on.
3. Under **Computer Configuration** or **User Configuration**, navigate to **Policies**, then **Administrative Templates**, then **System**, then **Folder Redirection**.
4. Right-click **Redirect folders on primary computers only**, and then select **Edit**.
5. Select **Enabled**, and then select **OK**.

## Step 3: Optionally enable primary computers for Roaming User Profiles in Group Policy

The next step is to optionally configure Group Policy to enable primary computer support for Roaming User Profiles. Doing so enables a user's profile to roam on computers designated as the user's primary computers, but not on any other computers.

Here's how to enable primary computers for Roaming User Profiles:

1. Enable primary computer support for Folder Redirection, if you haven't already.
   This keeps documents and other user files out of the user profiles, which helps profiles remain small and sign

on times stay fast.

2. In Group Policy Management, right-click the GPO you created (for example, **Folder Redirection and Roaming User Profiles Settings**), and then select **Edit**.
3. Navigate to **Computer Configuration**, then **Policies**, then **Administrative Templates**, then **System**, and then **User Profiles**.
4. Right-click **Download roaming profiles on primary computers only,** and then select **Edit**.
5. Select **Enabled**, and then select **OK**.

## Step 4: Enable the GPO

Once you have completed configuring Folder Redirection and Roaming User Profiles, enable the GPO if you have not already. Doing so permits it to be applied to affected users and computers.

Here's how to enable the Folder Redirection and/or Roaming User Profiles GPOs:

1. Open Group Policy Management
2. Right-click the GPOs that you created, and then select **Link Enabled**. A checkbox should appear next to the menu item.

## Step 5: Test primary computer function

To test primary computer support, sign in to a primary computer, confirm that the folders and profiles are redirected, then sign in to a non-primary computer and confirm that the folders and profiles are not redirected.

Here's how to test primary computer functionality:

1. Sign in to a designated primary computer with a user account for which you have enabled Folder Redirection and/or Roaming User Profiles.
2. If the user account has signed on to the computer previously, open a Windows PowerShell session or Command Prompt window as an administrator, type the following command and then sign off when prompted to ensure that the latest Group Policy settings are applied to the client computer:

   ```
   Gpupdate /force
   ```

3. Open File Explorer.
4. Right-click a redirected folder (for example, the My Documents folder in the Documents library), and then select **Properties**.
5. Select the **Location** tab, and confirm that the path displays the file share you specified instead of a local path. To confirm that the user profile is roaming, open **Control Panel**, select **System and Security**, select **System**, select **Advanced System Settings**, select **Settings** in the User Profiles section and then look for **Roaming** in the **Type** column.
6. Sign in with the same user account to a computer that is not designated as the user's primary computer.
7. Repeat steps 2–5, instead looking for local paths and a **Local** profile type.

> **NOTE**
> If folders were redirected on a computer before you enabled primary computer support, the folders will remain redirected unless the following setting is configured in each folder's folder redirection policy setting: **Redirect the folder back to the local userprofile location when the policy is removed**. Similarly, profiles that were previously roaming on a particular computer will show **Roaming** in the **Type** columns; however, the **Status** column will show **Local**.

## More information

- Deploy Folder Redirection with Offline Files
- Deploy Roaming User Profiles
- Folder Redirection, Offline Files, and Roaming User Profiles overview
- Digging a little deeper into Windows 8 Primary Computer

# Disable Offline Files on individual redirected folders

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows (Semi-annual Channel)

This topic describes how to disable Offline Files caching on individual folders that are redirected to network shares by using Folder Redirection. This provides the ability to specify which folders to exclude from caching locally, reducing the Offline Files cache size and time required to synchronize Offline Files.

> **NOTE**
> This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Windows PowerShell Basics.

## Prerequisites

To disable Offline Files caching of specific redirected folders, your environment must meet the following prerequisites.

- An Active Directory Domain Services (AD DS) domain, with client computers joined to the domain. There are no forest or domain functional-level requirements or schema requirements.
- Client computers running Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 or Windows (Semi-annual Channel).
- A computer with Group Policy Management installed.

## Disabling Offline Files on individual redirected folders

To disable Offline Files caching of specific redirected folders, use Group Policy to enable the **Do not automatically make specific redirected folders available offline** policy setting for the appropriate Group Policy Object (GPO). Configuring this policy setting to **Disabled** or **Not Configured** makes all redirected folders available offline.

> **NOTE**
> Only domain administrators, enterprise administrators, and members of the Group Policy creator owners group can create GPOs.

**To disable Offline Files on specific redirected folders**

1. Open **Group Policy Management**.
2. To optionally create a new GPO that specifies which users should have redirected folders excluded from being made available offline, right-click the appropriate domain or organizational unit (OU) and then select **Create a GPO in this domain, and Link it here**.
3. In the console tree, right-click the GPO for which you want to configure the Folder Redirection settings and then select **Edit**. The Group Policy Management Editor appears.
4. In the console tree, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and expand **Folder Redirection**.
5. Right-click **Do not automatically make specific redirected folders available offline** and then select **Edit**.

The **Do not automatically make specific redirected folders available offline** window appears.

6. Select **Enabled**. In the **Options** pane select the folders that should not be made available offline by selecting the appropriate check boxes. Select **OK**.

### Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the procedure described in Disabling Offline Files on individual redirected folders. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

This example creates a new GPO named *Offline Files Settings* in the *MyOu* organizational unit in the *contoso.com* domain (the LDAP distinguished name is "ou=MyOU,dc=contoso,dc=com"). It then disables Offline Files for the Videos redirected folder.

```
New-GPO -Name "Offline Files Settings" | New-Gplink -Target "ou=MyOu,dc=contoso,dc=com" -LinkEnabled Yes

Set-GPRegistryValue –Name "Offline Files Settings" –Key
"HKCU\Software\Policies\Microsoft\Windows\NetCache\{18989B1D-99B5-455B-841C-AB7C74E4DDFC}" -ValueName
DisableFRAdminPinByFolder –Type DWORD –Value 1
```

See the following table for a listing of registry key names (folder GUIDs) to use for each redirected folder.

| REDIRECTED FOLDER | REGISTRY KEY NAME (FOLDER GUID) |
|---|---|
| AppData(Roaming) | {3EB685DB-65F9-4CF6-A03A-E3EF65729F3D} |
| Desktop | {B4BFCC3A-DB2C-424C-B029-7FE99A87C641} |
| Start Menu | {625B53C3-AB48-4EC1-BA1F-A1EF4146FC19} |
| Documents | {FDD39AD0-238F-46AF-ADB4-6C85480369C7} |
| Pictures | {33E28130-4E1E-4676-835A-98395C3BC3BB} |
| Music | {4BD8D571-6D19-48D3-BE97-422220080E43} |
| Videos | {18989B1D-99B5-455B-841C-AB7C74E4DDFC} |
| Favorites | {1777F761-68AD-4D8A-87BD-30B759FA33DD} |
| Contacts | {56784854-C6CB-462b-8169-88E350ACB882} |
| Downloads | {374DE290-123F-4565-9164-39C4925E467B} |
| Links | {BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} |
| Searches | {7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} |
| Saved Games | {4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} |

## More information

- Folder Redirection, Offline Files, and Roaming User Profiles overview
- Deploy Folder Redirection with Offline Files

# Enable Always Offline mode for faster access to files

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, and Windows (Semi-annual Channel)

This document describes how to use the Always Offline mode of Offline Files to provide faster access to cached files and redirected folders. Always Offline also provides lower bandwidth usage because users are always working offline, even when they are connected through a high-speed network connection.

## Prerequisites

To enable Always Offline mode, your environment must meet the following prerequisites.

- An Active Directory Domain Services (AD DS) domain with client computers joined to the domain. There are no forest or domain functional-level requirements or schema requirements.
- Client computers running Windows 10, Windows 8.1, Windows 8, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012. (Client computers running earlier versions of Windows might continue to transition to Online mode on very high-speed network connections.)
- A computer with Group Policy Management installed.

## Enable Always Offline mode

To enable Always Offline mode, use Group Policy to enable the **Configure slow-link mode** policy setting and set the latency to **1** (millisecond). Doing so causes client computers running Windows 8 or Windows Server 2012 to automatically use Always Offline mode.

> **NOTE**
> Computers running Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008 might continue to transition to the Online mode if the latency of the network connection drops below one millisecond.

1. Open **Group Policy Management**.
2. To optionally create a new Group Policy Object (GPO) for Offline Files settings, right-click the appropriate domain or organizational unit (OU), and then select **Create a GPO in this domain, and link it here**.
3. In the console tree, right-click the GPO for which you want to configure the Offline Files settings and then select **Edit**. The **Group Policy Management Editor** appears.
4. In the console tree, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Network**, and expand **Offline Files**.
5. Right-click **Configure slow-link mode**, and then select **Edit**. The **Configure slow-link mode** window will appear.
6. Select **Enabled**.
7. In the **Options** box, select **Show**. The **Show Contents window** will appear.
8. In the **Value name** box, specify the file share for which you want to enable Always Offline mode.
9. To enable Always Offline mode on all file shares, enter *.
10. In the **Value** box, enter **Latency=1** to set the latency threshold to one millisecond, and then select **OK**.

> **NOTE**
>
> By default, when in Always Offline mode, Windows synchronizes files in the Offline Files cache in the background every two hours. To change this value, use the **Configure Background Sync** policy setting.

## More information

- Folder Redirection, Offline Files, and Roaming User Profiles overview
- Deploy Folder Redirection with Offline Files

# Enable optimized moves of redirected folders

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server (Semi-annual Channel)

This topic describes how to perform an optimized move of redirected folders (Folder Redirection) to a new file share. If you enable this policy setting, when an administrator moves the file share hosting redirected folders and updates the target path of the redirected folders in Group Policy, the cached content is simply renamed in the local Offline Files cache without any delays or potential data loss for the user.

Previously, administrators could change the target path of the redirected folders in Group Policy and let the client computers copy the files at the affected user's next sign in, causing a delayed sign in. Alternatively, administrators could move the file share and update the target path of the redirected folders in Group Policy. However, any changes made locally on the client computers between the start of the move and the first sync after the move would be lost.

## Prerequisites

Optimized move has the following requirements:

- Folder Redirection must be setup. For more information see Deploy Folder Redirection with Offline Files.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 or Windows Server (Semi-annual Channel).

## Step 1: Enable optimized move in Group Policy

To optimize the relocation of Folder Redirection data, use Group Policy to enable the **Enable optimized move of contents in Offline Files cache on Folder Redirection server path change** policy setting for the appropriate Group Policy Object (GPO). Configuring this policy setting to **Disabled** or **Not Configured** causes the client to copy all the Folder Redirection content to the new location and then delete the content from the old location if the server path changes.

Here's how to enable optimized moving of redirected folders:

1. In Group Policy Management, right-click the GPO you created for Folder Redirection settings (for example, **Folder Redirection and Roaming User Profiles Settings**), and then select **Edit**.
2. Under **User Configuration**, navigate to **Policies**, then **Administrative Templates**, then **System**, then **Folder Redirection**.
3. Right-click **Enable optimized move of contents in Offline Files cache on Folder Redirection server path change**, and then select **Edit**.
4. Select **Enabled**, and then select **OK**.

## Step 2: Relocate the file share for redirected folders

When moving the file share that contains users' redirected folders, it is important to take precautions to ensure that the folders are relocated properly.

> **IMPORTANT**
> If the users' files are in use or if the full file state is not preserved in the move, users might experience poor performance as the files are copied over the network, synchronization conflicts generated by Offline Files, or even data loss.

1. Notify users in advance that the server hosting their redirected folders will change and recommend that they perform the following actions:

   - Synchronize the contents of their Offline Files cache and resolve any conflicts.
   - Open an elevated command prompt, enter **GpUpdate /Target:User /Force**, and then sign out and sign back in to ensure that the latest Group Policy settings are applied to the client computer

     > **NOTE**
     > By default, client computers update Group Policy every 90 minutes, so if you allow sufficient time for client computers to receive updated policy, you do not need to ask users to use **GpUpdate**.

2. Remove the file share from the server to ensure that no files in the file share are in use. To do so in Server Manager, on the **Shares** page of File and Storage Services, right-click the appropriate file share, then select **Remove**.

   Users will work offline using Offline Files until the move is complete and they receive the updated Folder Redirection settings from Group Policy.

3. Using an account with backup privileges, move the contents of the file share to the new location using a method that preserves file timestamps, such as a backup and restore utility. To use the **Robocopy** command, open an elevated command prompt, and then type the following command, where `<Source>` is the current location of the file share, and `<Destination>` is the new location:

   ```
   Robocopy /B <Source> <Destination> /Copyall /MIR /EFSRAW
   ```

   > **NOTE**
   > The **Xcopy** command does not preserve all of the file state.

4. Edit the Folder Redirection policy settings, updating the target folder location for each redirected folder that you want to relocate. For more information, see Step 4 of Deploy Folder Redirection with Offline Files.

5. Notify users that the server hosting their redirected folders has changed, and that they should use the **GpUpdate /Target:User /Force** command, and then sign out and sign back in to get the updated configuration and resume proper file synchronization.

   Users should sign on to all machines at least once to ensure that the data gets properly relocated in each Offline Files cache.

## More information

- Deploy Folder Redirection with Offline Files
- Deploy Roaming User Profiles
- Folder Redirection, Offline Files, and Roaming User Profiles overview

# Troubleshoot user profiles with events

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows 10, Windows 8, Windows 8.1, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server (Semi-annual Channel).

This topic discusses how to troubleshoot problems loading and unloading user profiles by using events and trace logs. The following sections describe how to use the three event logs that record user profile information.

## Step 1: Checking events in the Application log

The first step in troubleshooting issues with loading and unloading user profiles (including roaming user profiles) is to use Event Viewer to examine any Warning and Error events that User Profile Service records in the Application log.

Here's how to view User Profile Services events in the Application log:

1. Start Event Viewer. To do so, open **Control Panel**, select **System and Security**, and then, in the **Administrative Tools** section, select **View event logs**. The Event Viewer window opens.
2. In the console tree, first navigate to **Windows Logs**, then **Application**.
3. In the Actions pane, select **Filter Current Log**. The Filter Current Log dialog box opens.
4. In the **Event sources** box, select the **User Profiles Service** checkbox, and then select **OK**.
5. Review the listing of events, paying particular attention to Error events.
6. When you find noteworthy events, select the Event Log Online Help link to display additional information and troubleshooting procedures.
7. To perform further troubleshooting, note the date and time of noteworthy events and then examine the Operational log (as described in Step 2) to view details about what the User Profile Service was doing around the time of the Error or Warning events.

> **NOTE**
> You can safely ignore User Profile Service event 1530 "Windows detected your registry file is still in use by other applications or services."

## Step 2: View the Operational log for the User Profile Service

If you cannot resolve the issue using the Application log alone, use the following procedure to view User Profile Service events in the Operational log. This log shows some of the inner workings of the service, and can help pinpoint where in the profile load or unload process the problem is occurring.

Both the Windows Application log and the User Profile Service Operational log are enabled by default in all Windows installations.

Here's how to view the Operational log for the User Profile Service:

1. In the Event Viewer console tree, navigate to **Applications and Services Logs**, then **Microsoft**, then **Windows**, then **User Profile Service**, and then **Operational**.
2. Examine the events that occurred around the time of the Error or Warning events that you noted in the Application log.

## Step 3: Enable and view analytic and debug logs

If you require more detail than the Operational log provides, you can enable analytic and debug logs on the affected computer. This level of logging is much more detailed and should be disabled except when trying to troubleshoot an issue.

Here's how to enable and view analytic and debug logs:

1. In the **Actions** pane of Event Viewer, select **View**, and then select **Show Analytic and Debug Logs**.
2. Navigate to **Applications and Services Logs**, then **Microsoft**, then **Windows**, then **User Profile Service**, and then **Diagnostic**.
3. Select **Enable Log** and then select **Yes**. This enables the Diagnostic log, which will start logging.
4. If you require even more detailed information, see Step 4: Creating and decoding a trace for more information about how to create a trace log.
5. When you are finished troubleshooting the issue, navigate to the **Diagnostic** log, select **Disable Log**, select **View** and then clear the **Show Analytic and Debug Logs** checkbox to hide analytic and debug logging.

## Step 4: Creating and decoding a trace

If you cannot resolve the issue using events, you can create a trace log (an ETL file) while reproducing the issue, and then decode it using public symbols from the Microsoft symbol server. Trace logs provide very specific information about what the User Profile Service is doing, and can help pinpoint where the failure occurred.

The best strategy when using ETL tracing is to first capture the smallest log possible. Once the log is decoded, search the log for failures.

Here's how to create and decode a trace for the User Profile Service:

1. Sign on to the computer where the user is experiencing problems, using an account that is a member of the local Administrators group.
2. From an elevated command prompt enter the following commands, where *<Path>* is the path to a local folder that you have previously created, for example C:\logs:

   ```
   logman create trace -n RUP -o <Path>\RUP.etl -ets
   logman update RUP -p {eb7428f5-ab1f-4322-a4cc-1f1a9b2c5e98} 0x7FFFFFFF 0x7 -ets
   ```

3. From the Start screen, select the user name, and then select **Switch account**, being careful not to log off the administrator. If you are using Remote Desktop, close the Administrator session to establish the user session.
4. Reproduce the problem. The procedure to reproduce the problem is typically to sign on as the user experiencing the issue, sign the user off, or both.
5. After reproducing the problem, sign on as the local administrator again.
6. From an elevated command prompt run the following command to save the log into an ETL file:

   ```
   logman stop -n RUP -ets
   ```

7. Type the following command to export the ETL file into a human-readable file in the current directory (likely your home folder or the %WINDIR%\System32 folder):

   ```
   Tracerpt <path>\RUP.etl
   ```

8. Open the **Summary.txt** file and **Dumpfile.xml** file (you can open them in Microsoft Excel to more easily

view the complete details of the log). Look for events that include **fail** or **failed**; you can safely ignore lines that include the **Unknown** event name.

## More information

- Deploy Roaming User Profiles

# iSCSI Target Server overview

12/16/2020 • 2 minutes to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic provides a brief overview of iSCSI Target Server, a role service in Windows Server that enables you to make storage available via the iSCSI protocol. This is useful for providing access to storage on your Windows server for clients that can't communicate over the native Windows file sharing protocol, SMB.

iSCSI Target Server is ideal for the following:

- **Network and diskless boot** By using boot-capable network adapters or a software loader, you can deploy hundreds of diskless servers. With iSCSI Target Server, the deployment is fast. In Microsoft internal testing, 256 computers deployed in 34 minutes. By using differencing virtual hard disks, you can save up to 90% of the storage space that was used for operating system images. This is ideal for large deployments of identical operating system images, such as on virtual machines running Hyper-V or in high-performance computing (HPC) clusters.
- **Server application storage** Some applications require block storage. iSCSI Target Server can provide these applications with continuously available block storage. Because the storage is remotely accessible, it can also consolidate block storage for central or branch office locations.
- **Heterogeneous storage** iSCSI Target Server supports non-Microsoft iSCSI initiators, making it easy to share storage on servers in a mixed software environment.
- **Development, test, demonstration, and lab environments** When iSCSI Target Server is enabled, a computer running the Windows Server operating system becomes a network-accessible block storage device. This is useful for testing applications prior to deployment in a storage area network (SAN).

## Block storage requirements

Enabling iSCSI Target Server to provide block storage leverages your existing Ethernet network. No additional hardware is needed. If high availability is an important criterion, consider setting up a high-availability cluster. You need shared storage for a high-availability cluster—either hardware for Fibre Channel storage or a serial attached SCSI (SAS) storage array.

If you enable guest clustering, you need to provide block storage. Any servers running Windows Server software with iSCSI Target Server can provide block storage.

## See Also

iSCSI Target Block Storage, How To What's New in iSCSI Target Server in Windows Server

# iSCSI Target Server Scalability Limits

12/16/2020 • 5 minutes to read • Edit Online

Applies To: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic provides the supported and tested Microsoft iSCSI Target Server limits on Windows Server. The following tables display the tested support limits and, where applicable, whether the limits are enforced.

## General limits

| ITEM | SUPPORT LIMIT | ENFORCED? | COMMENT |
|---|---|---|---|
| iSCSI target instances per iSCSI Target Server | 256 | No | |
| iSCSI logical units (LUs) or virtual disks per iSCSI Target Server | 512 | No | Testing configurations included: 8 LUs per target instance with an average over 64 targets, and 256 target instances with one LU per target. |
| iSCSI LUs or virtual disks per iSCSI target instance | 256 (128 on Windows Server 2012) | Yes | |
| Sessions that can simultaneously connect to an iSCSI target instance | 544 (512 on Windows Server 2012) | Yes | |
| Snapshots per LU | 512 | Yes | There is a limit of 512 snapshots per independent iSCSI application volume. |
| Locally mounted virtual disks or snapshots per storage appliance | 32 | Yes | Locally mounted virtual disks don't offer any iSCSI-specific functionality, and are deprecated - for more info, see Features Removed or Deprecated in Windows Server 2012 R2. |

## Fault Tolerance limits

| ITEM | SUPPORT LIMIT | ENFORCED? | COMMENT |
| --- | --- | --- | --- |
| Failover cluster nodes | 8 (5 on Windows Server 2012) | No | |
| Multiple active cluster nodes | Supported | N/A | Each active node in the failover cluster owns a different iSCSI Target Server clustered instance with other nodes acting as possible owner nodes. |
| Error recovery level (ERL) | 0 | Yes | |
| Connections per session | 1 | Yes | |
| Sessions that can simultaneously connect to an iSCSI target instance | 544 (512 on Windows Server 2012) | No | |
| Multipath Input/Output (MPIO) | Supported | N/A | |
| MPIO paths | 4 | No | |
| Converting a stand-alone iSCSI Target Server to a clustered iSCSI Target Server or vice versa | Not supported | No | The iSCSI Target instance and virtual disk configuration data, including snapshot metadata, is lost during conversion. |

## Network limits

| ITEM | SUPPORT LIMIT | ENFORCED? | COMMENT |
| --- | --- | --- | --- |
| Maximum number of active network adapters | 8 | No | Applies to network adapters that are dedicated to iSCSI traffic, rather than the total number of network adapters in the appliance. |
| Portal (IP addresses) supported | 64 | Yes | |

| | | | |
|---|---|---|---|
| Network port speed | 1Gbps, 10 Gbps, 40Gbps, 56 Gbps (Windows Server 2012 R2 and newer only) | No | |
| IPv4 | Supported | N/A | |
| IPv6 | Supported | N/A | |
| TCP offload | Supported | N/A | Leverage Large Send (segmentation), checksum, interrupt moderation, and RSS offload |
| iSCSI offload | Not supported | N/A | |
| Jumbo frames | Supported | N/A | |
| IPSec | Supported | N/A | |
| CRC offload | Supported | N/A | |

# iSCSI virtual disk limits

| ITEM | SUPPORT LIMIT | ENFORCED? | COMMENT |
|---|---|---|---|
| From an iSCSI initiator converting the virtual disk from a basic disk to a dynamic disk | Yes | No | |
| Virtual hard disk format | .vhdx (Windows Server 2012 R2 and newer only)<br>.vhd | | |
| VHD minimum format size | .vhdx: 3 MB<br>.vhd: 8 MB | Yes | Applies to all supported VHD types: parent, differencing, and fixed. |

| | | | |
|---|---|---|---|
| Parent VHD max size | .vhdx: 64 TB<br>.vhd: 2 TB | Yes | |
| Fixed VHD max size | .vhdx: 64 TB<br>.vhd: 16 TB | Yes | |
| Differencing VHD max size | .vhdx: 64 TB<br>.vhd: 2 TB | Yes | |
| VHD fixed format | Supported | No | |
| VHD differencing format | Supported | No | Snapshots cannot be taken of differencing VHD-based iSCSI virtual disks. |
| Number of differencing VHDs per parent VHD | 256 | No (Yes on Windows Server 2012) | Two levels of depth (grandchildren .vhdx files) is the maximum for .vhdx files; one level of depth (child .vhd files) is the maximum for .vhd files. |
| VHD dynamic format | .vhdx: Yes<br>.vhd: Yes (No on Windows Server 2012) | Yes | Unmap isn't supported. |
| exFAT/FAT32/FAT (hosting volume of the VHD) | Not supported | Yes | |
| CSV v2 | Not supported | Yes | |
| ReFS | Supported | N/A | |
| NTFS | Supported | N/A | |
| Non-Microsoft CFS | Not supported | Yes | |

| | | | |
|---|---|---|---|
| Thin provisioning | No | N/A | Dynamic VHDs are supported, but Unmap isn't supported. |
| Logical Unit shrink | Yes (Windows Server 2012 R2 and newer only) | N/A | Use Resize-iSCSIVirtualDisk to shrink a LUN. |
| Logical Unit cloning | Not supported | N/A | You can rapidly clone disk data by using differencing VHDs. |

## Snapshot limits

| ITEM | SUPPORT LIMIT | COMMENT |
|---|---|---|
| Snapshot create | Supported | |
| Snapshot restore | Supported | |
| Writable snapshots | Not supported | |
| Snapshot – convert to full | Not supported | |
| Snapshot – online rollback | Not supported | |
| Snapshot – convert to writable | Not supported | |
| Snapshot - redirection | Not supported | |
| Snapshot - pinning | Not supported | |
| Local mount | Supported | Locally mounted iSCSI virtual disks are deprecated - for more info, see Features Removed or Deprecated in Windows Server 2012 R2. Dynamic disk snapshots cannot be locally mounted. |

## iSCSI Target Server manageability and backup

If you want to create volume shadow copies (VSS open-file snapshots) of data on iSCSI virtual disks from an application server, or you want to manage iSCSI virtual disks with an older app (such as the Diskraid command)

that requires a Virtual Disk Service (VDS) hardware provider, install the iSCSI Target Storage Provider on the server from which you want to take a snapshot or use a VDS management app.

The iSCSI Target Storage Provider is a role service in Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012; you can also download and install iSCSI Target Storage Providers (VDS/VSS) for down-level application servers on the following operating systems as long as the iSCSI Target Server is running on Windows Server 2012:

- Windows Storage Server 2008 R2
- Windows Server 2008 R2
- Windows HPC Server 2008 R2
- Windows HPC Server 2008

Note that if the iSCSI Target Server is hosted by a server running Windows Server 2012 R2 or newer and you want to use VSS or VDS from a remote server, the remote server has to also run the same version of Windows Server and have the iSCSI Target Storage Provider role service installed. Also note that on all versions of Windows you should install only one version of the iSCSI Target Storage Provider role service.

For more info about the iSCSI Target Storage Provider, see iSCSI Target Storage (VDS/VSS) Provider.

## Tested compatibility with iSCSI initiators

We've tested the iSCSI Target Server software with the following iSCSI initiators:

| Initiator | Windows Server 2012 R2 | Windows Server 2012 | Comments |
|---|---|---|---|
| Windows Server 2012 R2 | Validated | | |
| Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 | Validated | Validated | |
| VMWare vSphere 5 | | Validated | |
| VMWare ESXi 5.0 | Validated | | |
| VMWare ESX 4.1 | Validated | | |
| CentOS 6.x | Validated | | Must log out a session and log back in to detect a resized virtual disk. |
| Red Hat Enterprise Linux 6 | Validated | | |

| | | | |
|---|---|---|---|
| RedHat Enterprise Linux 5 and 5 | Validated | Validated | |
| SUSE Linux Enterprise Server 10 | | Validated | |
| Oracle Solaris 11.x | Validated | | |

We've also tested the following iSCSI initiators performing a diskless boot from virtual disks hosted by iSCSI Target Server:

- Windows Server 2012 R2
- Windows Server 2012
- PCIe NIC with iPXE
- CD or USB disk with iPXE

## Additional References

The following list provides additional resources about iSCSI Target Server and related technologies.

- iSCSI Target Block Storage Overview
- iSCSI Target Boot Overview
- Storage in Windows Server

# iSCSI target boot overview

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

iSCSI Target Server in Windows Server can boot hundreds of computers from a single operating system image that is stored in a centralized location. This improves efficiency, manageability, availability, and security.

## Feature description

By using differencing virtual hard disks (VHDs), you can use a single operating system image (the "master image") to boot up to 256 computers. As an example, let's assume that you deployed Windows Server with an operating system image of approximately 20 GB, and you used two mirrored disk drives to act as the boot volume. You would have needed approximately 10 TB of storage for only the operating system image to boot 256 computers. With iSCSI Target Server, you will use 40 GB for the operating system base image, and 2 GB for differencing virtual hard disks per server instance, totaling 552 GB for the operating system images. This provides a savings of over 90% on storage for the operating system images alone.

## Practical applications

Using a controlled operating system image provides the following benefits:

**More secure and easier to manage.** Some enterprises require that data be secured by physically locking storage in a centralized location. In this scenario, servers access the data remotely, including the operating system image. With iSCSI Target Server, administrators can centrally manage the operating system boot images, and control which applications to use for the master image.

**Rapid deployment.** Because the master image is prepared by using Sysprep, when computers boot from the master image, they skip the file copying and installation phase that occurs during Windows Setup, and they go straight to the customization phase. In Microsoft internal testing, 256 computers were deployed in 34 minutes.

**Fast recovery.** Because the operating system images are hosted on the computer running iSCSI Target Server, if a diskless client needs to be replaced, the new computer can point to the operating system image, and boot up immediately.

> **NOTE**
>
> Various vendors provide a storage area network (SAN) boot solution, which can be used by the iSCSI Target Server in Windows Server on commodity hardware.

## Hardware requirements

iSCSI Target Server does not require special hardware for functional verification. In data centers with large-scale deployments, the design should be validated against specific hardware. For reference, Microsoft internal testing indicated that a 256 computer deployment required 24x15k-RPM disks in a RAID 10 configuration for storage. A network bandwidth of 10 GB is optimal. A general estimate is 60 iSCSI boot servers per 1 GB network adapter.

A network adapter is not required for this scenario, and a software boot loader can be used (such as iPXE open source boot firmware).

## Software requirements

iSCSI Target Server can be installed as part of the File and iSCSI Services role service in Server Manager.

> **NOTE**
>
> Booting Nano Server from iSCSI (either from the Windows iSCSI Target Server, or a 3rd party target implementation) is not supported.

## Additional References

- iSCSI Target Server
- iSCSI initiator cmdlets
- iSCSI Target Server cmdlets

# Resilient File System (ReFS) overview

12/16/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server (Semi-Annual Channel)

The Resilient File System (ReFS) is Microsoft's newest file system, designed to maximize data availability, scale efficiently to large data sets across diverse workloads, and provide data integrity by means of resiliency to corruption. It seeks to address an expanding set of storage scenarios and establish a foundation for future innovations.

## Key benefits

**Resiliency**

ReFS introduces new features that can precisely detect corruptions and also fix those corruptions while remaining online, helping provide increased integrity and availability for your data:

- **Integrity-streams** - ReFS uses checksums for metadata and optionally for file data, giving ReFS the ability to reliably detect corruptions.
- **Storage Spaces integration** - When used in conjunction with a mirror or parity space, ReFS can automatically repair detected corruptions using the alternate copy of the data provided by Storage Spaces. Repair processes are both localized to the area of corruption and performed online, requiring no volume downtime.
- **Salvaging data** - If a volume becomes corrupted and an alternate copy of the corrupted data doesn't exist, ReFS removes the corrupt data from the namespace. ReFS keeps the volume online while it handles most non-correctable corruptions, but there are rare cases that require ReFS to take the volume offline.
- **Proactive error correction** - In addition to validating data before reads and writes, ReFS introduces a data integrity scanner, known as a *scrubber*. This scrubber periodically scans the volume, identifying latent corruptions and proactively triggering a repair of corrupt data.

**Performance**

In addition to providing resiliency improvements, ReFS introduces new features for performance-sensitive and virtualized workloads. Real-time tier optimization, block cloning, and sparse VDL are good examples of the evolving capabilities of ReFS, which are designed to support dynamic and diverse workloads:

- **Mirror-accelerated parity** - Mirror-accelerated parity delivers both high performance and also capacity efficient storage for your data.
    - To deliver both high performance and capacity efficient storage, ReFS divides a volume into two logical storage groups, known as tiers. These tiers can have their own drive and resiliency types, allowing each tier to optimize for either performance or capacity. Some example configurations include:

| PERFORMANCE TIER | CAPACITY TIER |
|---|---|
| Mirrored SSD | Mirrored HDD |
| Mirrored SSD | Parity SSD |

| PERFORMANCE TIER | CAPACITY TIER |
| --- | --- |
| Mirrored SSD | Parity HDD |

- Once these tiers are configured, ReFS use them to deliver fast storage for hot data and capacity-efficient storage for cold data:
  - All writes will occur in the performance tier, and large chunks of data that remain in the performance tier will be efficiently moved to the capacity tier in real-time.
  - If using a hybrid deployment (mixing flash and HDD drives), the cache in Storage Spaces Direct helps accelerate reads, reducing the effect of data fragmentation characteristic of virtualized workloads. Otherwise, if using an all-flash deployment, reads also occur in the performance tier.

> **NOTE**
> For Server deployments, mirror-accelerated parity is only supported on Storage Spaces Direct. We recommend using mirror-accelerated parity with archival and backup workloads only. For virtualized and other high performance random workloads, we recommend using three-way mirrors for better performance.

- **Accelerated VM operations** - ReFS introduces new functionality specifically targeted to improve the performance of virtualized workloads:
  - Block cloning - Block cloning accelerates copy operations, enabling quick, low-impact VM checkpoint merge operations.
  - Sparse VDL - Sparse VDL allows ReFS to zero files rapidly, reducing the time needed to create fixed VHDs from 10s of minutes to mere seconds.
- **Variable cluster sizes** - ReFS supports both 4K and 64K cluster sizes. 4K is the recommended cluster size for most deployments, but 64K clusters are appropriate for large, sequential IO workloads.

### Scalability

ReFS is designed to support extremely large data sets--millions of terabytes--without negatively impacting performance, achieving greater scale than prior file systems.

## Supported deployments

Microsoft has developed NTFS specifically for general-purpose use with a wide range of configurations and workloads, however for customers specially requiring the availability, resiliency, and/or scale that ReFS provides, Microsoft supports ReFS for use under the following configurations and scenarios.

> **NOTE**
> All ReFS supported configurations must use Windows Server Catalog certified hardware and meet application requirements.

### Storage Spaces Direct

Deploying ReFS on Storage Spaces Direct is recommended for virtualized workloads or network-attached storage:

- Mirror-accelerated parity and the cache in Storage Spaces Direct deliver high performance and capacity-efficient storage.
- The introduction of block clone and sparse VDL dramatically accelerates .vhdx file operations, such as creation, merge, and expansion.
- Integrity-streams, online repair, and alternate data copies enable ReFS and Storage Spaces Direct to jointly to detect and correct storage controller and storage media corruptions within both metadata and data.

- ReFS provides the functionality to scale and support large data sets.

### Storage Spaces

- Integrity-streams, online repair, and alternate data copies enable ReFS and Storage Spaces to jointly to detect and correct storage controller and storage media corruptions within both metadata and data.
- Storage Spaces deployments can also utilize block-cloning and the scalability offered in ReFS.
- Deploying ReFS on Storage Spaces with shared SAS enclosures is suitable for hosting archival data and storing user documents.

> **NOTE**
> Storage Spaces supports local non-removable direct-attached via BusTypes SATA, SAS, NVME, or attached via HBA (aka RAID controller in pass-through mode).

### Basic disks

Deploying ReFS on basic disks is best suited for applications that implement their own software resiliency and availability solutions.

- Applications that introduce their own resiliency and availability software solutions can leverage integrity-streams, block-cloning, and the ability to scale and support large data sets.

> **IMPORTANT**
> If you plan to use ReFS for CSV (Cluster Shared Volumes), please consider the limitations to pre-format your later CSV volumes with ReFS. For CSV: NTFS should be used for traditional SANs. ReFS should be used on top of S2D.

> **NOTE**
> Basic disks include local non-removable direct-attached via BusTypes SATA, SAS, NVME, or RAID. Basic disks do not include Storage Spaces.

### Backup target

Deploying ReFS as a backup target is best suited for applications and hardware that implement their own resiliency and availability solutions.

- Applications that introduce their own resiliency and availability software solutions can leverage integrity-streams, block-cloning, and the ability to scale and support large data sets.

> **NOTE**
> Backup targets include the above supported configurations. Please contact application and storage array vendors for support details on Fiber Channel and iSCSI SANs. For SANs, if features such as thin provisioning, TRIM/UNMAP, or Offloaded Data Transfer (ODX) are required, NTFS must be used.

## Feature comparison

### Limits

| FEATURE | REFS | NTFS |
| --- | --- | --- |
| Maximum file name length | 255 Unicode characters | 255 Unicode characters |

| FEATURE | REFS | NTFS |
| --- | --- | --- |
| Maximum path name length | 32K Unicode characters | 32K Unicode characters |
| Maximum file size | 35 PB (petabytes) | 256 TB |
| Maximum volume size | 35 PB | 256 TB |

### Functionality

**The following features are available on ReFS and NTFS:**

| FUNCTIONALITY | REFS | NTFS |
| --- | --- | --- |
| BitLocker encryption | Yes | Yes |
| Data Deduplication | Yes[1] | Yes |
| Cluster Shared Volume (CSV) support | Yes[2] [4] | Yes |
| Soft links | Yes | Yes |
| Failover cluster support | Yes | Yes |
| Access-control lists | Yes | Yes |
| USN journal | Yes | Yes |
| Changes notifications | Yes | Yes |
| Junction points | Yes | Yes |
| Mount points | Yes | Yes |
| Reparse points | Yes | Yes |
| Volume snapshots | Yes | Yes |
| File IDs | Yes | Yes |
| Oplocks | Yes | Yes |
| Sparse files | Yes | Yes |
| Named streams | Yes | Yes |
| Thin Provisioning | Yes[3] | Yes |
| Trim/Unmap | Yes[3] | Yes |

1. Available on Windows Server, version 1709 and later, Windows Server 2019 (1809) LTSC or later.
2. Available on Windows Server 2012 R2 and later.
3. Storage Spaces only
4. CSV will not use Direct I/O in junction with Storage Space, Storage Spaces Direct (S2D) or SAN

**The following features are only available on ReFS:**

| FUNCTIONALITY | REFS | NTFS |
|---|---|---|
| Block clone | Yes | No |
| Sparse VDL | Yes | No |
| Mirror-accelerated parity | Yes (on Storage Spaces Direct) | No |

**The following features are unavailable on ReFS at this time:**

| FUNCTIONALITY | REFS | NTFS |
|---|---|---|
| File system compression | No | Yes |
| File system encryption | No | Yes |
| Transactions | No | Yes |
| Hard links | Yes[1] | Yes |
| Object IDs | No | Yes |
| Offloaded Data Transfer (ODX) | No | Yes |
| Short names | No | Yes |
| Extended attributes | No | Yes |
| Disk quotas | No | Yes |
| Bootable | No | Yes |
| Page file support | No | Yes |
| Supported on removable media | No | Yes |

1. Version ReFS 3.5 formatted by Windows 10 Enterprise Insider Preview build 19536. Added hardlink support if **fresh formatted volume. Can't use hardlink if upgraded from previous version**

# Additional References

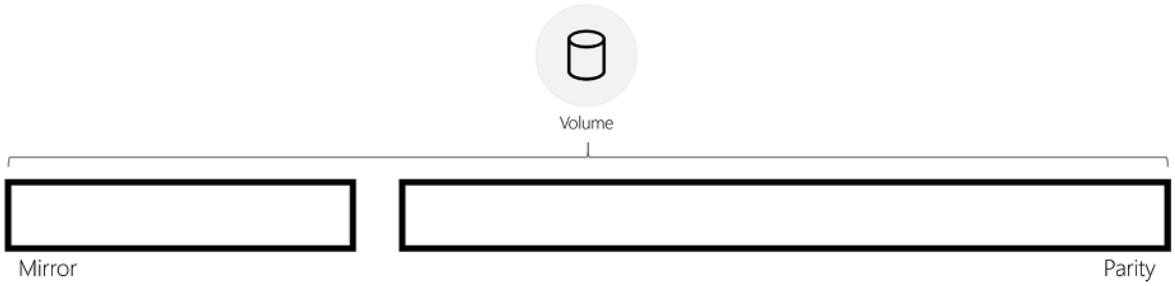
- Cluster size recommendations for ReFS and NTFS
- Storage Spaces Direct overview
- ReFS block cloning
- ReFS integrity streams
- Troubleshoot ReFS with ReFSUtil
- Use of ReFS with Cluster-Shared Volumes
- ReFS versions and compatibility matrix

# Mirror-accelerated parity

12/16/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Storage Spaces can provide fault tolerance for data using two fundamental techniques: mirror and parity. In Storage Spaces Direct, ReFS introduces mirror-accelerated parity, which enables you to create volumes that use both mirror and parity resiliencies. Mirror-accelerated parity offers inexpensive, space-efficient storage without sacrificing performance.




## Background

Mirror and parity resiliency schemes have fundamentally different storage and performance characteristics:

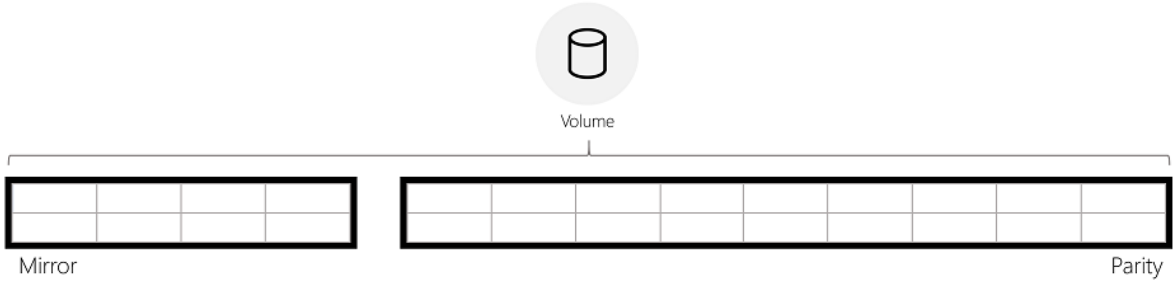
- Mirror resiliency allows users to attain fast write performance, but replicating the data for each copy isn't space efficient.
- Parity, on the other hand, must re-compute parity for every write, causing random write performance to suffer. Parity does, however, allow users to store their data with greater space efficiency. For more info, see Storage Spaces fault tolerance.

Thus, mirror is predisposed to deliver performance-sensitive storage while parity offers improved storage capacity utilization. In mirror-accelerated parity, ReFS leverages the benefits of each resiliency type to deliver both capacity-efficient and performance-sensitive storage by combining both resiliency schemes within a single volume.

## Data rotation on mirror-accelerated parity

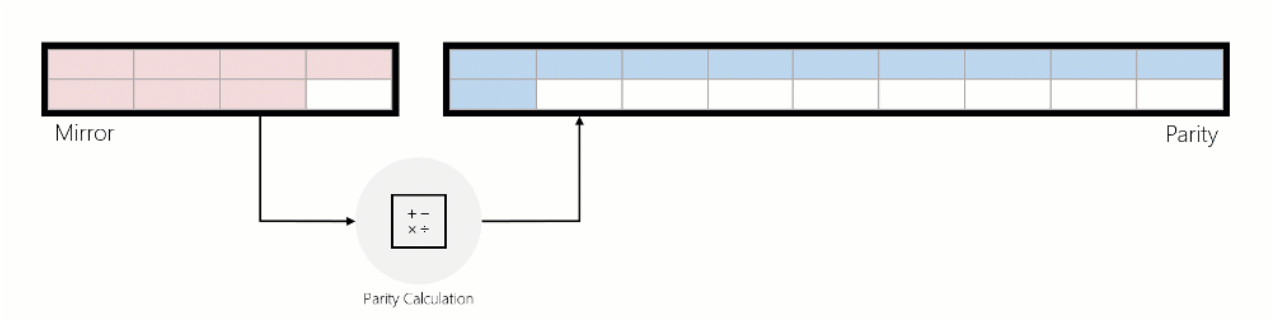
ReFS actively rotates data between mirror and parity, in real-time. This allows incoming writes to be quickly written to mirror then rotated to parity to be stored efficiently. In doing so, incoming IO is serviced quickly in mirror while cold data is stored efficiently in parity, delivering both optimal performance and lost-cost storage within the same volume.

To rotate data between mirror and parity, ReFS logically divides the volume into regions of 64 MiB, which are the unit of rotation. The image below depicts a mirror-accelerated parity volume divided into regions.




ReFS begins rotating full regions from mirror to parity once the mirror tier has reached a specified capacity level. Instead of immediately moving data from mirror to parity, ReFS waits and retains data in mirror as long as possible, allowing ReFS to continue delivering optimal performance for the data (see "IO performance" below).

When data is moved from mirror to parity, the data is read, parity encodings are computed, and then that data is written to parity. The animation below illustrates this using a three-way mirrored region that is converted into an erasure coded region during rotation:



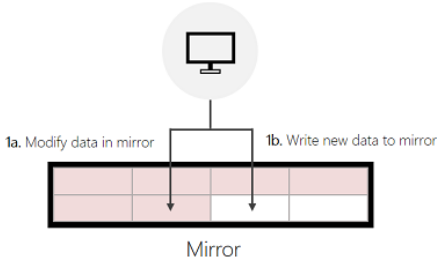

# IO on mirror-accelerated parity

**IO behavior**

**Writes:** ReFS services incoming writes in three distinct ways:

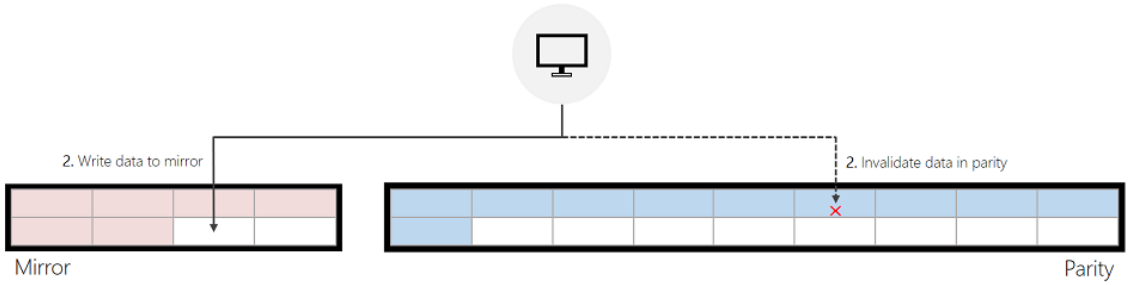
1. **Writes to Mirror:**

   - **1a.** If the incoming write modifies existing data in mirror, ReFS will modify the data in place.
   - **1b.** If the incoming write is a new write, and ReFS can successfully find enough free space in mirror to service this write, ReFS will write to mirror.



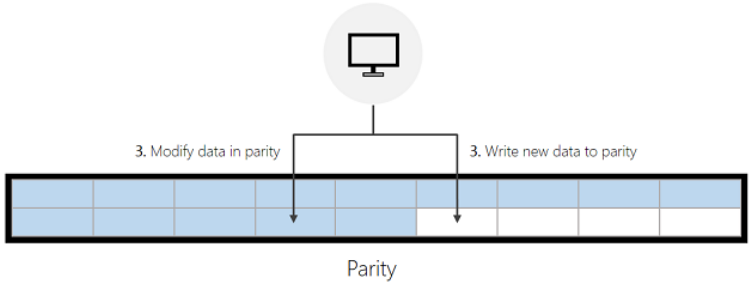

2. **Writes to Mirror, Reallocated from Parity:**

   If the incoming write modifies data that's in parity, and ReFS can successfully find enough free space in mirror to service the incoming write, ReFS will first invalidate the previous data in parity and then write to mirror. This invalidation is a quick and inexpensive metadata operation that helps meaningfully improve write performance made to parity.




3. **Writes to Parity:**

   If ReFS cannot successfully find enough free space in mirror, ReFS will write new data to parity or modify existing data in parity directly. The "Performance optimizations" section below provides guidance that helps minimize writes to parity.




**Reads:** ReFS will read directly from the tier containing the relevant data. If parity is constructed with HDDs, the cache in Storage Spaces Direct will cache this data to accelerate future reads.

> **NOTE**
> Reads never cause ReFS to rotate data back into the mirror tier.

**IO performance**

**Writes:** Each type of write described above has its own performance characteristics. Roughly speaking, writes to the mirror tier are much faster than reallocated writes, and reallocated writes are significantly faster than writes made directly to the parity tier. This relationship is illustrated by the inequality below:

- **Mirror Tier > Reallocated Writes >> Parity Tier**

**Reads:** There is no meaningful, negative performance impact when reading from parity:

- If mirror and parity are constructed with the same media type, read performance will be equivalent.
- If mirror and parity are constructed with different media types—Mirrored SSDs, Parity HDDs, for example—the cache in Storage Spaces Direct will help cache hot data to accelerate any reads from parity.

# ReFS compaction

In this Fall's semi-annual release, ReFS introduces compaction, which substantially improves performance for mirror-accelerated parity volumes that are 90+% full.

**Background:** Previously, as mirror-accelerated parity volumes became full, the performance of these volumes could degrade. The performance degrades because hot and cold data become mixed throughout the volume overtime. This means less hot data can be stored in mirror since cold data occupies space in mirror that could otherwise be used by hot data. Storing hot data in mirror is critical to maintaining high performance because writes directly to mirror are much faster than reallocated writes and orders of magnitude faster than writes directly to parity. Thus, having cold data in mirror is bad for performance, as it reduces the likelihood that ReFS can make writes directly to mirror.

ReFS compaction addresses these performance issues by freeing up space in mirror for hot data. Compaction first consolidates all data—from both mirror and parity—into parity. This reduces fragmentation within the volume and increases the amount of addressable space in mirror. More importantly, this process enables ReFS to consolidate hot data back into mirror:

- When new writes come in, they will be serviced in mirror. Thus, newly written, hot data resides in mirror.
- When a modifying write is made to data in parity, ReFS makes a reallocated write, so this write is serviced in mirror as well. Consequently, hot data that was moved into parity during compaction will be reallocated back into mirror.

## Performance optimizations

> **IMPORTANT**
>
> We recommend placing write-heavy VHDs in different subdirectories. This is because ReFS writes metadata changes at the level of a directory and its files. So if you distribute write-heavy files across directories, metadata operations are smaller and run in parallel, reducing latency for apps.

**Performance counters**

ReFS maintains performance counters to help evaluate the performance of mirror-accelerated parity.

- As described above in the Write to Parity section, ReFS will write directly to parity when it can't find free space in mirror. Generally, this occurs when the mirrored tier fills up faster than ReFS can rotate data to parity. In other words, ReFS rotation is not able to keep up with the ingestion rate. The performance counters below identify when ReFS writes directly to parity:

```
# Windows Server 2016
ReFS\Data allocations slow tier/sec
ReFS\Metadata allocations slow tier/sec

# Windows Server 2019
ReFS\Allocation of Data Clusters on Slow Tier/sec
ReFS\Allocation of Metadata Clusters on Slow Tier/sec
```

- If these counters are non-zero, this indicates ReFS is not rotating data fast enough out of mirror. To help alleviate this, one can either change the rotation aggressiveness or increase the size of the mirrored tier.

**Rotation aggressiveness**

ReFS begins rotating data once mirror has reached a specified capacity threshold.

- Higher values of this rotation threshold cause ReFS to retain data in the mirror tier longer. Leaving hot data in the mirror tier is optimal for performance, but ReFS will not be able to effectively service large amounts of incoming IO.
- Lower values enable ReFS to proactively destage data and better ingest incoming IO. This is applicable to ingest-heavy workloads, such as archival storage. Lower values, however, could degrade performance for general purpose workloads. Unnecessarily rotating data out of the mirror tier carries a performance penalty.

ReFS introduces a tunable parameter to adjust this threshold, which is configurable using a registry key. This registry key must be configured on **each node in a Storage Spaces Direct deployment**, and a restart is required for any changes to take effect.

- **Key:** HKEY_LOCAL_MACHINE\System\CurrentControlSet\Policies
- **ValueName (DWORD):** DataDestageSsdFillRatioThreshold
- **ValueType:** Percentage

If this registry key is not set, ReFS will use a default value of 85%. This default value is recommended for most deployments, and values below 50% are not recommended. The PowerShell command below demonstrates how to set this registry key with a value of 75%:

```
Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Policies -Name DataDestageSsdFillRatioThreshold -Value
75
```

To configure this registry key across each node in a Storage Spaces Direct deployment, you can use the PowerShell command below:

```
$Nodes = 'S2D-01', 'S2D-02', 'S2D-03', 'S2D-04'
Invoke-Command $Nodes {Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Policies -Name
DataDestageSsdFillRatioThreshold -Value 75}
```

**Increasing the size of the mirrored tier**

Increasing the size of the mirrored tier enables ReFS to retain a larger portion of the working set in mirror. This improves the likelihood that ReFS can write directly to mirror, which will help achieve better performance. The PowerShell cmdlets below demonstrate how to increase the size of the mirrored tier:

```
Resize-StorageTier -FriendlyName “Performance” -Size 20GB
Resize-StorageTier -InputObject (Get-StorageTier -FriendlyName “Performance”) -Size 20GB
```

> **TIP**
> Make sure to resize the **Partition** and **Volume** after you resize the **StorageTier**. For more information and examples, see Resize-Volumes.

## Creating a mirror-accelerated parity volume

The PowerShell cmdlet below creates a mirror-accelerated parity volume with a Mirror:Parity ratio of 20:80, which is the recommended configuration for most workloads. For more information and examples, see Creating volumes in Storage Spaces Direct.

```
New-Volume – FriendlyName “TestVolume” -FileSystem CSVFS_ReFS -StoragePoolFriendlyName “StoragePoolName” -
StorageTierFriendlyNames Performance, Capacity -StorageTierSizes 200GB, 800GB
```

## Additional References

- ReFS overview
- ReFS block cloning
- ReFS integrity streams
- Storage Spaces Direct overview

# Block cloning on ReFS

12/16/2020 • 3 minutes to read • Edit Online

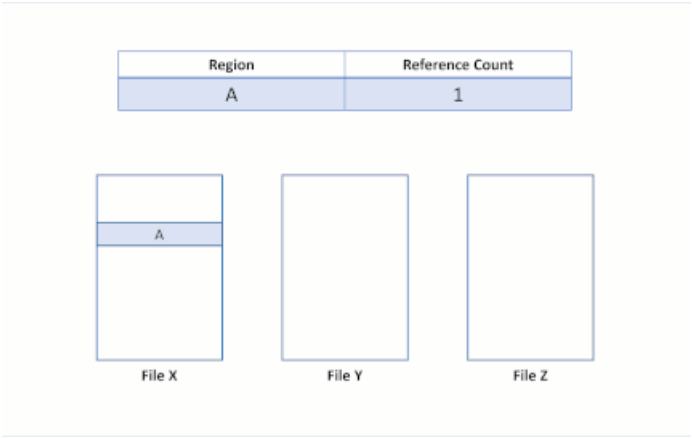
Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

Block cloning instructs the file system to copy a range of file bytes on behalf of an application, where the destination file may be the same as, or different from, the source file. Copy operations, unfortunately, are expensive, since they trigger expensive read and writes to the underlying, physical data.

Block cloning in ReFS, however, performs copies as a low-cost metadata operation rather than reading from and writing to file data. Because ReFS enables multiple files to share the same logical clusters (physical locations on a volume), copy operations only need to remap a region of a file to a separate physical location, converting an expensive, physical operation to a quick, logical one. This allows copies to complete faster and generate less I/O to the underlying storage. This improvement also benefits virtualization workloads, as .vhdx checkpoint merge operations are dramatically accelerated when using block clone operations. Additionally, because multiple files can share the same logical clusters, identical data isn't physically stored multiple times, improving storage capacity.

## How it works

Block cloning on ReFS converts a file data operation into a metadata operation. In order to make this optimization, ReFS introduces reference counts into its metadata for copied regions. This reference count records the number of distinct file regions that reference the same physical regions. This allows multiple files to share the same physical data:




By keeping a reference count for each logical cluster, ReFS doesn't break the isolation between files: writes to shared regions trigger an allocate-on-write mechanism, where ReFS allocates a new region for the incoming write. This mechanism preserves the integrity of the shared logical clusters.

**Example**

Suppose there are two files, X and Y, where each file is composed of three regions, and each region maps to separate logical clusters.

| File X |
| --- |
| A |
| B |
| C |

| File Y |
| --- |
| D |
| E |
| F |

| Region | Reference Count |
| --- | --- |
| A | 1 |
| B | 1 |
| C | 1 |
| D | 1 |
| E | 1 |
| F | 1 |

Now suppose an application issues a block clone operation from File X to File Y, for regions A and B to be copied at the offset of region E. The following file system state would result:

| File X |
| --- |
| A |
| B |
| C |

| File Y |
| --- |
| D |
| A |
| B |

| Region | Reference Count |
| --- | --- |
| A | 2 |
| B | 2 |
| C | 1 |
| D | 1 |
| | |
| | |

This file system state reveals a successful duplication of the block cloned region. Because ReFS performs this copy operation by only updating VCN to LCN mappings, no physical data was read, nor was the physical data in File Y overwritten. File X and Y now share logical clusters, reflected by the reference counts in the table. Because no data was physically copied, ReFS reduces capacity consumption on the volume.

Now suppose the application attempts to overwrite region A in File X. ReFS will duplicate the shared region, update the reference counts appropriately, and perform the incoming write to the newly duplicated region. This ensures that isolation between the files is preserved.

| File X |
| --- |
| G |
| B |
| C |

| File Y |
| --- |
| D |
| A |
| B |

| Region | Reference Count |
| --- | --- |
| A | 1 |
| B | 2 |
| C | 1 |
| D | 1 |
| G | 1 |
| | |

After the modifying write, region B is still shared by both files. Note that if region A were larger than a cluster, only the modified cluster would have been duplicated, and the remaining portion would have remained shared.

## Functionality restrictions and remarks

- The source and destination region must begin and end at a cluster boundary.
- The cloned region must be less than 4GB in length.
- The maximum number of file regions that can map to the same physical region is 8175.
- The destination region must not extend past the end of the file. If the application wishes to extend the destination with cloned data, it must first call SetEndOfFile.
- If the source and destination regions are in the same file, they must not overlap. (The application may be able to proceed by splitting up the block clone operation into multiple block clones that no longer overlap).
- The source and destination files must be on the same ReFS volume.

- The source and destination files must have the same Integrity Streams setting.
- If the source file is sparse, the destination file must also be sparse.
- The block clone operation will break Shared Opportunistic Locks (also know as Level 2 Opportunistic Locks).
- The ReFS volume must have been formatted with Windows Server 2016, and if Failover Clustering is in use, the Clustering Functional Level must have been Windows Server 2016 or later at format time.

## Additional References

- ReFS overview
- ReFS integrity streams
- Storage Spaces Direct overview
- DUPLICATE_EXTENTS_DATA
- FSCTL_DUPLICATE_EXTENTS_TO_FILE

# ReFS integrity streams

12/16/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server (Semi-Annual Channel), Windows 10

Integrity streams is an optional feature in ReFS that validates and maintains data integrity using checksums. While ReFS always uses checksums for metadata, ReFS doesn't, by default, generate or validate checksums for file data. Integrity streams is an optional feature that allows users to utilize checksums for file data. When integrity streams are enabled, ReFS can clearly determine if data is valid or corrupt. Additionally, ReFS and Storage Spaces can jointly correct corrupt metadata and data automatically.

## How it works

Integrity streams can be enabled for individual files, directories, or the entire volume, and integrity stream settings can be toggled at any time. Additionally, integrity stream settings for files and directories are inherited from their parent directories.

Once integrity streams is enabled, ReFS will create and maintain a checksum for the specified file(s) in that file's metadata. This checksum allows ReFS to validate the integrity of the data before accessing it. Before returning any data that has integrity streams enabled, ReFS will first calculate its checksum:

Then, this checksum is compared to the checksum contained in the file metadata. If the checksums match, then the data is marked as valid and returned to the user. If the checksums don't match, then the data is corrupt. The resiliency of the volume determines how ReFS responds to corruptions:

- If ReFS is mounted on a non-resilient simple space or a bare drive, ReFS will return an error to the user without returning the corrupted data.
- If ReFS is mounted on a resilient mirror or parity space, ReFS will attempt to correct the corruption.
  - If the attempt is successful, ReFS will apply a corrective write to restore the integrity of the data, and it will return the valid data to the application. The application remains unaware of any corruptions.
  - If the attempt is unsuccessful, ReFS will return an error.

ReFS will record all corruptions in the System Event Log, and the log will reflect whether the corruptions were fixed.


## Performance

Though integrity streams provides greater data integrity for the system, it also incurs a performance cost. There are a couple different reasons for this:

- If integrity streams are enabled, all write operations become allocate-on-write operations. Though this avoids any read-modify-write bottlenecks since ReFS doesn't need to read or modify any existing data, file data frequently becomes fragmented, which delays reads.
- Depending on the workload and underlying storage of the system, the computational cost of computing and validating the checksum can cause IO latency to increase.

Because integrity streams carries a performance cost, we recommend leaving integrity streams disabled on performance sensitive systems.

## Integrity scrubber

As described above, ReFS will automatically validate data integrity before accessing any data. ReFS also uses a background scrubber, which enables ReFS to validate infrequently accessed data. This scrubber periodically scans the volume, identifies latent corruptions, and proactively triggers a repair of any corrupt data.

> **NOTE**
> The data integrity scrubber can only validate file data for files where integrity streams is enabled.

By default, the scrubber runs every four weeks, though this interval can be configured within Task Scheduler under Microsoft\Windows\Data Integrity Scan.

## Examples

To monitor and change the file data integrity settings, ReFS uses the **Get-FileIntegrity** and **Set-FileIntegrity** cmdlets.

### Get-FileIntegrity

To see if integrity streams is enabled for file data, use the **Get-FileIntegrity** cmdlet.

```
PS C:\> Get-FileIntegrity -FileName 'C:\Docs\TextDocument.txt'
```

You can also use the **Get-Item** cmdlet to get the integrity stream settings for all the files in a specified directory.

```
PS C:\> Get-Item -Path 'C:\Docs\*' | Get-FileIntegrity
```

**Set-FileIntegrity**

To enable/disable integrity streams for file data, use the **Set-FileIntegrity** cmdlet.

```
PS C:\> Set-FileIntegrity -FileName 'H:\Docs\TextDocument.txt' -Enable $True
```

You can also use the **Get-Item** cmdlet to set the integrity stream settings for all the files in a specified folder.

```
PS C:\> Get-Item -Path 'H\Docs\*' | Set-FileIntegrity -Enable $True
```

The **Set-FileIntegrity** cmdlet can also be used on volumes and directories directly.

```
PS C:\> Set-FileIntegrity H:\ -Enable $True
PS C:\> Set-FileIntegrity H:\Docs -Enable $True
```

## Additional References

- ReFS overview
- ReFS block cloning
- Storage Spaces Direct overview

# ReFSUtil

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows 10

ReFSUtil is a tool included in Windows and Windows Server that attempts to diagnose heavily damaged ReFS volumes, identify remaining files, and copy those files to another volume. This comes in Windows 10 in the `%SystemRoot%\Windows\System32` folder or in Windows Server in the `%SystemRoot%\System32` folder.

ReFS salvage is the primary function of ReFSUtil, and is useful for recovering data from volumes that show as RAW in Disk Management. ReFS Salvage has two phases: Scan Phase and a Copy Phase. In automatic mode, the Scan Phase and Copy Phase will run sequentially. In manual mode, each phase can be run separately. Progress and logs are saved in a working directory to allow phases to be run separately as well as Scan Phase to be paused and resumed. You shouldn't need to use the ReFSutil tool unless the volume is RAW. If read-only, then data is still accessible.

## Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| `<source volume>` | Specifies the ReFS volume to process. The drive letter must be formatted as "L:", or you must provide a path to the volume mount point. |
| `<working directory>` | Specifies the location to store temporary information and logs. It must **not** be located on the `<source volume>`. |
| `<target directory>` | Specifies the location where identified files are copied to. It must **not** be located on the `<source volume>`. |
| -m | Recovers all possible files including deleted ones.<br>**WARNING:** Not only does this parameter cause the process to take longer to run, but it can also lead to unexpected results. |
| -v | Specifies to use verbose mode. |
| -x | Forces the volume to dismount first, if necessary. All opened handles to the volume are then invalid. For example, `refsutil salvage -QA R: N:\WORKING N:\DATA -x`. |

## Usage and available options

### Quick automatic mode command line usage

Performs a Quick Scan Phase followed by a Copy Phase. This mode runs quicker as it assumes some critical structures of the volume aren't corrupted and so there's no need to scan the entire volume to locate them. This also reduces the recovery of stale files/directories/volumes.

```
refsutil salvage -QA <source volume> <working directory> <target directory> <options>
```

#### Full automatic mode command line usage

Performs a Full Scan Phase followed by a Copy Phase. This mode may take a long time as it will scan the entire volume for any recoverable files/directories/volumes.

```
refsutil salvage -FA <source volume> <working directory> <target directory> <options>
```

#### Diagnose phase command line usage (manual mode)

First, try to determine if the `<source volume>` is an ReFS volume and determine if the volume is mountable. If a volume isn't mountable, the reason(s) will be provided. This is a standalone phase.

```
refsutil salvage -D <source volume> <working directory> <options>
```

#### Quick Scan phase command line usage

Performs a Quick Scan of the `<source volume>` for any recoverable files. This mode runs quicker as it assumes some critical structures of the volume are not corrupted and so there's no need to scan the entire volume to locate them. This also reduces the recovery of stale files/directories/volumes. Discovered files are logged to the `foundfiles.<volume signature>.txt` file, located in your `<working directory>`. If the Scan Phase was previously stopped, running with the **-QS** flag again resumes the scan from where it left off.

```
refsutil salvage -QS <source volume> <working directory> <options>
```

#### Full Scan phase command line usage

Scans the entire `<source volume>` for any recoverable files. This mode may take a long time as it will scan the entire volume for any recoverable files. Discovered files will be logged to the `foundfiles.<volume signature>.txt` file, located in your `<working directory>`. If the Scan Phase was previously stopped, running with the **-FS** flag again resumes the scan from where it left off.

```
refsutil salvage -FS <source volume> <working directory> <options>
```

#### Copy phase command line usage

Copies all files described in the `foundfiles.<volume signature>.txt` file to your `<target directory>`. If you stop the Scan Phase too early, it's possible that the the `foundfiles.<volume signature>.txt` file might not yet exist, so no file is copied to the `<target directory>`.

```
refsutil salvage -C <source volume> <working directory> <target directory> <options>
```

#### Copy phase with list command line usage

Copies all the files in the `<file list>` from the `<source volume>` to your `<target directory>`. The files in the `<file list>` must have first been identified by the Scan Phase, though the scan need not have been run to completion. The `<file list>` can be generated by copying `foundfiles.<volume signature>.txt` to a new file, removing lines referencing files that shouldn't be restored, and preserving files that should be restored. The PowerShell cmdlet **Select-String** may be helpful in filtering `foundfiles.<volume signature>.txt` to only include desired paths, extensions, or file names.

```
refsutil salvage -SL <source volume> <working directory> <target directory> <file list> <options>
```

**Copy phase with interactive console**

Advanced users can salvage files using an interactive console. This mode also requires files generated from either of the Scan Phases.

```
refsutil salvage -IC <source volume> <working directory> <options>
```

## Additional References

- Command-Line Syntax Key

# Storage Migration Service overview

11/2/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server (Semi-Annual Channel)

Storage Migration Service makes it easier to migrate storage to Windows Server or to Azure. It provides a graphical tool that inventories data on Windows and Linux servers and then transfers the data to newer servers or to Azure virtual machines. Storage Migration Service also provides the option to transfer the identity of a server to the destination server so that apps and users can access their data without changing links or paths.

This topic discusses why you'd want to use Storage Migration Service, how the migration process works, what the requirements are for source and destination servers, and what's new in Storage Migration Service.

## Why use Storage Migration Service

Use Storage Migration Service because you've got a server (or a lot of servers) that you want to migrate to newer hardware or virtual machines. Storage Migration Service is designed to help by doing the following:

- Inventory multiple servers and their data
- Rapidly transfer files, file shares, and security configuration from the source servers
- Optionally take over the identity of the source servers (also known as cutting over) so that users and apps don't have to change anything to access existing data
- Manage one or multiple migrations from the Windows Admin Center user interface

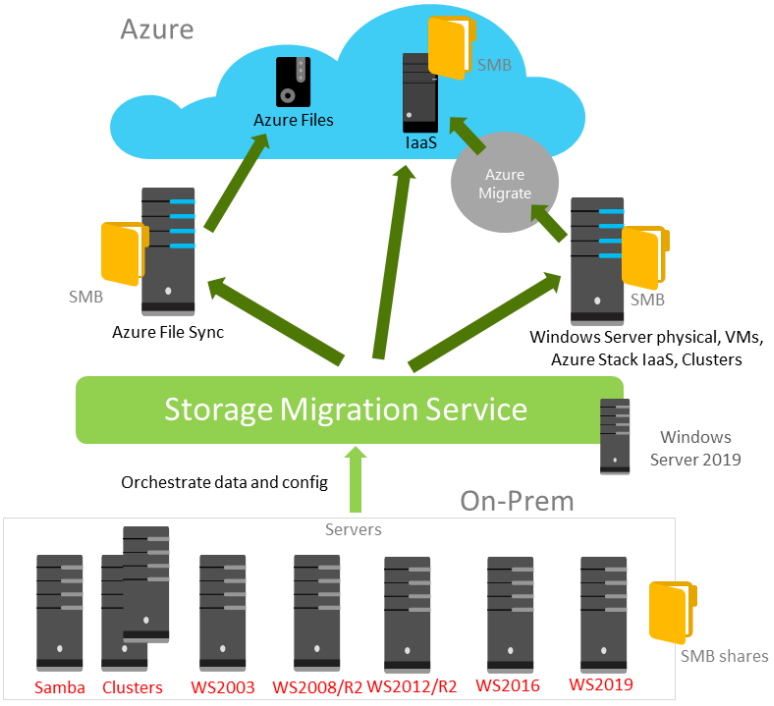



**Figure 1: Storage Migration Service sources and destinations**

## How the migration process works

Migration is a three-step process:

1. **Inventory servers** to gather info about their files and configuration (shown in Figure 2).
2. **Transfer (copy) data** from the source servers to the destination servers.
3. **Cut over to the new servers** (optional).
   The destination servers assume the source servers' former identities so that apps and users don't have to change anything.
   The source servers enter a maintenance state where they still contain the same files they always have (we never remove files from the source servers) but are unavailable to users and apps. You can then decommission the servers at your convenience.

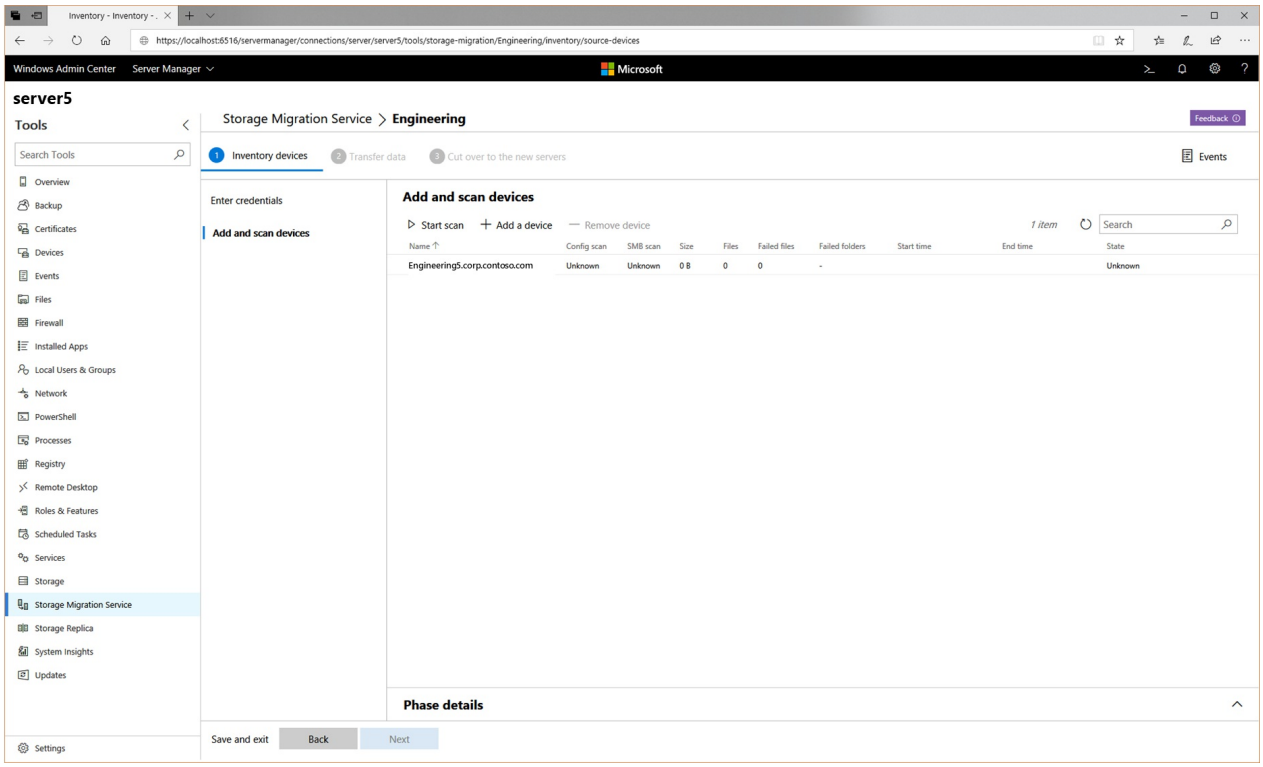



**Figure 2: Storage Migration Service inventorying servers**

Here's a video showing how to use Storage Migration Service to take a server, such as a Windows Server 2008 R2 server that's now out of support, and move the storage to a newer server.

# Requirements

To use Storage Migration Service, you need the following:

- A **source server** or **failover cluster** to migrate files and data from
- A **destination server** running Windows Server 2019 (clustered or standalone) to migrate to. Windows Server 2016 and Windows Server 2012 R2 work as well but are around 50% slower
- An **orchestrator server** running Windows Server 2019 to manage the migration
  If you're migrating only a few servers and one of the servers is running Windows Server 2019, you can use that as the orchestrator. If you're migrating more servers, we recommend using a separate orchestrator server.
- A **PC or server running** Windows Admin Center to run the Storage Migration Service user interface, unless you prefer using PowerShell to manage the migration. The Windows Admin Center and Windows Server 2019 version must both be at least version 1809.

We strongly recommend that the orchestrator and destination computers have at least two cores or two vCPUs, and at least 2 GB of memory. Inventory and transfer operations are significantly faster with more processors and memory.

**Security requirements, the Storage Migration Service proxy service, and firewall ports**

- A migration account that is an administrator on the source computers and the orchestrator computer.
- A migration account that is an administrator on the destination computers and the orchestrator computer.
- The orchestrator computer must have the File and Printer Sharing (SMB-In) firewall rule enabled *inbound*.
- The source and destination computers must have the following firewall rules enabled *inbound* (though you might already have them enabled):
  - File and Printer Sharing (SMB-In)
  - Netlogon Service (NP-In)
  - Windows Management Instrumentation (DCOM-In)
  - Windows Management Instrumentation (WMI-In)

  > **TIP**
  > Installing the Storage Migration Service Proxy service on a Windows Server 2019 computer automatically opens the necessary firewall ports on that computer. To do so, connect to the destination server in Windows Admin Center and then go to **Server Manager** (in Windows Admin Center) > **Roles and features**, select **Storage Migration Service Proxy**, and then select **Install**.

- If the computers belong to an Active Directory Domain Services domain, they should all belong to the same forest. The destination server must also be in the same domain as the source server if you want to transfer the source's domain name to the destination when cutting over. Cutover technically works across domains, but the fully-qualified domain name of the destination will be different from the source...

**Requirements for source servers**

The source server must run one of the following operating systems:

- Windows Server, Semi-Annual Channel
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows Small Business Server 2003 R2
- Windows Small Business Server 2008
- Windows Small Business Server 2011
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials
- Windows Server 2016 Essentials
- Windows Server 2019 Essentials
- Windows Storage Server 2008
- Windows Storage Server 2008 R2
- Windows Storage Server 2012
- Windows Storage Server 2012 R2
- Windows Storage Server 2016

Note: Windows Small Business Server and Windows Server Essentials are domain controllers. Storage Migration

Service can't yet cut over from domain controllers, but can inventory and transfer files from them.

You can migrate the following additional source types if the orchestrator is running Windows Server, version 1903 or later, or if the orchestrator is running an earlier version of Windows Server with KB4512534 installed:

- Failover clusters running Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
- Linux servers that use Samba. We've tested the following:
  - CentOS 7
  - Debian GNU/Linux 8
  - RedHat Enterprise Linux 7.6
  - SUSE Linux Enterprise Server (SLES) 11 SP4
  - Ubuntu 16.04 LTS and 12.04.5 LTS
  - Samba 4.8, 4.7, 4.3, 4.2, and 3.6

**Requirements for destination servers**

The destination server must run one of the following operating systems:

- Windows Server, Semi-Annual Channel
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

> **TIP**
> Destination servers running Windows Server 2019 or Windows Server, Semi-Annual Channel or later have double the transfer performance of earlier versions of Windows Server. This performance boost is due to the inclusion of a built-in Storage Migration Service proxy service, which also opens the necessary firewall ports if they're not already open.

## Azure VM Migration

Windows Admin Center version 1910 allows you to deploy Azure virtual machines. This integrates VM deployment into Storage Migration Service. Instead of building new servers and VMs in the Azure Portal by hand prior to deploying your workload - and possibly missing required steps and configuration - Windows Admin Center can deploy the Azure VM, configure its storage, join it to your domain, install roles, and then set up your distributed system.

Here's a video showing how to use Storage Migration Service to migrate to Azure VMs.

If you want to lift and shift virtual machines to Azure without migrating to a later operating system, consider using Azure Migrate. For more info, see Azure Migrate overview.

## What's new in Storage Migration Service

Windows Admin Center version 1910 adds the ability to deploy Azure virtual machines. This integrates Azure VM deployment into Storage Migration Service. For more info, see Azure VM migration.

The following new features are available when running the Storage Migration Server orchestrator on Windows Server, version 1903 or later, or an earlier version of Windows Server with KB4512534 installed:

- Migrate local users and groups to the new server
- Migrate storage from failover clusters, migrate to failover clusters, and migrate between standalone servers and failover clusters

- Migrate storage from a Linux server that uses Samba
- More easily sync migrated shares into Azure by using Azure File Sync
- Migrate to new networks such as Azure

## Additional References

- Migrate a file server by using Storage Migration Service
- Storage Migration Services frequently asked questions (FAQ)
- Storage Migration Service known issues

# Use Storage Migration Service to migrate a server

11/2/2020 • 9 minutes to read • Edit Online

This topic discusses how to migrate a server, including its files and configuration, to another server by using Storage Migration Service and Windows Admin Center. Migrating takes three steps once you've installed the service and opened any necessary firewall ports: inventory your servers, transfer data, and cut over to the new servers.

## Step 0: Install Storage Migration Service and check firewall ports

Before you get started, install Storage Migration Service and make sure that the necessary firewall ports are open.

1. Check the Storage Migration Service requirements and install Windows Admin Center on your PC or a management server if you haven't already. If migrating domain-joined source computers, you must install and run the Storage Migration Service on a server joined to the same domain or forest as the source computers.

2. In Windows Admin Center, connect to the orchestrator server running Windows Server 2019.
   This is the server that you'll install Storage Migration Service on and use to manage the migration. If you're migrating only one server, you can use the destination server as long as it's running Windows Server 2019. We recommend you use a separate orchestration server for any multi-server migrations.

3. Go to **Server Manager** (in Windows Admin Center) > **Storage Migration Service** and select **Install** to install Storage Migration Service and its required components (shown in Figure 1).

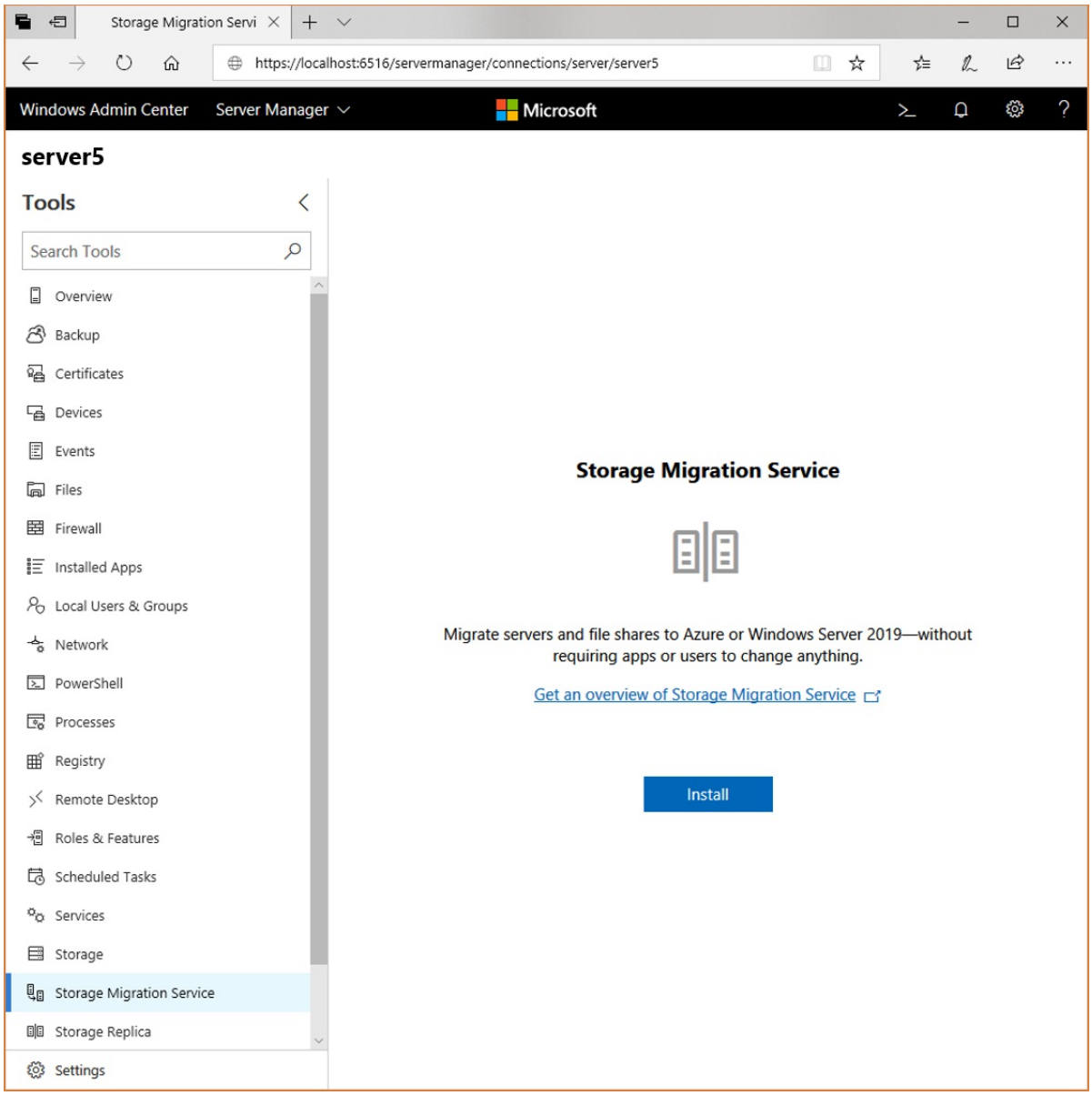



Figure 1: Installing Storage Migration Service

4. Install the Storage Migration Service proxy on all destination servers running Windows Server 2019. This doubles the transfer speed when installed on destination servers.
   To do so, connect to the destination server in Windows Admin Center and then go to **Server Manager** (in Windows Admin Center) > **Roles and features**, > **Features**, select **Storage Migration Service Proxy**, and then select **Install**.

5. If you intend to migrate to or from Windows Failver Clusters, install the Failover Clustering tools on the orchestrator server.
   To do so, connect to the orchestrator server in Windows Admin Center and then go to **Server Manager** (in Windows Admin Center) > **Roles and features**, > **Features**, > **Remote Server Administration Tools**, > **Feature Administration Tools**, select **Failover Clustering Tools**, and then select **Install**.

6. On all source servers and on any destination servers running Windows Server 2012 R2 or Windows Server 2016, in Windows Admin Center, connect to each server, go to **Server Manager** (in Windows Admin Center) > **Firewall** > **Incoming rules**, and then check that the following rules are enabled:

   - File and Printer Sharing (SMB-In)
   - Netlogon Service (NP-In)
   - Windows Management Instrumentation (DCOM-In)
   - Windows Management Instrumentation (WMI-In)

   If you're using third party firewalls, the inbound port ranges to open are TCP/445 (SMB), TCP/135

(RPC/DCOM endpoint mapper), and TCP 1025-65535 (RPC/DCOM ephemeral ports). The Storage Migration service ports are TCP/28940 (Orchestrator) and TCP/28941 (Proxy).

7. If you're using an orchestrator server to manage the migration and you want to download events or a log of what data you transfer, check that the File and Printer Sharing (SMB-In) firewall rule is enabled on that server as well.

## Step 1: Create a job and inventory your servers to figure out what to migrate

In this step, you specify what servers to migrate and then scan them to collect info on their files and configurations.

1. Select **New job**, name the job, and then select whether to migrate Windows servers and clusters or Linux servers that use Samba. Then select **OK**.

2. On the **Enter credentials** page, type admin credentials that work on the servers you want to migrate from, and then select **Next**.
   If you're migrating from Linux servers, instead enter credentials on the **Samba credentials** and **Linux credentials** pages, including an SSH password or private key.

3. Select **Add a device**, type a source server name or the name of a clustered file server, and then select **OK**. Repeat this for any other servers that you want to inventory.

4. Select **Start scan**.
   The page updates to shows when the scan is complete.

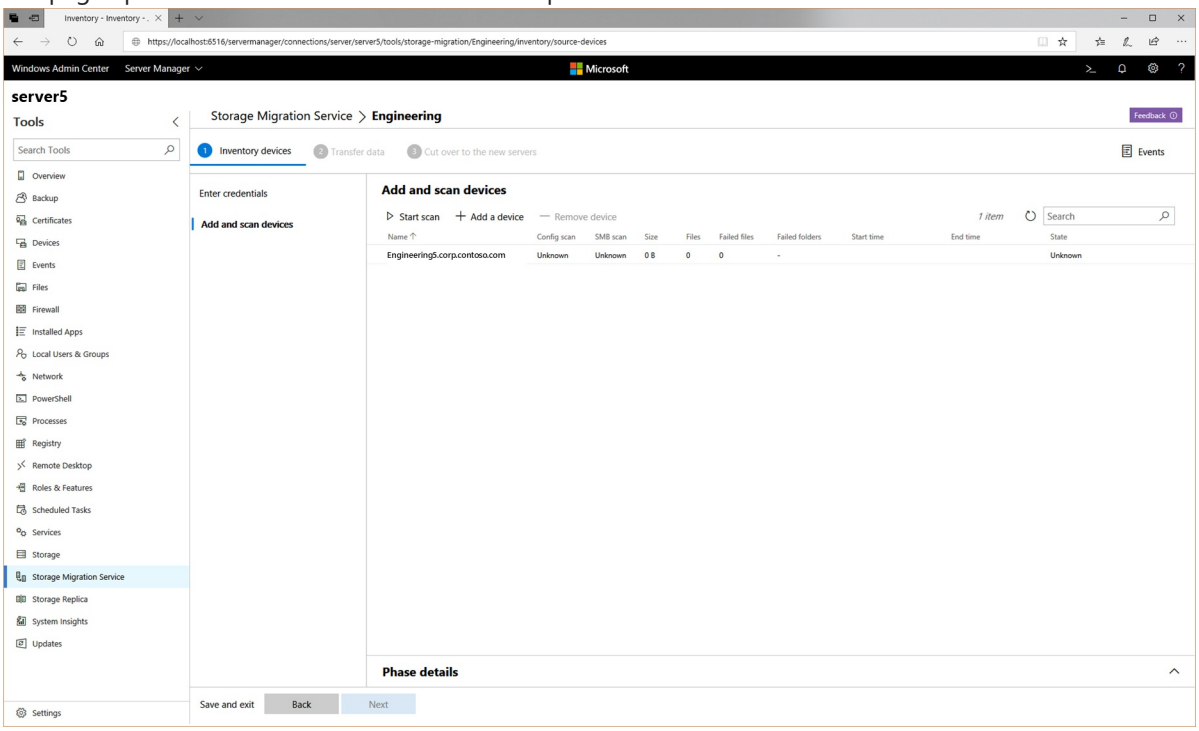



**Figure 2: Inventorying servers**

5. Select each server to review the shares, configuration, network adapters, and volumes that were inventoried.

   Storage Migration Service won't transfer files or folders that we know could interfere with Windows operation, so in this release you'll see warnings for any shares located in the Windows system folder. You'll have to skip these shares during the transfer phase. For more info, see What files and folders are excluded from transfers.

6. Select **Next** to move on to transferring data.

# Step 2: Transfer data from your old servers to the destination servers

In this step you transfer data after specifying where to put it on the destination servers.

1. On the **Transfer data** > **Enter credentials** page, type admin credentials that work on the destination servers you want to migrate to, and then select **Next**.

2. On the **Add a destination device and mappings** page, the first source server is listed. Type the name of the server or clustered file server to which you want to migrate and then select **Scan device**. If migrating from a domain-joined source computer, the destination server must be joined to the same domain. You can also click "Create a new Azure VM" then use the wizard to deploy a new destination server in Azure. This will automatically size your VM, provision storage, format disks, join the domain, and add the Storage Migration Service proxy to a Windows Server 2019 destination. You can choose from Windows Server 2019 (recommended), Windows Server 2016, and Windows Server 2012 R2 VMs of any size and use managed disks.

   > **NOTE**
   >
   > Using "Create a new Azure VM" requires that you have:
   >
   > - A valid Azure subscription.
   > - An existing Azure Compute resource group where you have Create rights.
   > - An existing Azure Virtual Network and subnet.
   > - An Azure Express Route or VPN solution tied to the Virtual Network and subnet that allows connectivity from this Azure IaaS VM to your on-premises clients, domain controllers, the Storage Migration Service orchestrator computer, the Windows Admin Center computer, and the source computer to be migrated.

   Here's a video showing how to use Storage Migration Service to migrate to Azure VMs.

3. Map the source volumes to destination volumes, clear the **Include** checkbox for any shares you don't want to transfer (including any administrative shares located in the Windows system folder), and then select **Next**.

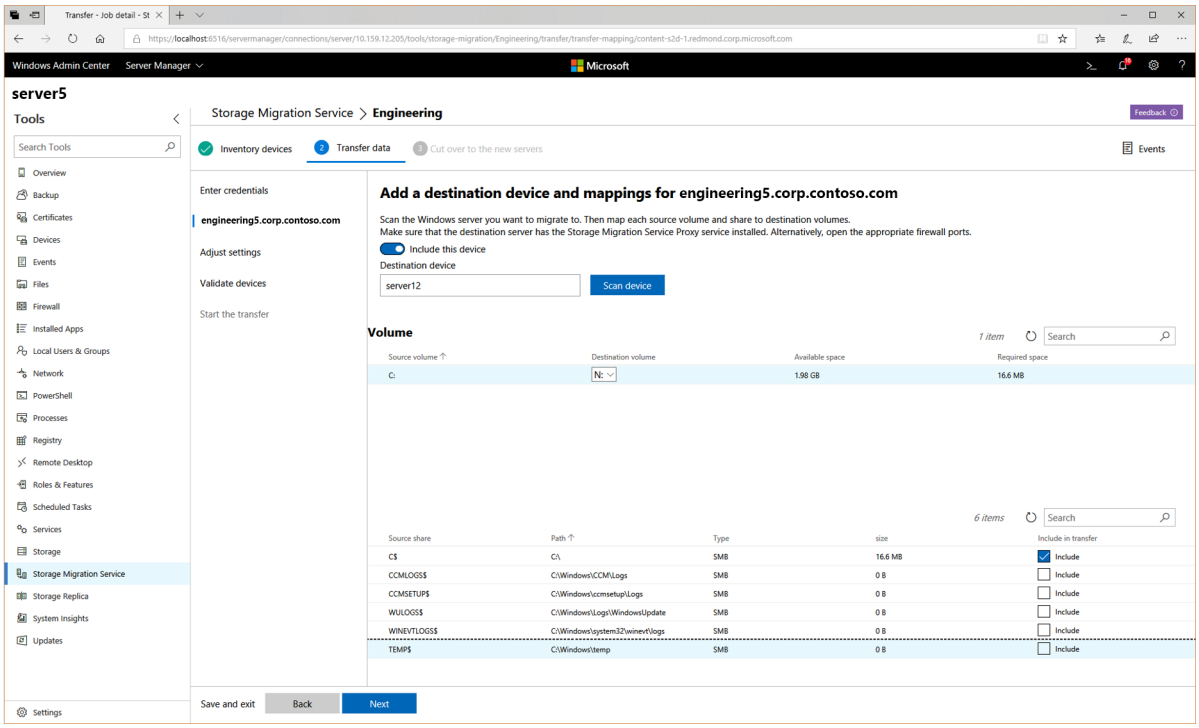



**Figure 3: A source server and where its storage will be transferred to**

4. Add a destination server and mappings for any more source servers, and then select **Next**.

5. On the **Adjust transfer settings** page, specify whether to migrate local users and groups on the source servers and then select **Next**. This lets you recreate any local users and groups on the destination servers so that file or share permissions set to local users and groups aren't lost. Here are the options when migrating local users and groups:

   - **Rename accounts with the same name** is selected by default and migrates all local users and groups on the source server. If it finds local users or groups with the same name on the source and destination, it renames them on the destination unless they're built-in (for example, the Administrator user and the Administrators group). Do not use this setting if your source or destination server is a domain controller.
   - **Reuse accounts with the same name** maps identically named users and groups on the source and destination. Do not use this setting if your source or destination server is a domain controller.
   - **Don't transfer users and groups** skips migrating local users and groups, which is required when your source or destination is a domain controller, or when seeding data for DFS Replication (DFS Replication doesn't support local groups and users).

   > **NOTE**
   > Migrated user accounts are disabled on the destination and assigned a 127-character password that's both complex and random, so you'll have to enable them and assign a new password when you're finished to keep using them. This helps ensure any old accounts with forgotten and weak passwords on the source don't continue to be a security problem on the destination. You might also want to check out Local Administrator Password Solution (LAPS) as a way to manage local Administrator passwords.

6. Select **Validate** and then select **Next**.

7. Select **Start transfer** to start transferring data.
   The first time you transfer, we'll move any existing files in a destination to a backup folder. On subsequent transfers, by default we'll refresh the destination without backing it up first.
   Also, Storage Migration Service is smart enough to deal with overlapping shares—we won't copy the same folders twice in the same job.

8. After the transfer completes, check out the destination server to make sure everything transferred properly. Select **Error log only** if you want to download a log of any files that didn't transfer.

   > **NOTE**
   > If you want to keep an audit trail of transfers or are planning to perform more than one transfer in a job, click **Transfer log** or the other log save options to save a CSV copy. Every subsequent transfer overwrites the database information of a previous run.

At this point, you have three options:

- **Go to the next step**, cutting over so that the destination servers adopt the identities of the source servers.
- **Consider the migration complete** without taking over the source servers' identities.
- **Transfer again**, copying only files that were updated since the last transfer.

If your goal is to sync the files with Azure, you could set up the destination servers with Azure File Sync after transferring files, or after cutting over to the destination servers (see Planning for an Azure File Sync deployment).

## Step 3: Cut over to the new servers

In this step you cut over from the source servers to the destination servers, moving the IP addresses and computer names to the destination servers. After this step is finished, apps and users access the new servers via the names and addresses of the servers you migrated from.

1. If you've navigated away from the migration job, in Windows Admin Center, go to **Server Manager** > **Storage Migration Service** and then select the job that you want to complete.

2. On the **Cut over to the new servers** > **Enter credentials** page, select **Next** to use the credentials you typed previously.

   If your destination is a clustered file server, you might need to provide credentials with permissions to remove the cluster from the domain and then add it back with the new name.

3. On the **Configure cutover** page, specify which network adapter on the destination should take over the settings from each adapter on the source. This moves the IP address from the source to the destination as part of the cutover, giving the source server a new DHCP or static IP address. You have the option to skip all network migrations or certain interfaces.

4. Specify what IP address to use for the source server after cutover moves its address to the destination. You can use DHCP or a static address. If using a static address, the new subnet must be the same as the old subnet or cutover will fail.

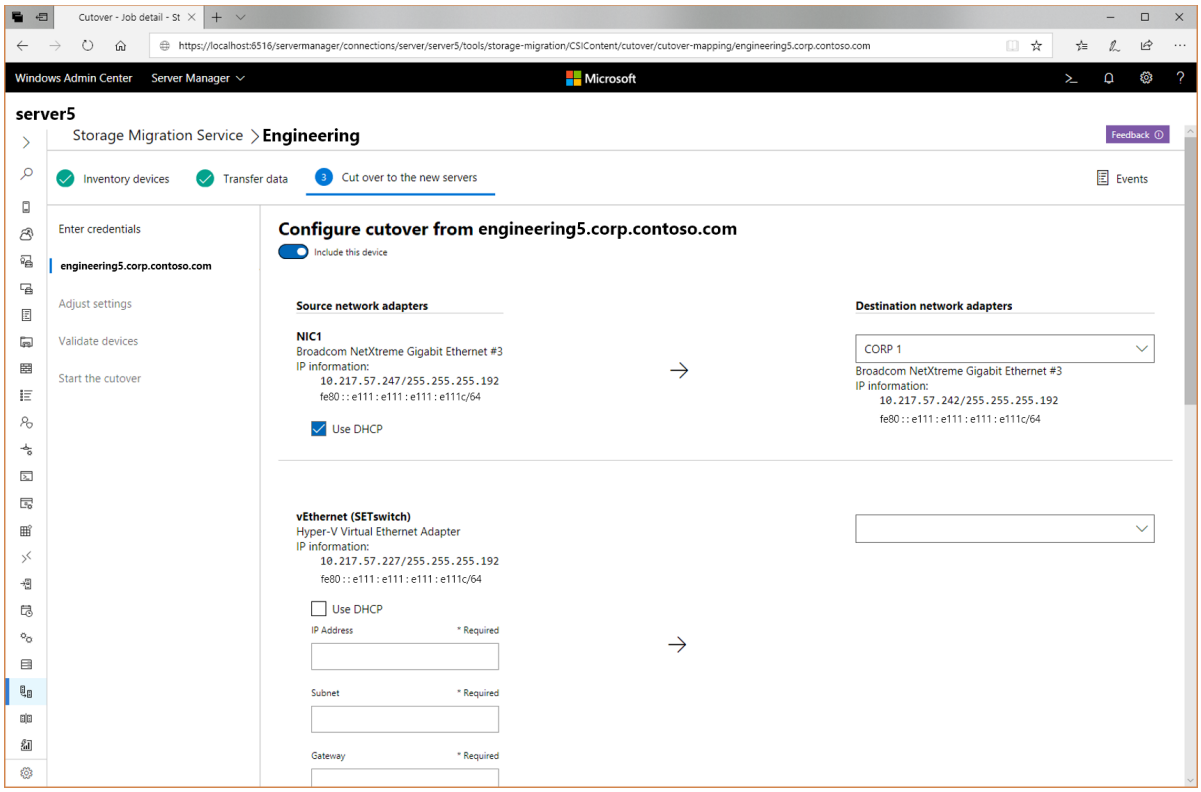



**Figure 4: A source server and how its network configuration will move to the destination**

5. Specify how to rename the source server after the destination server takes over its name. You can use a randomly generated name or type one yourself. Then select **Next**.

6. Select **Next** on the **Adjust cutover settings** page.

7. Select **Validate** on the **Validate source and destination device** page, and then select **Next**.

8. When you're ready to perform the cutover, select **Start cutover**.
   Users and apps might experience an interruption while the address and names are moved and the servers restarted several times each, but will otherwise be unaffected by the migration. How long cutover takes depends on how quickly the servers restart, as well as Active Directory and DNS replication times.

## Additional References

- Storage Migration Service overview
- Storage Migration Services frequently asked questions (FAQ)
- Planning for an Azure File Sync deployment

# How cutover works in Storage Migration Service

11/2/2020 • 7 minutes to read • Edit Online

Cutover is the phase of migration that moves the network identity of the source computer to the destination computer. After cutover, the source computer will still contain the same files as before, but it won't be available to users and apps.

## Summary

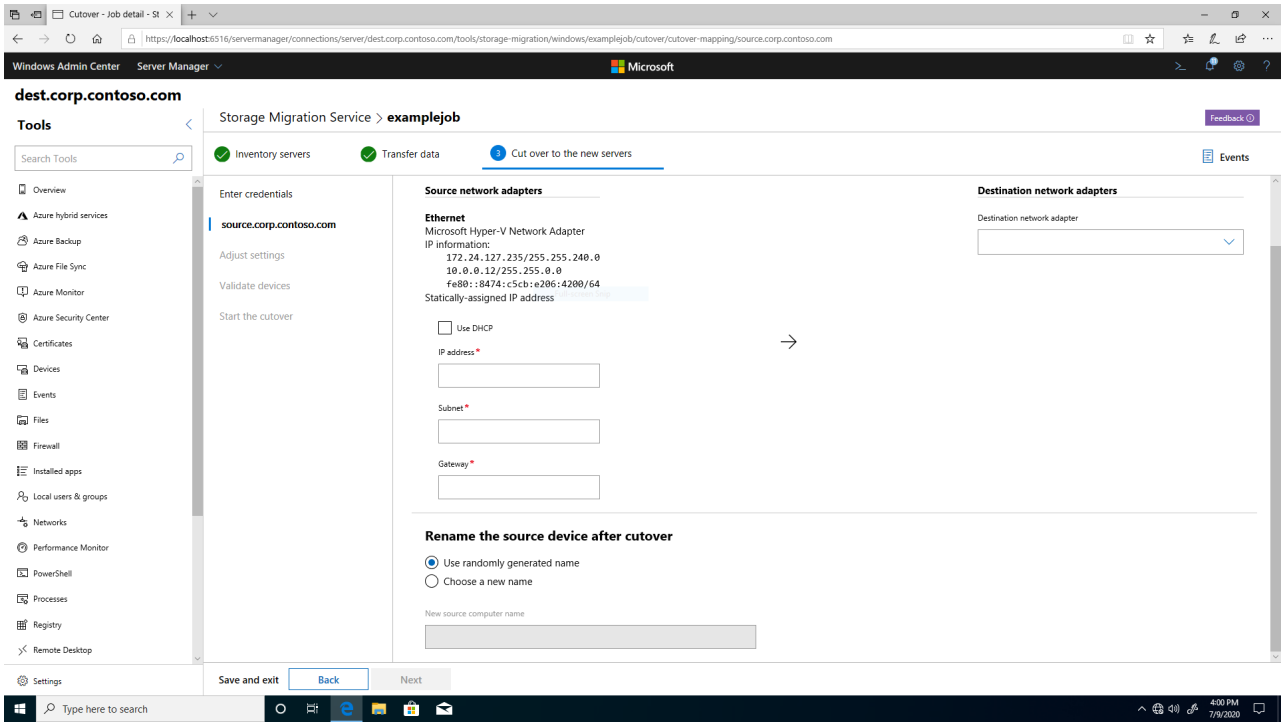



**Figure 1: Storage Migration Service cutover configuration**

Before cutover starts, you provide the network configuration information needed to cut over from the source computer to the destination computer. You can also choose a new unique name for the source computer or let Storage Migration Service create a random one.

Then, Storage Migration Service takes the following steps to cut over the source computer to the destination computer:

1. We connect to the source and destination computers. They should both already have the following firewall rules enabled inbound:
   - File and Printer Sharing (SMB-In), TCP Port 445
   - Netlogon Service (NP-In), TCP Port 445
   - Windows Management Instrumentation (DCOM-In), TCP Port 135
   - Windows Management Instrumentation (WMI-In), TCP, Any Port
2. We set security permissions on the destination computer in Active Directory Domain Services to match the source computer's permissions.
3. We create a temporary local user account on the source computer. If the computer is domain-joined, the account username is "MsftSmsStorMigratSvc". We disable the local account token filter policy on the source computer to allow the account through, and then connect to the source computer. We make this temporary account so that when we restart and remove the source computer from the domain later, we can still access

the source computer.

4. We repeat the previous step on the destination computer.
5. We remove the source computer from the domain to free up its Active Directory account, which the destination computer will later take over.
6. We map network interfaces on the source computer and rename the source computer.
7. We add the source computer back to the domain. The source computer now has a new identity and is available to admins, but not to users and apps.
8. On the source computer, we remove any lingering alternate computer names, remove the temporary local account we created, and re-enable the local account token filter policy.
9. We remove the destination computer from the domain.
10. We replace the IP addresses on the destination computer with the IP information provided by the source, and then rename the destination computer to the source computer's original name.
11. We join the destination computer back to the domain. When joined, it uses the source computer's original Active Directory computer account. This preserves group memberships and security ACLs. The destination computer now has the identity of the source computer.
12. On the destination computer, we remove any lingering alternate computer names, remove the temporary local account we created, and re-enable the local account token filter policy, completing cutover.

After cutover finishes, the destination computer has taken on the identity of the source computer, and you can then decommission the source computer.

## Detailed stages

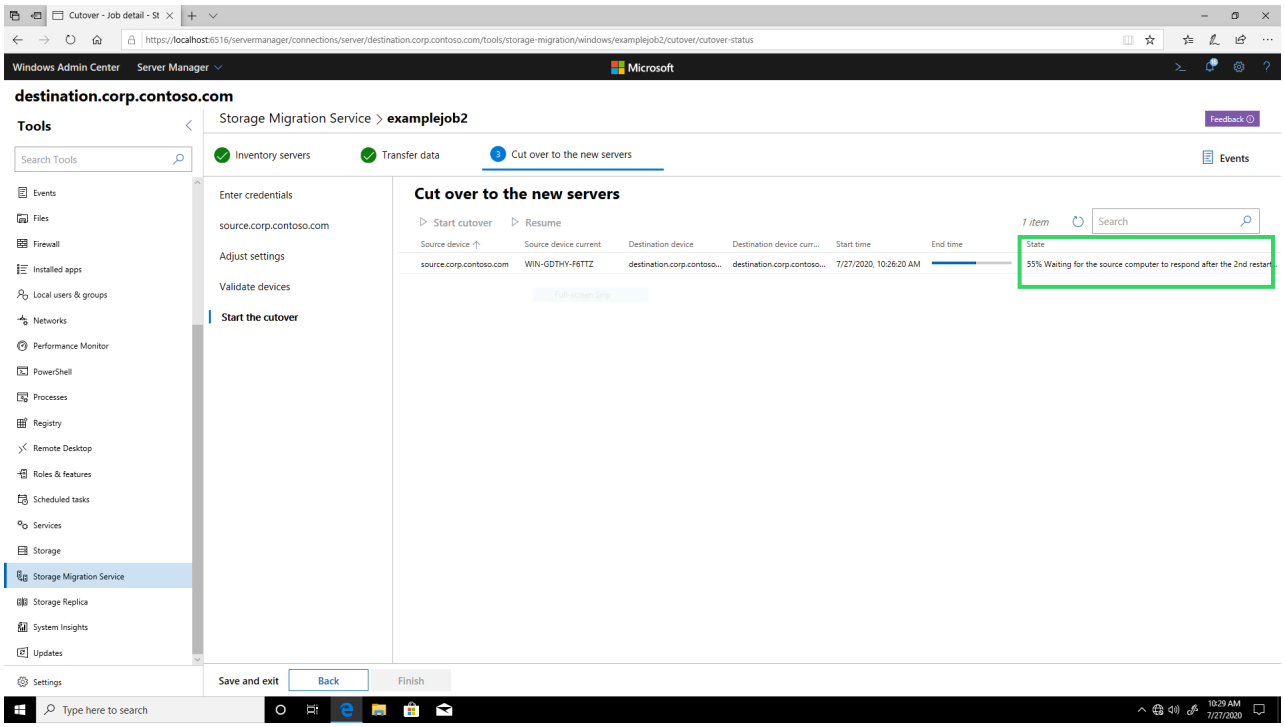



**Figure 2: Storage Migration Service showing a cutover stage description**

You can keep track of cutover progress through descriptions of each stage that appear as shown in the figure above. The following table shows each possible stage along with its progress, description, and any clarifying notes.

| PROGRESS | DESCRIPTION | NOTES |
| --- | --- | --- |
| 0% | The cutover is idle. | |
| 2% | Connecting to the source computer... | Please ensure that the requirements for both source and destination computers are fulfilled. |
| 5% | Connecting to the destination computer... | |
| 6% | Setting security permissions on the computer object in Active Directory... | Replicates the source computer's Active Directory object security permissions on the destination computer. |
| 8% | Making sure that the temporary account that we created was successfully deleted on the source computer... | Makes sure that we can create a temporary account with the same name. |
| 11% | Creating a temporary local user account on the source computer... | If the source computer is domain-joined, the temporary account username is "MsftSmsStorMigratSvc". The password consists of 127 random unicode wide characters with letters, numbers, symbols, and case changes. If the source computer is in a workgroup, we use the original source credentials. |
| 13% | Setting the local account token filter policy on the source computer... | Disables the policy so that we can connect to the source when it's not joined to the domain. Learn more about the local account token filter policy here. |
| 16% | Connecting to the source computer using the temporary local user account... | |
| 19% | Making sure that the temporary account that we created was successfully deleted on the destination computer... | |
| 22% | Creating a temporary local user account on the destination computer... | If the destination computer is domain-joined, the temporary account username is "MsftSmsStorMigratSvc". The password consists of 127 random unicode wide characters with letters, numbers, symbols, and case changes. If the destination computer is in a workgroup, we use the original destination credentials. |
| 25% | Setting the local account token filter policy on the destination computer... | Disables the policy so that we can connect to the destination when it's not joined to the domain. Learn more about the local account token filter policy here. |

| PROGRESS | DESCRIPTION | NOTES |
| --- | --- | --- |
| 27% | Connecting to the destination computer using the temporary local user account... | |
| 30% | Removing the source computer from the domain... | |
| 31% | Collecting the source computer IP addresses. | Applies only to Linux source computers. |
| 33% | Restarting the source computer... (1st restart) | |
| 36% | Waiting for the source computer to respond after the 1st restart... | Likely to become unresponsive if the source computer isn't covered by a DHCP subnet, but you selected DHCP during network configuration. |
| 38% | Mapping network interfaces on the source computer... | |
| 41% | Renaming the source computer... | |
| 42% | Restarting the source computer... (1st restart) | Applies only to Linux source computers. |
| 43% | Restarting the source computer... (2nd restart) | Applies only to domain-joined Windows Server 2003 source computers. |
| 43% | Waiting for the source computer to respond after the 1st restart... | |
| 43% | Waiting for the source computer to respond after the 2nd restart... | |
| 44% | Adding the source computer to the domain... | |
| 47% | Restarting the source computer... (1st restart) | |
| 50% | Restarting the source computer... (2nd restart) | |
| 51% | Restarting the source computer... (3rd restart) | Applies only to Windows Server 2003 source computers. |
| 52% | Waiting for the source computer to respond... | |
| 52% | Waiting for the source computer to respond after the 1st restart... | |

| PROGRESS | DESCRIPTION | NOTES |
| --- | --- | --- |
| 55% | Waiting for the source computer to respond after the 2nd restart... | |
| 56% | Waiting for the source computer to respond after the 3rd restart... | |
| 57% | Removing alternate computer names on the source... | Ensures that the source is unreachable to other users and apps. For more info, see Netdom computername. |
| 58% | Removing a temporary local account we created on the source computer... | |
| 61% | Resetting the local account token filter policy on the source computer... | Enables the policy. |
| 63% | Removing the destination computer from the domain... | |
| 66% | Restarting the destination computer... (1st restart) | |
| 69% | Waiting for the destination computer to respond after the 1st restart... | |
| 72% | Mapping network interfaces on destination computer... | Maps each network adapter and IP address from the source computer onto the destination computer, replacing the destination's network information. |
| 75% | Renaming the destination computer... | |
| 77% | Adding the destination computer to the domain... | The destination computer takes over the old source computer's Active Directory object. This can fail if the destination user isn't a member of Domain Admins or doesn't have admin rights to the source computer Active Directory object. You can specify alternate destination credentials in the "Enter credentials" step before cutover starts. |
| 80% | Restarting the destination computer... (1st restart) | |
| 83% | Restarting the destination computer... (2nd restart) | |
| 84% | Waiting for the destination computer to respond... | |
| 86% | Waiting for the destination computer to respond after the 1st restart... | |

| PROGRESS | DESCRIPTION | NOTES |
| --- | --- | --- |
| 88% | Waiting for the destination computer to respond after the 2nd restart... | |
| 91% | Waiting for the destination computer to respond with the new name... | May take a long time due to Active Directory and DNS replication. |
| 93% | Removing alternate computer names on the destination... | Ensures that the destination name has been replaced. |
| 94% | Removing a temporary local account we created on the destination computer... | |
| 97% | Resetting the local account token filter policy on the destination computer... | Enables the policy. |
| (100%) | Succeeded | |

# FAQ

**Is domain controller migration supported?**

Not currently, but see the FAQ page for a workaround.

# Known issues

> Ensure that you have fulfilled the requirements from the Storage Migration Service overview and installed the latest Windows update on the computer running Storage Migration Service.

See the known issues page for more information on the following issues.

- **Storage Migration Service cutover validation fails with error "Access is denied for the token filter policy on destination computer"**
- **Error "CLUSCTL_RESOURCE_NETNAME_REPAIR_VCO failed against netName resource" and Windows Server 2008 R2 cluster cutover fails**
- **Cutover hangs on "38% Mapping network interfaces on the source computer..." when using static IPs**
- **Cutover hangs on "38% Mapping network interfaces on the source computer..."**

# Additional References

- Storage Migration Service overview
- Migrate a file server by using Storage Migration Service
- Storage Migration Services frequently asked questions (FAQ)
- Storage Migration Service known issues

# Storage Migration Service frequently asked questions (FAQ)

11/2/2020 • 11 minutes to read • Edit Online

This topic contains answers to frequently asked questions (FAQs) about using Storage Migration Service to migrate servers.

## What files and folders are excluded from transfers?

Storage Migration Service won't transfer files or folders that we know could interfere with Windows operation. Specifically, here's what we won't transfer or move into the PreExistingData folder on the destination:

- Windows, Program Files, Program Files (x86), Program Data, Users
- $Recycle.bin, Recycler, Recycled, System Volume Information, $UpgDrv$, $SysReset, $Windows.~BT, $Windows.~LS, Windows.old, boot, Recovery, Documents and Settings
- pagefile.sys, hiberfil.sys, swapfile.sys, winpepge.sys, config.sys, bootsect.bak, bootmgr, bootnxt
- Any files or folders on the source server that conflicts with excluded folders on the destination.
  For example, if there's a N:\Windows folder on the source and it gets mapped to the C:\ volume on the destination, it won't get transferred—regardless of what it contains—because it would interfere with the C:\Windows system folder on the destination.

## Are locked files migrated?

The Storage Migration Service doesn't migrate files that applications exclusively lock. The service does automatically retry three times with a sixty second delay between tries, and you can control the number of attempts and the delay. You can also re-run transfers to copy just the files that were previously skipped due to sharing violations.

## Are domain migrations supported?

The Storage Migration Service doesn't allow migrating between Active Directory domains. Migrations between servers will always join the destination server to the same domain. You can use migration credentials from different domains in the Active Directory forest. The Storage Migration Service does support migrating between workgroups.

## Are clusters supported as sources or destinations?

The Storage Migration Service supports migrating from and to clusters after installation of cumulative update KB4513534 or subsequent updates. This includes migrating from a source cluster to a destination cluster as well as migrating from a standalone source server to a destination cluster for device consolidation purposes. You cannot, however, migrate a cluster to a standalone server.

## Do local groups and local users migrate?

The Storage Migration Service supports migrating local users and groups after installation of cumulative update KB4513534 or subsequent updates.

## Is domain controller migration supported?

The Storage Migration Service doesn't currently migrate domain controllers in Windows Server 2019. As a workaround, as long as you have more than one domain controller in the Active Directory domain, demote the domain controller before migrating it, then promote the destination after cut over completes. If you do choose to migrate a domain controller source or destination, you won't be able to cut over. You must never migrate users and groups when migrating from or to a domain controller.

## What attributes are migrated by the Storage Migration Service?

Storage Migration Service migrates all flags, settings, and security of SMB shares. That list of flags that Storage Migration Service migrates includes:

- Share State
- Availability Type
- Share Type
- Folder Enumeration Mode *(aka Access-Based Enumeration or ABE)*
- Caching Mode
- Leasing Mode
- Smb Instance
- CA Timeout
- Concurrent User Limit
- Continuously Available
- Description
- Encrypt Data
- Identity Remoting
- Infrastructure
- Name
- Path
- Scoped
- Scope Name
- Security Descriptor
- Shadow Copy
- Special
- Temporary

## Can I consolidate multiple servers into one server?

The Storage Migration Service version shipped in Windows Server 2019 doesn't support consolidating multiple servers into one server. An example of consolidation would be migrating three separate source servers - which may have the same share names and local file paths - onto a single new server that virtualized those paths and shares to prevent any overlap or collision, then answered all three previous servers names and IP address. You can migrate standalone servers onto multiple file server resources on a single cluster, however.

## Can I migrate from sources other than Windows Server?

The Storage Migration Service supports migrating from Samba Linux servers after installation of cumulative update KB4513534 or subsequent updates. See the requirements for a list of supported Samba versions and Linux distros.

## Can I migrate previous file versions?

The Storage Migration Service version shipped in Windows Server 2019 doesn't support migrating Previous

Versions (made with the volume shadow copy service) of files. Only the current version will migrate.

## Optimizing inventory and transfer performance

The Storage Migration Service contains a multi-threaded read and copy engine called the Storage Migration Service Proxy service which we designed to be both fast as well as bring along perfect data fidelity lacking in many file copy tools. While the default configuration will be optimal for many customers, there are ways to improve SMS performance during inventory and transfer.

- **Use Windows Server 2019 for the destination operating system.** Windows Server 2019 contains the Storage Migration Service Proxy service. When you install this feature and migrate to Windows Server 2019 destinations, all transfers operate as direct line of sight between source and destination. This service runs on the orchestrator during transfer if the destination computers are Windows Server 2012 R2 or Windows Server 2016, which means the transfers double-hop and will be much slower. If there are multiple jobs running with Windows Server 2012 R2 or Windows Server 2016 destinations, the orchestrator will become a bottleneck.
- **Install latest monthly Cumulative Update.** We have improved the Storage Migration Service Proxy service in several updates for better transfer and re-transfer performance, as well as Inventory performance. Install KB4580390 October 2020 Cumulative Update or later to gain significant speed improvements.
- **Alter default transfer threads.** The Storage Migration Service Proxy service copies 8 files simultaneously in a given job. You can increase the number of simultaneous copy threads by adjusting the following registry REG_DWORD value name in decimal on every node running the Storage Migration Service Proxy:

  HKEY_Local_Machine\Software\Microsoft\SMSProxy

  FileTransferThreadCount

  The valid range is 1 to 512 in Windows Server 2019. You don't need to restart the service to start using this setting as long as you create a new job. Use caution with this setting; setting it higher may require additional cores, storage performance, and network bandwidth. Setting it too high may lead to reduced performance compared to default settings.
- **Alter default parallel share threads.** The Storage Migration Service Proxy service copies from 8 shares simultaneously in a given job. You can increase the number of simultaneous share threads by adjusting the following registry REG_DWORD value name in decimal on the Storage Migration Service orchestrator server:

  HKEY_Local_Machine\Software\Microsoft\SMS

  EndpointFileTransferTaskCount

  The valid range is 1 to 512 in Windows Server 2019. You don't need to restart the service to start using this setting as long as you create a new job. Use caution with this setting; setting it higher may require additional cores, storage performance, and network bandwidth. Setting it too high may lead to reduced performance compared to default settings.

  The sum of FileTransferThreadCount and EndpointFileTransferTaskCount is how many files the Storage Migration Service can simultaneously copy from one source node in a job. To add more parallel source nodes, create and run more simultaneous jobs.
- **Add cores and memory.** We strongly recommend that the source, orchestrator, and destination computers have at least two processor cores or two vCPUs, and more can significantly aid inventory and transfer performance, especially when combined with FileTransferThreadCount (above). When transferring

files that are larger than the usual Office formats (gigabytes or greater) transfer performance will benefit from more memory than the default 2GB minimum.

- **Create multiple jobs.** When creating a job with multiple server sources, each server is contacted in serial fashion for inventory, transfer, and cutover. This means that each server must complete its phase before another server starts. To run more servers in parallel, simply create multiple jobs, with each job containing only one server. SMS supports up to 100 simultaneously running jobs, meaning a single orchestrator can parallelize many Windows Server 2019 destination computers. We do not recommend running multiple parallel jobs if your destination computers are Windows Server 2016 or Windows Server 2012 R2 as without the SMS proxy service running on the destination, the orchestrator must perform all transfers itself and could become a bottleneck. The ability for servers to run in parallel inside a single job is a feature we plan to add in a later version of SMS.

- **Use SMB 3 with RDMA networks.** If transferring from a Windows Server 2012 or later source computer, SMB 3.x supports SMB Direct mode and RDMA networking. RDMA moves most CPU cost of transfer from the motherboard CPUs to onboard NIC processors, reducing latency and server CPU utilization. In addition, RDMA networks like ROCE and iWARP typically have substantially higher bandwidth than typical TCP/ethernet, including 25, 50, and 100Gb speeds per interface. Using SMB Direct typically moves the transfer speed limit from the network down to the storage itself.

- **Use SMB 3 multichannel.** If transferring from a Windows Server 2012 or later source computer, SMB 3.x supports multichannel copies that can greatly improve file copy performance. This feature works automatically as long as the source and destination both have:

  - Multiple network adapters
  - One or more network adapters that support Receive Side Scaling (RSS)
  - One of more network adapters that are configured by using NIC Teaming
  - One or more network adapters that support RDMA

- **Update drivers.** As appropriate, install latest vendor storage and enclosure firmware and drivers, latest vendor HBA drivers, latest vendor BIOS/UEFI firmware, latest vendor network drivers, and latest motherboard chipset drivers on source, destination, and orchestrator servers. Restart nodes as needed. Consult your hardware vendor documentation for configuring shared storage and networking hardware.

- **Enable high-performance processing.** Ensure that BIOS/UEFI settings for servers enable high performance, such as disabling C-State, setting QPI speed, enabling NUMA, and setting highest memory frequency. Ensure power management in Windows Server is set to High Performance. Restart as required. Don't forget to return these to appropriate states after completing migration.

- **Tune hardware** Review the Performance Tuning Guidelines for Windows Server 2016 for tuning the orchestrator and destination computers running Windows Server 2019 and Windows Server 2016. The Network Subsystem Performance Tuning section contains especially valuable information.

- **Use faster storage.** While it may be difficult to upgrade the source computer storage speed, you should ensure the destination storage is at least as fast at write IO performance as the source is at read IO performance in order to ensure there is no unnecessary bottleneck in transfers. If the destination is a VM, ensure that, at least for the purposes of migration, it runs in the fastest storage layer of your hypervisor hosts, such as on the flash tier or with Storage Spaces Direct HCI clusters utilizing mirrored all-flash or hybrid spaces. When the SMS migration is complete the VM can be live migrated to a slower tier or host.

- **Update antivirus.** Always ensure your source and destination are running the latest patched version of antivirus software to ensure minimal performance overhead. As a test, you can *temporarily* exclude scanning of folders you're inventorying or migrating on the source and destination servers. If your transfer performance is improved, contact your antivirus software vendor for instructions or for an updated version of the antivirus software or an explanation of expected performance degradation.

## Can I migrate from NTFS to REFS?

The Storage Migration Service version shipped in Windows Server 2019 doesn't support migrating from the NTFS to REFS file systems. You can migrate from NTFS to NTFS and REFS to ReFS. This is by design, due to the many differences in functionality, metadata, and other aspects that ReFS doesn't duplicate from NTFS. ReFS is intended as an application workload file system, not a general file system. For more information, see Resilient File System (ReFS) overview

## Can I move the Storage Migration Service database?

The Storage Migration Service uses an extensible storage engine (ESE) database that is installed by default in the hidden c:\programdata\microsoft\storagemigrationservice folder. This database will grow as jobs are added and transfers are completed, and can consume significant drive space after migrating millions of files if you do not delete jobs. If the database needs to move, perform the following steps:

1. Stop the "Storage Migration Service" service on the orchestrator computer.
2. Take ownership of the `%programdata%/Microsoft/StorageMigrationService` folder
3. Add your user account to have full control over that share and all of its files and subfolders.
4. Move the folder to another drive on the orchestrator computer.
5. Set the following registry REG_SZ value:

   HKEY_Local_Machine\Software\Microsoft\SMS DatabasePath = *path to the new database folder on a different volume*
6. Ensure that SYSTEM has full control to all files and subfolders of that folder
7. Remove your own accounts permissions.
8. Start the "Storage Migration Service" service.

## Does the Storage Migration Service migrate locally installed applications from the source computer?

No, the Storage Migration Service doesn't migrate locally installed applications. After you complete migration, re-install any applications onto the destination computer that were running on the source computer. There's no need to reconfigure any users or their applications; the Storage Migration Service is designed to make the server change invisible to clients.

## What happens with existing files on the destination server?

When performing a transfer, the Storage Migration Service seeks to mirror data from the source server. The destination server should not contain any production data or connected users, as that data could be overwritten. By default, the first transfer makes a backup copy of any data on the destination server as a safeguard. On all subsequent transfers, by default, the Storage Migration Service will mirror data onto the destination; this means not only adding new files, but also arbitrarily overwriting any existing files and deleting any files not present on the source. This behavior is intentional and provides perfect fidelity with the source computer.

## What do the error numbers mean in the transfer CSV?

Most errors found in the transfer CSV file are Windows System Error Codes. You can find out what each error means by reviewing the Win32 error codes documentation.

## What are my options to give feedback, file bugs, or get support?

To give feedback on the Storage Migration Service:

- Use the Feedback Hub tool included in Windows 10, clicking "Suggest a Feature", and specifying the category of "Windows Server" and subcategory of "Storage Migration"
- Use the Windows Server UserVoice site
- Email smsfeed@microsoft.com

To file bugs:

- Use the Feedback Hub tool included in Windows 10, clicking "Report a Problem", and specifying the category of "Windows Server" and subcategory of "Storage Migration"
- Open a support case via Microsoft Support

To get support:

- Post a question on the Windows Server Tech Community
- Post on the Windows Server 2019 forum
- Open a support case via Microsoft Support

## Additional References

- Storage Migration Service overview

# Storage Migration Service known issues

12/16/2020 • 22 minutes to read • Edit Online

This topic contains answers to known issues when using Storage Migration Service to migrate servers.

Storage Migration Service is released in two parts: the service in Windows Server, and the user interface in Windows Admin Center. The service is available in Windows Server, Long-Term Servicing Channel, as well as Windows Server, Semi-Annual Channel; while Windows Admin Center is available as a separate download. We also periodically include changes in cumulative updates for Windows Server, released via Windows Update.

For example, Windows Server, version 1903 includes new features and fixes for Storage Migration Service, which are also available for Windows Server 2019 and Windows Server, version 1809 by installing KB4512534.

## How to collect log files when working with Microsoft Support

The Storage Migration Service contains event logs for the Orchestrator service and the Proxy Service. The orchestrator server always contains both event logs, and destination servers with the proxy service installed contain the proxy logs. These logs are located under:

- Application and Services Logs \ Microsoft \ Windows \ StorageMigrationService
- Application and Services Logs \ Microsoft \ Windows \ StorageMigrationService-Proxy

If you need to gather these logs for offline viewing or to send to Microsoft Support, there's an open-source PowerShell script available on GitHub:

Storage Migration Service Helper

Review the README for usage.

## Storage Migration Service doesn't show up in Windows Admin Center unless managing Windows Server 2019

When using the 1809 version of Windows Admin Center to manage a Windows Server 2019 orchestrator, you don't see the tool option for Storage Migration Service.

The Windows Admin Center Storage Migration Service extension is version-bound to only manage Windows Server 2019 version 1809 or later operating systems. If you use it to manage older Windows Server operating systems or insider previews, the tool will not appear. This behavior is by design.

To resolve, use or upgrade to Windows Server 2019 build 1809 or later.

## Storage Migration Service cutover validation fails with error "Access is denied for the token filter policy on destination computer"

When running cutover validation, you receive error "Fail: Access is denied for the token filter policy on destination computer." This occurs even if you provided correct local administrator credentials for both the source and destination computers.

This issue was fixed in the KB4512534 update.

## Storage Migration Service isn't included in Windows Server 2019

## Evaluation or Windows Server 2019 Essentials edition

When using Windows Admin Center to connect to a Windows Server 2019 Evaluation release or Windows Server 2019 Essentials edition, there isn't an option to manage the Storage Migration Service. Storage Migration Service also isn't included in Roles and Features.

This issue is caused by a servicing issue in the Evaluation media of Windows Server 2019 and Windows Server 2019 Essentials.

To work around this issue for evaluation, install a retail, MSDN, OEM, or Volume License version of Windows Server 2019 and don't activate it. Without activation, all editions of Windows Server operate in evaluation mode for 180 days.

We've fixed this issue in a later release of Windows Server.

## Storage Migration Service times out downloading the transfer error CSV

When using Windows Admin Center or PowerShell to download the transfer operations detailed errors-only CSV log, you receive error:

```
Transfer Log - Please check file sharing is allowed in your firewall. : This request operation sent to
net.tcp://localhost:28940/sms/service/1/transfer did not receive a reply within the configured timeout
(00:01:00). The time allotted to this operation may have been a portion of a longer timeout. This may be
because the service is still processing the operation or because the service was unable to send a reply
message. Please consider increasing the operation timeout (by casting the channel/proxy to IContextChannel and
setting the OperationTimeout property) and ensure that the service is able to connect to the client.
```

This issue is caused by an extremely large number of transferred files that can't be filtered in the default one minute timeout allowed by Storage Migration Service.

To work around this issue:

1. On the orchestrator computer, edit the *%SYSTEMROOT%\SMS\Microsoft.StorageMigration.Service.exe.config* file using Notepad.exe to change the "sendTimeout" from its 1 minute default to 10 minutes

   ```
   <bindings>
     <netTcpBinding>
       <binding name="NetTcpBindingSms"
                sendTimeout="00:10:00"
   ```

2. Restart the "Storage Migration Service" service on the orchestrator computer.
3. On the orchestrator computer, start Regedit.exe
4. Create the following registry subkey if it doesn't already exist:

   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\SMSPowershell
   ```

5. On the Edit menu, point to New, and then click DWORD Value.
6. Type "WcfOperationTimeoutInMinutes" for the name of the DWORD, and then press ENTER.
7. Right-click "WcfOperationTimeoutInMinutes", and then click Modify.
8. In the Base data box, click "Decimal"
9. In the Value data box, type "10", and then click OK.

10. Exit Registry Editor.
11. Attempt to download the errors-only CSV file again.

You may need to increase this timeout to more than 10 minutes if you are migrating an extremely large number of files.

## Validation warnings for destination proxy and credential administrative privileges

When validating a transfer job, you see the following warnings:

```
The credential has administrative privileges.
Warning: Action isn't available remotely.
The destination proxy is registered.
Warning: The destination proxy wasn't found.
```

If you have not installed the Storage Migration Service Proxy service on the Windows Server 2019 destination computer, or the destination computer is Windows Server 2016 or Windows Server 2012 R2, this behavior is by design. We recommend migrating to a Windows Server 2019 computer with the proxy installed for significantly improved transfer performance.

## Certain files don't inventory or transfer, error 5 "Access is denied"

When inventorying or transferring files from source to destination computers, files from which a user has removed permissions for the Administrators group fail to migrate. Examining the Storage Migration Service-Proxy debug shows:

```
Log Name: Microsoft-Windows-StorageMigrationService-Proxy/Debug
Source: Microsoft-Windows-StorageMigrationService-Proxy
Date: 2/26/2019 9:00:04 AM
Event ID: 10000
Task Category: None
Level: Error
Keywords:
User: NETWORK SERVICE
Computer: srv1.contoso.com
Description:

02/26/2019-09:00:04.860 [Error] Transfer error for \\srv1.contoso.com\public\indy.png: (5) Access is denied.
Stack Trace:
at Microsoft.StorageMigration.Proxy.Service.Transfer.FileDirUtils.OpenFile(String fileName, DesiredAccess
desiredAccess, ShareMode shareMode, CreationDisposition creationDisposition, FlagsAndAttributes
flagsAndAttributes)
at Microsoft.StorageMigration.Proxy.Service.Transfer.FileDirUtils.GetTargetFile(String path)
at Microsoft.StorageMigration.Proxy.Service.Transfer.FileDirUtils.GetTargetFile(FileInfo file)
at Microsoft.StorageMigration.Proxy.Service.Transfer.FileTransfer.InitializeSourceFileInfo()
     at Microsoft.StorageMigration.Proxy.Service.Transfer.FileTransfer.Transfer()
at Microsoft.StorageMigration.Proxy.Service.Transfer.FileTransfer.TryTransfer()
```

This issue is caused by a code defect in the Storage Migration Service where the backup privilege was not being invoked.

To resolve this issue, install Windows Update April 2, 2019—KB4490481 (OS Build 17763.404) on the orchestrator computer and the destination computer if the proxy service is installed there. Ensure that the source migration user account is a local administrator on the source computer and the Storage Migration Service orchestrator. Ensure that the destination migration user account is a local administrator on the destination computer and the Storage Migration Service orchestrator.

# DFSR hashes mismatch when using Storage Migration Service to preseed data

When using the Storage Migration Service to transfer files to a new destination, then configuring DFS Replication to replicate that data with an existing server through preseeded replication or DFS Replication database cloning, all files experience a hash mismatch and are re-replicated. The data streams, security streams, sizes, and attributes all appear to be perfectly matched after using Storage Migration Service to transfer them. Examining the files with ICACLS or the DFS Replication database cloning debug log reveals:

**Source file**

```
icacls d:\test\Source:

icacls d:\test\thatcher.png /save out.txt /t thatcher.png
D:AI(A;;FA;;;BA)(A;;0x1200a9;;;DD)(A;;0x1301bf;;;DU)(A;ID;FA;;;BA)(A;ID;FA;;;SY)(A;ID;0x1200a9;;;BU)
```

**Destination file**

```
icacls d:\test\thatcher.png /save out.txt /t thatcher.png
D:AI(A;;FA;;;BA)(A;;0x1301bf;;;DU)(A;;0x1200a9;;;DD)(A;ID;FA;;;BA)(A;ID;FA;;;SY)
(A;ID;0x1200a9;;;BU)**S:PAINO_ACCESS_CONTROL**
```

**DFSR Debug Log**

```
20190308 10:18:53.116 3948 DBCL  4045 [WARN] DBClone::IDTableImportUpdate Mismatch record was found.

Local ACL hash:1BCDFE03-A18BCE01-D1AE9859-23A0A5F6
LastWriteTime:20190308 18:09:44.876
FileSizeLow:1131654
FileSizeHigh:0
Attributes:32

Clone ACL hash:**DDC4FCE4-DDF329C4-977CED6D-F4D72A5B**
LastWriteTime:20190308 18:09:44.876
FileSizeLow:1131654
FileSizeHigh:0
Attributes:32
```

This issue is fixed by the KB4512534 update.

# Error "Couldn't transfer storage on any of the endpoints" when transferring from Windows Server 2008 R2

When attempting to transfer data from a Windows Server 2008 R2 source computer, no data transfers and you receive error:

```
Couldn't transfer storage on any of the endpoints.
0x9044
```

This error is expected if your Windows Server 2008 R2 computer isn't fully patched with all Critical and Important updates from Windows Update. It's especially important to keep a Windows Server 2008 R2 computer updated for security purposes, as that operating system doesn't contain the security improvements of newer versions of Windows Server.

# Error "Couldn't transfer storage on any of the endpoints" and "Check if

## the source device is online - we couldn't access it."

When attempting to transfer data from a source computer, some or all shares don't transfer, with the error:

```
Couldn't transfer storage on any of the endpoints.
0x9044
```

Examining the SMB transfer details shows error:

```
Check if the source device is online - we couldn't access it.
```

Examining the StorageMigrationService/Admin event log shows:

```
Couldn't transfer storage.

Job: Job1
ID:
State: Failed
Error: 36931
Error Message:

Guidance: Check the detailed error and make sure the transfer requirements are met. The transfer job couldn't
transfer any source and destination computers. This could be because the orchestrator computer couldn't reach
any source or destination computers, possibly due to a firewall rule, or missing permissions.
```

Examining the StorageMigrationService-Proxy/Debug log shows:

```
07/02/2019-13:35:57.231 [Error] Transfer validation failed. ErrorCode: 40961, Source endpoint is not
reachable, or doesn't exist, or source credentials are invalid, or authenticated user doesn't have sufficient
permissions to access it.
at Microsoft.StorageMigration.Proxy.Service.Transfer.TransferOperation.Validate()
at Microsoft.StorageMigration.Proxy.Service.Transfer.TransferRequestHandler.ProcessRequest(FileTransferRequest
fileTransferRequest, Guid operationId)
```

This was a code defect that would manifest if your migration account does not have at least Read permissions to the SMB shares. This issue was first fixed in cumulative update 4520062.

## Error 0x80005000 when running inventory

After installing KB4512534 and attempting to run inventory, inventory fails with errors:

```
EXCEPTION FROM HRESULT: 0x80005000

Log Name:      Microsoft-Windows-StorageMigrationService/Admin
Source:        Microsoft-Windows-StorageMigrationService
Date:          9/9/2019 5:21:42 PM
Event ID:      2503
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      FS02.TailwindTraders.net
Description:
Couldn't inventory the computers.
Job: foo2
ID: 20ac3f75-4945-41d1-9a79-d11dbb57798b
State: Failed
Error: 36934
Error Message: Inventory failed for all devices
Guidance: Check the detailed error and make sure the inventory requirements are met. The job couldn't
inventory any of the specified source computers. This could be because the orchestrator computer couldn't
reach it over the network, possibly due to a firewall rule or missing permissions.

Log Name:      Microsoft-Windows-StorageMigrationService/Admin
Source:        Microsoft-Windows-StorageMigrationService
Date:          9/9/2019 5:21:42 PM
Event ID:      2509
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      FS02.TailwindTraders.net
Description:
Couldn't inventory a computer.
Job: foo2
Computer: FS01.TailwindTraders.net
State: Failed
Error: -2147463168
Error Message:
Guidance: Check the detailed error and make sure the inventory requirements are met. The inventory couldn't
determine any aspects of the specified source computer. This could be because of missing permissions or
privileges on the source or a blocked firewall port.

Log Name:      Microsoft-Windows-StorageMigrationService-Proxy/Debug
Source:        Microsoft-Windows-StorageMigrationService-Proxy
Date:          2/14/2020 1:18:21 PM
Event ID:      10000
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      2019-rtm-orc.ned.contoso.com
Description:
02/14/2020-13:18:21.097 [Erro] Failed device discovery stage SystemInfo with error: (0x80005000) Unknown error
(0x80005000)
```

This error is caused by a code defect in Storage Migration Service when you provide migration credentials in the form of a User Principal Name (UPN), such as 'meghan@contoso.com'. The Storage Migration Service orchestrator service fails to parse this format correctly, which leads to a failure in a domain lookup that was added for cluster migration support in KB4512534 and 19H1.

To work around this issue, provide credentials in the domain\user format, such as 'Contoso\Meghan'.

## Error "ServiceError0x9006" or "The proxy isn't currently available." when

## migrating to a Windows Server failover cluster

When attempting to transfer data against a clustered File Server, you receive errors such as:

```
Make sure the proxy service is installed and running, and then try again. The proxy isn't currently available.
0x9006
ServiceError0x9006,Microsoft.StorageMigration.Commands.UnregisterSmsProxyCommand
```

This error is expected if the File Server resource moved from its original Windows Server 2019 cluster owner node to a new node and the Storage Migration Service Proxy feature wasn't installed on that node.

As a workaround, move the destination File Server resource back to the original owner cluster node that was in use when you first configured transfer pairings.

As an alternative workaround:

1. Install the Storage Migration Service Proxy feature on all nodes in a cluster.
2. Run the following Storage Migration Service PowerShell command on the orchestrator computer:

   ```
   Register-SMSProxy -ComputerName <destination server> -Force
   ```

## Error "Dll was not found" when running inventory from a cluster node

When attempting to run inventory with the Storage Migration Service and targeting a Windows Server failover cluster general use file server source, you receive the following errors:

```
DLL not found
[Error] Failed device discovery stage VolumeInfo with error: (0x80131524) Unable to load DLL
'Microsoft.FailoverClusters.FrameworkSupport.dll': The specified module could not be found. (Exception from
HRESULT: 0x8007007E)
```

To work around this issue, install the "Failover Cluster Management Tools" (RSAT-Clustering-Mgmt) on the server running the Storage Migration Service orchestrator.

## Error "There are no more endpoints available from the endpoint mapper" when running inventory against a Windows Server 2003 source computer

When attempting to run inventory with the Storage Migration Service orchestrator against a Windows Server 2003 source computer, you receive the following error:

```
There are no more endpoints available from the endpoint mapper
```

This issue is resolved by the KB4537818 update.

## Uninstalling a cumulative update prevents Storage Migration Service from starting

Uninstalling Windows Server cumulative updates may prevent the Storage Migration Service from starting. To resolve this issue, you can back up and delete the Storage Migration Service database:

1. Open an elevated cmd prompt, where you are a member of Administrators on the Storage Migration

Service orchestrator server, and run:

```
TAKEOWN /d y /a /r /f c:\ProgramData\Microsoft\StorageMigrationService

MD c:\ProgramData\Microsoft\StorageMigrationService\backup

ICACLS c:\ProgramData\Microsoft\StorageMigrationService\* /grant Administrators:(GA)

XCOPY c:\ProgramData\Microsoft\StorageMigrationService\* .\backup\*

DEL c:\ProgramData\Microsoft\StorageMigrationService\* /q

ICACLS c:\ProgramData\Microsoft\StorageMigrationService  /GRANT networkservice:F /T /C

ICACLS c:\ProgramData\Microsoft\StorageMigrationService /GRANT networkservice:(GA) /T /C
```

2. Start the Storage Migration Service service, which will create a new database.

## Error "CLUSCTL_RESOURCE_NETNAME_REPAIR_VCO failed against netName resource" and Windows Server 2008 R2 cluster cutover fails

When attempting to run cut over of a Windows Server 2008 R2 cluster source, the cut over gets stuck at phase "Renaming the source computer..." and you receive the following error:

```
Log Name:      Microsoft-Windows-StorageMigrationService-Proxy/Debug
Source:        Microsoft-Windows-StorageMigrationService-Proxy
Date:          10/17/2019 6:44:48 PM
Event ID:      10000
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      WIN-RNS0D0PMPJH.contoso.com
Description:
10/17/2019-18:44:48.727 [Erro] Exception error: 0x1. Message: Control code CLUSCTL_RESOURCE_NETNAME_REPAIR_VCO
failed against netName resource 2008r2FS., stackTrace:    at
Microsoft.FailoverClusters.Framework.ClusterUtils.NetnameRepairVCO(SafeClusterResourceHandle
netNameResourceHandle, String netName)
at Microsoft.FailoverClusters.Framework.ClusterUtils.RenameFSNetName(SafeClusterHandle ClusterHandle, String
clusterName, String FsResourceId, String NetNameResourceId, String newDnsName, CancellationToken ct)
at Microsoft.StorageMigration.Proxy.Cutover.CutoverUtils.RenameFSNetName(NetworkCredential networkCredential,
Boolean isLocal, String clusterName, String fsResourceId, String nnResourceId, String newDnsName,
CancellationToken ct)
[d:\os\src\base\dms\proxy\cutover\cutoverproxy\CutoverUtils.cs::RenameFSNetName::1510]
```

This issue is caused by a missing API in older versions of Windows Server. Currently there's no way to migrate Windows Server 2008 and Windows Server 2003 clusters. You can perform inventory and transfer without issue on Windows Server 2008 R2 clusters, then manually perform cutover by manually changing the cluster's source file server resource netname and IP address, then changing the destination cluster netname and IP address to match the original source.

## Cutover hangs on "38% Mapping network interfaces on the source computer..." when using static IPs

When attempting to run cut over of a source computer, having set the source computer to use a new static (not DHCP) IP address on one or more network interfaces, the cut over gets stuck at phase "38% Mapping network interfaces on the source computer..." and you receive the following error in the Storage Migration Service event log:

```
Log Name:      Microsoft-Windows-StorageMigrationService-Proxy/Admin
Source:        Microsoft-Windows-StorageMigrationService-Proxy
Date:          11/13/2019 3:47:06 PM
Event ID:      20494
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      orc2019-rtm.corp.contoso.com
Description:
Couldn't set the IP address on the network adapter.

Computer: fs12.corp.contoso.com
Adapter: microsoft hyper-v network adapter
IP address: 10.0.0.99
Network mask: 16
Error: 40970
Error Message: Unknown error (0xa00a)

Guidance: Confirm that the Netlogon service on the computer is reachable through RPC and that the credentials
provided are correct.
```

Examining the source computer shows that the original IP address fails to change.

This issue does not happen if you selected "Use DHCP" on the Windows Admin Center "configure cutover" screen, only if you specify a new static IP address.

There are two solutions for this issue:

1. This issue was first resolved by the KB4537818 update. That earlier code defect prevented all use of static IP addresses.
2. If you have not specified a default gateway IP address on the source computer's network interfaces, this issue will occur even with the KB4537818 update. To work around this issue, set a valid default IP address on the network interfaces using the Network Connections applet (NCPA.CPL) or Set-NetRoute Powershell cmdlet.

## Slower than expected re-transfer performance

After completing a transfer, then running a subsequent re-transfer of the same data, you may not see much improvement in transfer time even when little data has changed in the meantime on the source server.

This issue is resolved by kb4580390. To tune performance further, review Optimizing Inventory and Transfer Performance.

## Slower than expected inventory performance

While inventorying a source server, you find the file inventory taking a very long time when there are many files or nested folders. Millions of files and folders may lead to inventories taking many hours even on fast storage configurations.

This issue is resolved by kb4580390.

## Data does not transfer, user renamed when migrating to or from a domain controller

After starting the transfer from or to a domain controller:

1. No data is migrated and no shares are created on the destination.

2. There's a red error symbol shown in Windows Admin Center with no error message
3. One or more AD users and Domain Local groups have their name and/or pre-Windows 2000 logon attribute changed
4. You see event 3509 on the Storage Migration Service orchestrator:

   ```
   Log Name:      Microsoft-Windows-StorageMigrationService/Admin
   Source:        Microsoft-Windows-StorageMigrationService
   Date:          1/10/2020 2:53:48 PM
   Event ID:      3509
   Task Category: None
   Level:         Error
   Keywords:
   User:          NETWORK SERVICE
   Computer:      orc2019-rtm.corp.contoso.com
   Description:
   Couldn't transfer storage for a computer.

   Job: dctest3
   Computer: dc02-2019.corp.contoso.com
   Destination Computer: dc03-2019.corp.contoso.com
   State: Failed
   Error: 53251
   Error Message: Local accounts migration failed with error System.Exception: -2147467259
       at Microsoft.StorageMigration.Service.DeviceHelper.MigrateSecurity(IDeviceRecord
   sourceDeviceRecord, IDeviceRecord destinationDeviceRecord, TransferConfiguration config, Guid proxyId,
   CancellationToken cancelToken)
   ```

   This is expected behavior if you attempted to migrate from or to a domain controller with Storage Migration Service and used the "migrate users and groups" option to rename or reuse accounts. instead of selecting "Don't transfer users and groups". DC migration is not supported with Storage Migration Service. Because a DC doesn't have true local users and groups, Storage Migration Service treats these security principals as it would when migrating between two member servers and attempts to adjust ACLs as instructed, leading to the errors and mangled or copied accounts.

If you have already run transfer one ore more times:

1. Use the following AD PowerShell command against a DC to locate any modified users or groups (changing SearchBase to match your domain distinguished name):

   ```
   Get-ADObject -Filter 'Description -like "*storage migration service renamed*"' -SearchBase 'DC=
   <domain>,DC=<TLD>' | ft name,distinguishedname
   ```

2. For any users returned with their original name, edit their "User Logon Name (pre-Windows 2000)" to remove the random character suffix added by Storage Migration Service, so that this user can log on.
3. For any groups returned with their original name, edit their "Group Name (pre-Windows 2000)" to remove the random character suffix added by Storage Migration Service.
4. For any disabled users or groups with names that now contain a suffix added by Storage Migration Service, you can delete these accounts. You can confirm that user accounts were added later because they will only contain the Domain Users group and will have a created date/time matching the Storage Migration Service transfer start time.

   If you wish to use Storage Migration Service with domain controllers for transfer purposes, ensure you always select "Don't transfer users and groups" on the transfer settings page in Windows Admin Center.

## Error 53, "failed to inventory all specified devices" when running

## inventory,

When attempting to run inventory, you receive:

```
Failed to inventory all specified devices

Log Name:      Microsoft-Windows-StorageMigrationService/Admin
Source:        Microsoft-Windows-StorageMigrationService
Date:          1/16/2020 8:31:17 AM
Event ID:      2516
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      ned.corp.contoso.com
Description:
Couldn't inventory files on the specified endpoint.
Job: ned1
Computer: ned.corp.contoso.com
Endpoint: hithere
State: Failed
File Count: 0
File Size in KB: 0
Error: 53
Error Message: Endpoint scan failed
Guidance: Check the detailed error and make sure the inventory requirements are met. This could be because of
missing permissions on the source computer.

Log Name:      Microsoft-Windows-StorageMigrationService-Proxy/Debug
Source:        Microsoft-Windows-StorageMigrationService-Proxy
Date:          1/16/2020 8:31:17 AM
Event ID:      10004
Task Category: None
Level:         Critical
Keywords:
User:          NETWORK SERVICE
Computer:      ned.corp.contoso.com
Description:
01/16/2020-08:31:17.031 [Crit] Consumer Task failed with error:The network path was not found.
. StackTrace=   at Microsoft.Win32.RegistryKey.Win32ErrorStatic(Int32 errorCode, String str)
    at Microsoft.Win32.RegistryKey.OpenRemoteBaseKey(RegistryHive hKey, String machineName, RegistryView view)
    at Microsoft.StorageMigration.Proxy.Service.Transfer.FileDirUtils.GetEnvironmentPathFolders(String
ServerName, Boolean IsServerLocal)
    at Microsoft.StorageMigration.Proxy.Service.Discovery.ScanUtils.<ScanSMBEndpoint>d__3.MoveNext()
    at Microsoft.StorageMigration.Proxy.EndpointScanOperation.Run()
    at
Microsoft.StorageMigration.Proxy.Service.Discovery.EndpointScanRequestHandler.ProcessRequest(EndpointScanReque
st scanRequest, Guid operationId)
    at Microsoft.StorageMigration.Proxy.Service.Discovery.EndpointScanRequestHandler.ProcessRequest(Object
request)
    at Microsoft.StorageMigration.Proxy.Common.ProducerConsumerManager`3.Consume(CancellationToken token)

01/16/2020-08:31:10.015 [Erro] Endpoint Scan failed. Error: (53) The network path was not found.
Stack trace:
    at Microsoft.Win32.RegistryKey.Win32ErrorStatic(Int32 errorCode, String str)
    at Microsoft.Win32.RegistryKey.OpenRemoteBaseKey(RegistryHive hKey, String machineName, RegistryView view)
```

At this stage, Storage Migration Service orchestrator is attempting remote registry reads to determine source machine configuration, but is being rejected by the source server saying the registry path does not exist. This can be caused by:

- The Remote Registry service isn't running on the source computer.
- firewall does not allow remote registry connections to the source server from the Orchestrator.
- The source migration account does not have remote registry permissions to connect to the source computer.

- The source migration account does not have read permissions within the registry of the source computer, under "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" or under "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer"

## Cutover hangs on "38% Mapping network interfaces on the source computer..."

When attempting to run cut over of a source computer, the cut over gets stuck at phase "38% Mapping network interfaces on the source computer..." and you receive the following error in the Storage Migration Service event log:

```
Log Name:      Microsoft-Windows-StorageMigrationService-Proxy/Admin
Source:        Microsoft-Windows-StorageMigrationService-Proxy
Date:          1/11/2020 8:51:14 AM
Event ID:      20505
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      nedwardo.contosocom
Description:
Couldn't establish a CIM session with the computer.

Computer: 172.16.10.37
User Name: nedwardo\MsftSmsStorMigratSvc
Error: 40970
Error Message: Unknown error (0xa00a)

Guidance: Confirm that the Netlogon service on the computer is reachable through RPC and that the credentials
provided are correct.
```

This issue is caused by Group Policy that sets the following registry value on the source computer: "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy = 0"

This setting isn't part of standard Group Policy, it's an add-on configured using the Microsoft Security Compliance Toolkit:

- Windows Server 2012 R2: "Computer Configuration\Administrative Templates\SCM: Pass the Hash Mitigations\Apply UAC restrictions to local accounts on network logons"
- Widows Server 2016: "Computer Configuration\Administrative Templates\MS Security Guide\Apply UAC restrictions to local accounts on network logons"

It can also be set using Group Policy Preferences with a custom registry setting. You can use the GPRESULT tool to determine which policy is applying this setting to the source computer.

The Storage Migration Service temporarily enables the LocalAccountTokenFilterPolicy as part of the cut over process, then removes it when done. When Group Policy applies a conflicting Group Policy Object (GPO), it overrides the Storage Migration Service and prevents cut over.

To work around this issue, use one of the following options:

1. Temporarily move the source computer from the Active Directory OU that applies this conflicting GPO.
2. Temporarily disable the GPO that applies this conflicting policy.
3. Temporarily create a new GPO that sets this setting to Disabled and applies to specific OU of source servers, with a higher precedence than any other GPOs.

# Inventory or transfer fail when using credentials from a different domain

When attempting to run inventory or transfer with the Storage Migration Service and targeting a Windows Server while using migration credentials from a different domain than the targeted server, you receive the following errors

```
Exception from HRESULT:0x80131505

The server was unable to process the request due to an internal error

04/28/2020-11:31:01.169 [Error] Failed device discovery stage SystemInfo with error: (0x490) Could not find
computer object 'myserver' in Active Directory
[d:\os\src\base\dms\proxy\discovery\discoveryproxy\DeviceDiscoveryOperation.cs::TryStage::1042]
```

Examining the logs further shows that the migration account and the server being migrated from or two are in different domains:

```
06/25/2020-10:11:16.543 [Info] Creating new job=NedJob user=**CONTOSO**\ned
[d:\os\src\base\dms\service\StorageMigrationService.IInventory.cs::CreateJob::133]
```

```
GetOsVersion(fileserver75.**corp**.contoso.com)
[d:\os\src\base\dms\proxy\common\proxycommon\CimSessionHelper.cs::GetOsVersion::66] 06/25/2020-10:20:45.368
[Info] Computer 'fileserver75.corp.contoso.com': OS version
```

This issue is caused by a code defect in the Storage Migration Service. To work around this issue, use migration credentials from the same domain that the source and destination computer belong to. For instance, if the source and destination computer belong to the "corp.contoso.com" domain in the "contoso.com" forest, use 'corp\myaccount' to perform the migration, not a 'contoso\myaccount' credential.

# Inventory fails with "Element not found"

Consider the following scenario:

You have a source server with a DNS Host Name and Active Directory name more than 15 unicode characters, such as "iamaverylongcomputername". By design, Windows did not let you set the legacy NetBIOS name to be set this long and warned when the server was named that the NetBIOS name would be truncated to 15 unicode wide characters (example: "iamaverylongcom"). When you attempt to inventory this computer, you receive in Windows Admin Center and the event log:

```
"Element not found"
========================

Log Name:      Microsoft-Windows-StorageMigrationService/Admin
Source:        Microsoft-Windows-StorageMigrationService
Date:          4/10/2020 10:49:19 AM
Event ID:      2509
Task Category: None
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      WIN-6PJAG3DHPLF.corp.contoso.com
Description:
Couldn't inventory a computer.

Job: longnametest
Computer: iamaverylongcomputername.corp.contoso.com
State: Failed
Error: 1168
Error Message:

Guidance: Check the detailed error and make sure the inventory requirements are met. The inventory couldn't
determine any aspects of the specified source computer. This could be because of missing permissions or
privileges on the source or a blocked firewall port.
```

This issue is caused by a code defect in the Storage Migration Service. The only workaround currently is to rename the computer to have the same name as the NetBIOS name, then use NETDOM COMPUTERNAME /ADD to add an alternate computer name that contains the longer name that was in use prior to starting Inventory. Storage Migration Service supports migrating alternate computer names.

## Storage Migration Service inventory fails with "a parameter cannot be found that matches parameter name 'IncludeDFSN'"

When using the 2009 version of Windows Admin Center to manage a Windows Server 2019 orchestrator, you receive the following error when you attempt to inventory a source computer:

```
Remote exception : a parameter cannot be found that matches parameter name 'IncludeDFSN'"
```

To resolve, update the Storage Migration Service extension to at least version 1.113.0 in Windows Admin Center. The update should automatically appear in the feed and prompt for installation.

## Storage Migration Service transfer validation returns 'Error HRESULT E_FAIL has been returned from a call to a COM component'

After installing the Windows Server 2019 November cumulative update KB4586793, some transfer validations may fail with:

```
Error HRESULT E_FAIL has been returned from a call to a COM component
```

It doesn't necessarily happen for all source computers. We are working to diagnose this issue. As a workaround, install the 1.115 or later Storage Migration Service tool in Windows Admin Center. The update should automatically appear in the Windows Admin Center feed and prompt for installation, and will allow you to ignore this error. To work around it:

1. Navigate to the "Adjust Settings" step of the Transfer phase.
2. Enable "Override Transfer Validation".

3. Proceed with your transfer, either without running "Validate" or running it and ignoring the E_FAIL error.

> **IMPORTANT**
>
> Don't uninstall KB4586793. This update upgrades the Storage Migration Service database and removing the update will require you to delete your database.

## See also

- Storage Migration Service overview

# Storage Replica overview

12/16/2020 • 12 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

Storage Replica is Windows Server technology that enables replication of volumes between servers or clusters for disaster recovery. It also enables you to create stretch failover clusters that span two sites, with all nodes staying in sync.

Storage Replica supports synchronous and asynchronous replication:

- **Synchronous replication** mirrors data within a low-latency network site with crash-consistent volumes to ensure zero data loss at the file-system level during a failure.
- **Asynchronous replication** mirrors data across sites beyond metropolitan ranges over network links with higher latencies, but without a guarantee that both sites have identical copies of the data at the time of a failure.

## Why use Storage Replica?

Storage Replica offers disaster recovery and preparedness capabilities in Windows Server. Windows Server offers the peace of mind of zero data loss, with the ability to synchronously protect data on different racks, floors, buildings, campuses, counties, and cities. After a disaster strikes, all data exists elsewhere without any possibility of loss. The same applies *before* a disaster strikes; Storage Replica offers you the ability to switch workloads to safe locations prior to catastrophes when granted a few moments warning - again, with no data loss.

Storage Replica allows more efficient use of multiple datacenters. By stretching clusters or replicating clusters, workloads can be run in multiple datacenters for quicker data access by local proximity users and applications, as well as better load distribution and use of compute resources. If a disaster takes one datacenter offline, you can move its typical workloads to the other site temporarily.

Storage Replica may allow you to decommission existing file replication systems such as DFS Replication that were pressed into duty as low-end disaster recovery solutions. While DFS Replication works well over extremely low bandwidth networks, its latency is very high - often measured in hours or days. This is caused by its requirement for files to close and its artificial throttles meant to prevent network congestion. With those design characteristics, the newest and hottest files in a DFS Replication replica are the least likely to replicate. Storage Replica operates below the file level and has none of these restrictions.

Storage Replica also supports asynchronous replication for longer ranges and higher latency networks. Because it is not checkpoint-based, and instead continuously replicates, the delta of changes tends to be far lower than snapshot-based products. Furthermore, Storage Replica operates at the partition layer and therefore replicates all VSS snapshots created by Windows Server or backup software; this allows use of application-consistent data snapshots for point in time recovery, especially unstructured user data replicated asynchronously.

## Supported configurations

You can deploy Storage Replica in a stretch cluster, between cluster-to-cluster, and in server-to-server configurations (see Figures 1-3).

**Stretch Cluster** allows configuration of computers and storage in a single cluster, where some nodes share one set of asymmetric storage and some nodes share another, then synchronously or asynchronously replicate with site awareness. This scenario can utilize Storage Spaces with shared SAS storage, SAN and iSCSI-attached LUNs.

It is managed with PowerShell and the Failover Cluster Manager graphical tool, and allows for automated workload failover.

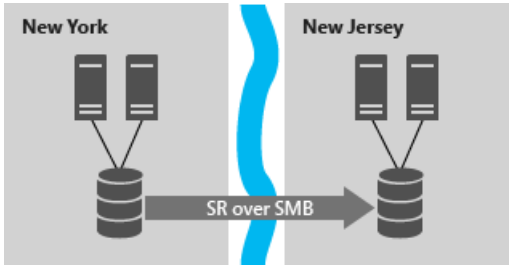



FIGURE 1: Storage replication in a stretch cluster using Storage Replica

**Cluster to Cluster** allows replication between two separate clusters, where one cluster synchronously or asynchronously replicates with another cluster. This scenario can utilize Storage Spaces Direct, Storage Spaces with shared SAS storage, SAN and iSCSI-attached LUNs. It is managed with Windows Admin Center and PowerShell, and requires manual intervention for failover.

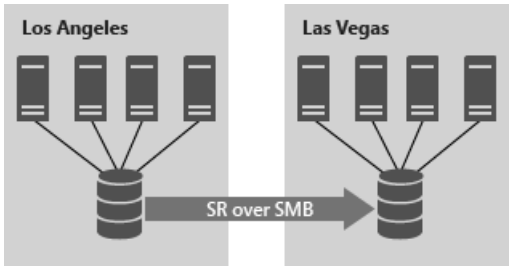



FIGURE 2: Cluster-to-cluster storage replication using Storage Replica

**Server to server** allows synchronous and asynchronous replication between two standalone servers, using Storage Spaces with shared SAS storage, SAN and iSCSI-attached LUNs, and local drives. It is managed with Windows Admin Center and PowerShell, and requires manual intervention for failover.

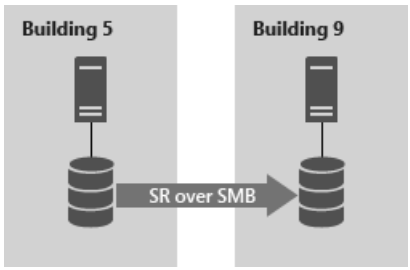



FIGURE 3: Server-to-server storage replication using Storage Replica

> **NOTE**
>
> You can also configure server-to-self replication, using four separate volumes on one computer. However, this guide does not cover this scenario.

## Storage Replica Features

- **Zero data loss, block-level replication**. With synchronous replication, there is no possibility of data loss. With block-level replication, there is no possibility of file locking.
- **Simple deployment and management**. Storage Replica has a design mandate for ease of use. Creation of a replication partnership between two servers can utilize the Windows Admin Center. Deployment of stretch clusters uses intuitive wizard in the familiar Failover Cluster Manager tool.
- **Guest and host**. All capabilities of Storage Replica are exposed in both virtualized guest and host-based

deployments. This means guests can replicate their data volumes even if running on non-Windows virtualization platforms or in public clouds, as long as using Windows Server in the guest.

- **SMB3-based**. Storage Replica uses the proven and mature technology of SMB 3, first released in Windows Server 2012. This means all of SMB's advanced characteristics - such as multichannel and SMB direct support on RoCE, iWARP, and InfiniBand RDMA network cards - are available to Storage Replica.
- **Security**. Unlike many vendor's products, Storage Replica has industry-leading security technology baked in. This includes packet signing, AES-128-GCM full data encryption, support for Intel AES-NI encryption acceleration, and pre-authentication integrity man-in-the-middle attack prevention. Storage Replica utilizes Kerberos AES256 for all authentication between nodes.
- **High performance initial sync**. Storage Replica supports seeded initial sync, where a subset of data already exists on a target from older copies, backups, or shipped drives. Initial replication only copies the differing blocks, potentially shortening initial sync time and preventing data from using up limited bandwidth. Storage replicas block checksum calculation and aggregation means that initial sync performance is limited only by the speed of the storage and network.
- **Consistency groups**. Write ordering guarantees that applications such as Microsoft SQL Server can write to multiple replicated volumes and know the data is written on the destination server sequentially.
- **User delegation**. Users can be delegated permissions to manage replication without being a member of the built-in Administrators group on the replicated nodes, therefore limiting their access to unrelated areas.
- **Network Constraint**. Storage Replica can be limited to individual networks by server and by replicated volumes, in order to provide application, backup, and management software bandwidth.
- **Thin provisioning**. Support for thin provisioning in Storage Spaces and SAN devices is supported, in order to provide near-instantaneous initial replication times under many circumstances.

Storage Replica includes the following features:

| FEATURE | DETAILS |
| --- | --- |
| Type | Host-based |
| Synchronous | Yes |
| Asynchronous | Yes |
| Storage hardware agnostic | Yes |
| Replication unit | Volume (Partition) |
| Windows Server stretch cluster creation | Yes |
| Server to server replication | Yes |
| Cluster to cluster replication | Yes |
| Transport | SMB3 |
| Network | TCP/IP or RDMA |

| FEATURE | DETAILS |
| --- | --- |
| Network constraint support | Yes |
| RDMA* | iWARP, InfiniBand, RoCE v2 |
| Replication network port firewall requirements | Single IANA port (TCP 445 or 5445) |
| Multipath/Multichannel | Yes (SMB3) |
| Kerberos support | Yes (SMB3) |
| Over the wire encryption and signing | Yes (SMB3) |
| Per-volume failovers allowed | Yes |
| Thin-provisioned storage support | Yes |
| Management UI in-box | PowerShell, Failover Cluster Manager |

*May require additional long haul equipment and cabling.

## Storage Replica prerequisites

- Active Directory Domain Services forest.
- Storage Spaces with SAS JBODs, Storage Spaces Direct, fibre channel SAN, shared VHDX, iSCSI Target, or local SAS/SCSI/SATA storage. SSD or faster recommended for replication log drives. Microsoft recommends that the log storage be faster than the data storage. Log volumes must never be used for other workloads.
- At least one ethernet/TCP connection on each server for synchronous replication, but preferably RDMA.
- At least 2GB of RAM and two cores per server.
- A network between servers with enough bandwidth to contain your IO write workload and an average of 5ms round trip latency or lower, for synchronous replication. Asynchronous replication does not have a latency recommendation.
- Windows Server, Datacenter Edition, or Windows Server, Standard Edition. Storage Replica running on Windows Server, Standard Edition, has the following limitations:
    - You must use Windows Server 2019 or later
    - Storage Replica replicates a single volume instead of an unlimited number of volumes.
    - Volumes can have a size of up to 2 TB instead of an unlimited size.

## Background

This section includes information about high-level industry terms, synchronous and asynchronous replication, and key behaviors.

**High-level industry terms**

Disaster Recovery (DR) refers to a contingency plan for recovering from site catastrophes so that the business continues to operate. Data DR means multiple copies of production data in a separate physical location. For example, a stretch cluster, where half the nodes are in one site and half are in another. Disaster Preparedness (DP)

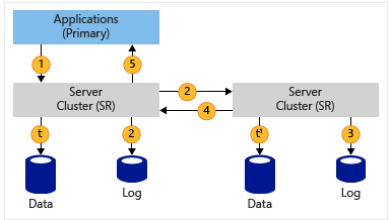
refers to a contingency plan for preemptively moving workloads to a different location prior to an oncoming disaster, such as a hurricane.

Service level agreements (SLAs) define the availability of a business' applications and their tolerance of down time and data loss during planned and unplanned outages. Recovery Time Objective (RTO) defines how long the business can tolerate total inaccessibility of data. Recovery Point Objective (RPO) defines how much data the business can afford to lose.

### Synchronous replication

Synchronous replication guarantees that the application writes data to two locations at once before completion of the IO. This replication is more suitable for mission critical data, as it requires network and storage investments, as well as a risk of degraded application performance.

When application writes occur on the source data copy, the originating storage does not acknowledge the IO immediately. Instead, those data changes replicate to the remote destination copy and return an acknowledgement. Only then does the application receive the IO acknowledgment. This ensures constant synchronization of the remote site with the source site, in effect extending storage IOs across the network. In the event of a source site failure, applications can failover to the remote site and resume their operations with assurance of zero data loss.

| MODE | DIAGRAM | STEPS |
|---|---|---|
| **Synchronous**<br>Zero Data Loss<br>RPO |  | 1. Application writes data<br>2. Log data is written and the data is replicated to the remote site<br>3. Log data is written at the remote site<br>4. Acknowledgement from the remote site<br>5. Application write acknowledged<br>t & t1 : Data flushed to the volume, logs always write through |

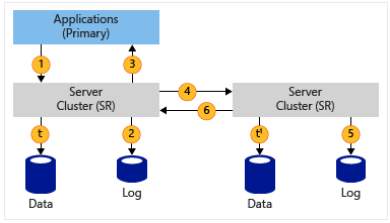
### Asynchronous replication

Contrarily, asynchronous replication means that when the application writes data, that data replicates to the remote site without immediate acknowledgment guarantees. This mode allows faster response time to the application as well as a DR solution that works geographically.

When the application writes data, the replication engine captures the write and immediately acknowledges to the application. The captured data then replicates to the remote location. The remote node processes the copy of the data and lazily acknowledges back to the source copy. Since replication performance is no longer in the application IO path, the remote site's responsiveness and distance are less important factors. There is risk of data loss if the source data is lost and the destination copy of the data was still in buffer without leaving the source.

With its higher than zero RPO, asynchronous replication is less suitable for HA solutions like Failover Clusters, as they are designed for continuous operation with redundancy and no loss of data.

| MODE | DIAGRAM | STEPS |
|---|---|---|

| MODE | DIAGRAM | STEPS |
| --- | --- | --- |
| **Asynchronous**<br>Near zero data loss<br>(depends on multiple factors)<br>RPO |  | 1. Application writes data<br>2. Log data written<br>3. Application write acknowledged<br>4. Data replicated to the remote site<br>5. Log data written at the remote site<br>6. Acknowledgement from the remote site<br>t & t1 : Data flushed to the volume, logs always write through |

**Key evaluation points and behaviors**

- Network bandwidth and latency with fastest storage. There are physical limitations around synchronous replication. Because Storage Replica implements an IO filtering mechanism using logs and requiring network round trips, synchronous replication is likely make application writes slower. By using low latency, high-bandwidth networks as well as high-throughput disk subsystems for the logs, you minimize performance overhead.
- The destination volume is not accessible while replicating in Windows Server 2016. When you configure replication, the destination volume dismounts, making it inaccessible to any reads or writes by users. Its driver letter may be visible in typical interfaces like File Explorer, but an application cannot access the volume itself. Block-level replication technologies are incompatible with allowing access to the destination target's mounted file system in a volume; NTFS and ReFS do not support users writing data to the volume while blocks change underneath them.

The **Test-Failover** cmdlet debuted in Windows Server, version 1709, and was also included in Windows Server 2019. This now supports temporarily mounting a read-write snapshot of the destination volume for backups, testing, etc. See https://aka.ms/srfaq for more info.

- The Microsoft implementation of asynchronous replication is different than most. Most industry implementations of asynchronous replication rely on snapshot-based replication, where periodic differential transfers move to the other node and merge. Storage Replica asynchronous replication operates just like synchronous replication, except that it removes the requirement for a serialized synchronous acknowledgment from the destination. This means that Storage Replica theoretically has a lower RPO as it continuously replicates. However, this also means it relies on internal application consistency guarantees rather than using snapshots to force consistency in application files. Storage Replica guarantees crash consistency in all replication modes
- Many customers use DFS Replication as a disaster recovery solution even though often impractical for that scenario - DFS Replication cannot replicate open files and is designed to minimize bandwidth usage at the expense of performance, leading to large recovery point deltas. Storage Replica may allow you to retire DFS Replication from some of these types of disaster recovery duties.
- Storage Replica is not a backup solution. Some IT environments deploy replication systems as backup solutions, due to their zero data loss options when compared to daily backups. Storage Replica replicates all changes to all blocks of data on the volume, regardless of the change type. If a user deletes all data from a volume, Storage Replica replicates the deletion instantly to the other volume, irrevocably removing the data from both servers. Do not use Storage Replica as a replacement for a point-in-time backup solution.
- Storage Replica is not Hyper-V Replica or Microsoft SQL AlwaysOn Availability Groups. Storage Replica is a general purpose, storage-agnostic engine. By definition, it cannot tailor its behavior as ideally as application-level replication. This may lead to specific feature gaps that encourage you to deploy or remain on specific application replication technologies.

> **NOTE**
>
> This document contains a list of known issues and expected behaviors as well as Frequently Asked Questions section.

### Storage Replica terminology

This guide frequently uses the following terms:

- The source is a computer's volume that allows local writes and replicates outbound. Also known as "primary".
- The destination is a computer's volume that does not allow local writes and replicates inbound. Also known as "secondary".
- A replication partnership is the synchronization relationship between a source and destination computer for one or more volumes and utilizes a single log.
- A replication group is the organization of volumes and their replication configuration within a partnership, on a per server basis. A group may contain one or more volumes.

### What's new for Storage Replica

For a list of new features in Storage Replica in Windows Server 2019, see What's new in storage

## Additional References

- Stretch Cluster Replication Using Shared Storage
- Server to Server Storage Replication
- Cluster to Cluster Storage Replication
- Storage Replica: Known Issues
- Storage Replica: Frequently Asked Questions
- Storage Spaces Direct in Windows Server 2016
- Windows IT Pro Support

# Stretch Cluster Replication Using Shared Storage

12/16/2020 • 30 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

In this evaluation example, you will configure these computers and their storage in a single stretch cluster, where two nodes share one set of storage and two nodes share another set of storage, then replication keeps both sets of storage mirrored in the cluster to allow immediate failover. These nodes and their storage should be located in separate physical sites, although it is not required. There are separate steps for creating Hyper-V and File Server clusters as sample scenarios.

> **IMPORTANT**
> In this evaluation, servers in different sites must be able to communicate with the other servers via a network, but not have any physical connectivity to the other site's shared storage. This scenario does not make use of Storage Spaces Direct.

## Terms

This walkthrough uses the following environment as an example:

- Four servers, named **SR-SRV01**, **SR-SRV02**, **SR-SRV03**, and **SR-SRV04** formed into a single cluster called **SR-SRVCLUS**.
- A pair of logical "sites" that represent two different data centers, with one called **Redmond** and the other called **Bellevue**.

> **NOTE**
> You can use only as few as two nodes, where one node each is in each site. However, you will not be able to perform intra-site failover with only two servers. You can use as many as 64 nodes.

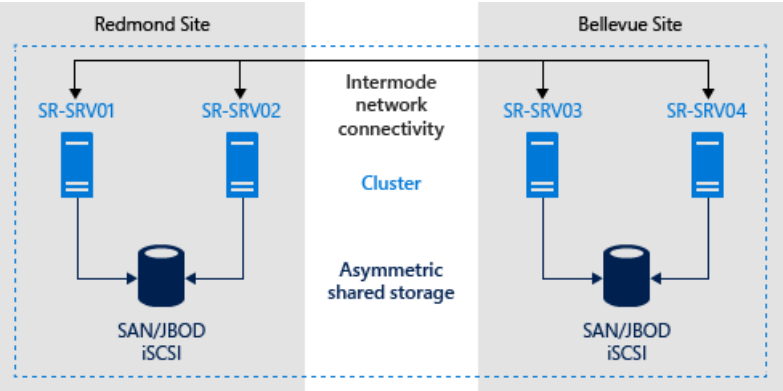



FIGURE 1: Storage Replication in a stretch cluster

## Prerequisites

- Active Directory Domain Services forest (does not need to run Windows Server 2016).
- 2-64 servers running Windows Server 2019 or Windows Server 2016, Datacenter Edition. If you're running Windows Server 2019, you can instead use Standard Edition if you're OK replicating only a single volume up to

2 TB in size.

- Two sets of shared storage, using SAS JBODs (such as with Storage Spaces), Fibre Channel SAN, Shared VHDX, or iSCSI Target. The storage should contain a mix of HDD and SSD media and must support Persistent Reservation. You will make each storage set available to two of the servers only (asymmetric).
- Each set of storage must allow creation of at least two virtual disks, one for replicated data and one for logs. The physical storage must have the same sector sizes on all the data disks. The physical storage must have the same sector sizes on all the log disks.
- At least one 1GbE connection on each server for synchronous replication, but preferably RDMA.
- At least 2GB of RAM and two cores per server. You will need more memory and cores for more virtual machines.
- Appropriate firewall and router rules to allow ICMP, SMB (port 445, plus 5445 for SMB Direct) and WS-MAN (port 5985) bi-directional traffic between all nodes.
- A network between servers with enough bandwidth to contain your IO write workload and an average of =5ms round trip latency, for synchronous replication. Asynchronous replication does not have a latency recommendation.
- The replicated storage cannot be located on the drive containing the Windows operating system folder.

Many of these requirements can be determined by using the `Test-SRTopology` cmdlet. You get access to this tool if you install Storage Replica or the Storage Replica Management Tools features on at least one server. There is no need to configure Storage Replica to use this tool, only to install the cmdlet. More information is included in the following steps.

## Provision operating system, features, roles, storage, and network

1. Install Windows Server on all server nodes, using either the Server Core or Server with Desktop Experience installation options.

   > **IMPORTANT**
   > From this point on, always logon as a domain user who is a member of the built-in administrator group on all servers. Always remember to elevate your PowerShell and CMD prompts going forward when running on a graphical server installation or on a Windows 10 computer.

2. Add network information and join the nodes to the domain, then restart them.

   > **NOTE**
   > As of this point, the guide presumes you have two pairings of servers for use in a stretch cluster. A WAN or LAN network separate the servers and the servers belong to either physical or logical sites. The guide considers **SR-SRV01** and **SR-SRV02** to be in site Redmond and **SR-SRV03** and **SR-SRV04** to be in site **Bellevue**.

3. Connect the first set of shared JBOD storage enclosure, Shared VHDX, iSCSI target, or FC SAN to the servers in site **Redmond**.

4. Connect the second set of storage to the servers in site **Bellevue**.

5. As appropriate, install latest vendor storage and enclosure firmware and drivers, latest vendor HBA drivers, latest vendor BIOS/UEFI firmware, latest vendor network drivers, and latest motherboard chipset drivers on all four nodes. Restart nodes as needed.

> **NOTE**
> Consult your hardware vendor documentation for configuring shared storage and networking hardware.

6. Ensure that BIOS/UEFI settings for servers enable high performance, such as disabling C-State, setting QPI speed, enabling NUMA, and setting highest memory frequency. Ensure power management in Windows Server is set to high performance. Restart as required.

7. Configure roles as follows:

   - **Graphical method**

     Run **ServerManager.exe** and add all server nodes by clicking **Manage** and **Add Servers**.

     > **IMPORTANT**
     > Install the **Failover Clustering**, and **Storage Replica** roles and features on each of the nodes and restart them. If planning to use other roles like Hyper-V, File Server, etc. you can install them now too.

   - **Using Windows PowerShell method**

     On **SR-SRV04** or a remote management computer, run the following command in a Windows PowerShell console to install the required features and roles for a stretch cluster on the four nodes and restart them:

     ```
     $Servers = 'SR-SRV01','SR-SRV02','SR-SRV03','SR-SRV04'

     $Servers | foreach { Install-WindowsFeature -ComputerName $_ -Name Storage-Replica,Failover-
     Clustering,FS-FileServer -IncludeManagementTools -restart }
     ```

     For more information on these steps, see Install or Uninstall Roles, Role Services, or Features.

8. Configure storage as follows:

   > **IMPORTANT**
   > - You must create two volumes on each enclosure: one for data and one for logs.
   > - Log and data disks must be initialized as GPT, not MBR.
   > - The two data volumes must be of identical size.
   > - The two log volumes should be of identical size.
   > - All replicated data disks must have the same sector sizes.
   > - All log disks must have the same sector sizes.
   > - The log volumes should use flash-based storage and high performance resiliency settings. Microsoft recommends that the log storage be as faster than the data storage. Log volumes must never be used for other workloads.
   > - The data disks can use HDD, SSD, or a tiered combination and can use either mirrored or parity spaces or RAID 1 or 10, or RAID 5 or RAID 50.
   > - The log volume must be at least 9GB by default and can to be larger or smaller based on log requirements.
   > - The volumes must be formatted with NTFS or ReFS.
   > - The File Server role is only necessary for Test-SRTopology to operate, as it opens the necessary firewall ports for testing.

   - **For JBOD enclosures:**

a. Ensure that each set of paired server nodes can see that site's storage enclosures only (i.e. asymmetric storage) and that the SAS connections are correctly configured.

b. Provision the storage using Storage Spaces by following **Steps 1-3** provided in the Deploy Storage Spaces on a Stand-Alone Server using Windows PowerShell or Server Manager.

- **For iSCSI storage:**

  a. Ensure that each set of paired server nodes can see that site's storage enclosures only (i.e. asymmetric storage). You should use more than one single network adapter if using iSCSI.

  b. Provision the storage using your vendor documentation. If using Windows-based iSCSI Targeting, consult iSCSI Target Block Storage, How To.

- **For FC SAN storage:**

  a. Ensure that each set of paired server nodes can see that site's storage enclosures only (i.e. asymmetric storage) and that you have properly zoned the hosts.

  b. Provision the storage using your vendor documentation.

## Configure a Hyper-V Failover Cluster or a File Server for a General Use Cluster

After you setup your server nodes, the next step is to create one of the following types of clusters:

- Hyper-V failover cluster
- File Server for general use cluster

**Configure a Hyper-V Failover Cluster**

> **NOTE**
> Skip this section and go to the Configure a file server for general use cluster section, if you want to create a file server cluster and not a Hyper-V cluster.

You will now create a normal failover cluster. After configuration, validation, and testing, you will stretch it using Storage Replica. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

**Graphical method**

1. Run **cluadmin.msc**.
2. Validate the proposed cluster and analyze the results to ensure you can continue.

   > **NOTE**
   > You should expect storage errors from cluster validation, due to the use of asymmetric storage.

3. Create the Hyper-V compute cluster. Ensure that the cluster name is 15 characters or fewer. The example used below is SR-SRVCLUS. If the nodes are going to reside in different subnets, you must create an IP Address for the Cluster Name for each subnet and use the "OR" dependency. More information can be found at Configuring IP Addresses and Dependencies for Multi-Subnet Clusters – Part III.
4. Configure a File Share Witness or Cloud Witness to provide quorum in the event of site loss.

> **NOTE**
> WIndows Server now includes an option for Cloud (Azure)-based Witness. You can choose this quorum option instead of the file share witness.

> **WARNING**
> For more information about quorum configuration, see the Configure and Manage the Quorum in a Windows Server 2012 Failover Cluster guide's Witness Configuration. For more information on the `Set-ClusterQuorum` cmdlet, see Set-ClusterQuorum.

5. Review Network Recommendations for a Hyper-V Cluster in Windows Server 2012 and ensure that you have optimally configured cluster networking.
6. Add one disk in the Redmond site to the cluster CSV. To do so, right click a source disk in the **Disks** node of the **Storage** section, and then click **Add to Cluster Shared Volumes**.
7. Using the Deploy a Hyper-V Cluster guide, follow steps 7-10 within **Redmond** site to create a test virtual machine only to ensure the cluster is working normally within the two nodes sharing the storage in the first test site.
8. If you're creating a two-node stretch cluster, you must add all storage before continuing. To do so, open a PowerShell session with administrative permissions on the cluster nodes, and run the following command: `Get-ClusterAvailableDisk -All | Add-ClusterDisk`.

   This is by-design behavior in Windows Server 2016.
9. Start Windows PowerShell and use the `Test-SRTopology` cmdlet to determine if you meet all the Storage Replica requirements.

   For example, to validate two of the proposed stretch cluster nodes that each have a **D:** and **E:** volume and run the test for 30 minutes:

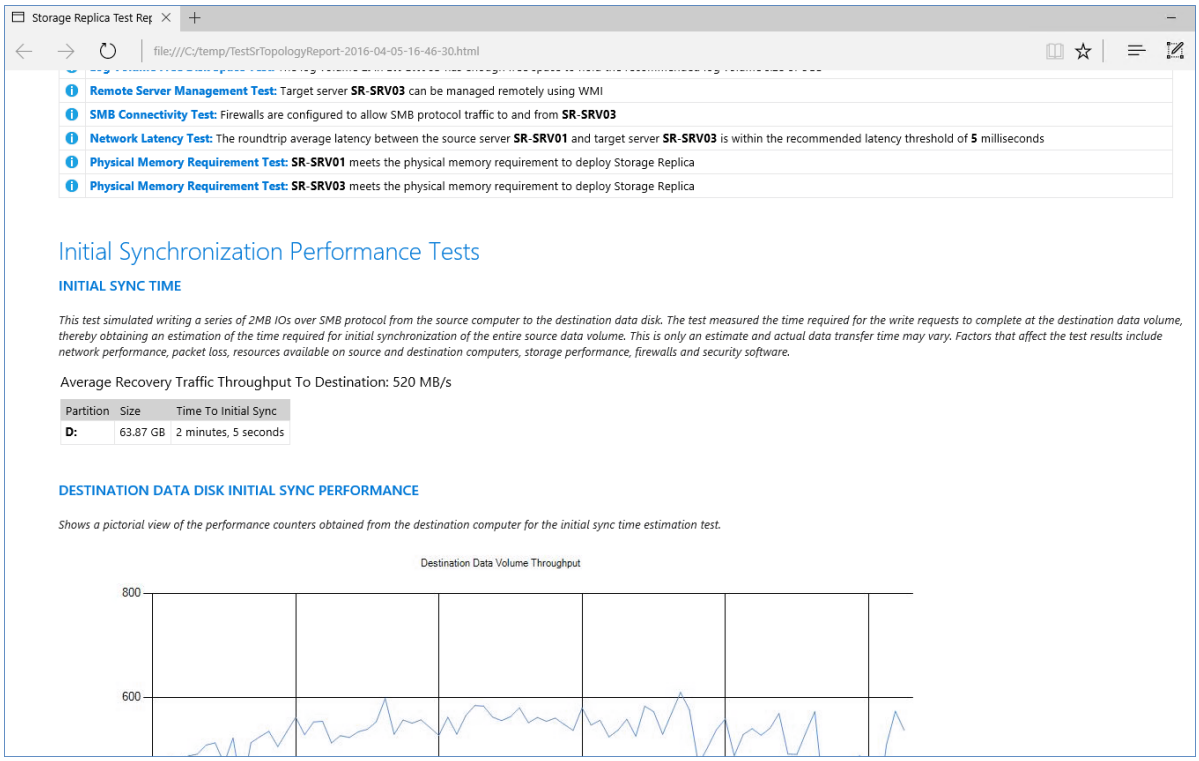
   a. Move all available storage to **SR-SRV01**.
   b. Click **Create Empty Role** in the **Roles** section of Failover Cluster Manager.
   c. Add the online storage to that empty role named **New Role**.
   d. Move all available storage to **SR-SRV03**.
   e. Click **Create Empty Role** in the **Roles** section of Failover Cluster Manager.
   f. Move the empty **New Role (2)** to **SR-SRV03**.
   g. Add the online storage to that empty role named **New Role (2)**.
   h. Now you have mounted all your storage with drive letters, and can evaluate the cluster with `Test-SRTopology`.

      For example:

```
MD c:\temp

Test-SRTopology -SourceComputerName SR-SRV01 -SourceVolumeName D: -SourceLogVolumeName E: -
DestinationComputerName SR-SRV03 -DestinationVolumeName D: -DestinationLogVolumeName E: -
DurationInMinutes 30 -ResultPath c:\temp
```

> **IMPORTANT**
>
> When using a test server with no write IO load on the specified source volume during the evaluation period, consider adding a workload or it Test-SRTopology will not generate a useful report. You should test with production-like workloads in order to see real numbers and recommended log sizes. Alternatively, simply copy some files into the source volume during the test or download and run DISKSPD to generate write IOs. For instance, a sample with a low write IO workload for ten minutes to the D: volume:
>
> `Diskspd.exe -c1g -d600 -W5 -C5 -b4k -t2 -o2 -r -w5 -i100 d:\test.dat`

10. Examine the **TestSrTopologyReport-< date >.html** report to ensure you meet the Storage Replica requirements and note the initial sync time prediction and log recommendations.




11. Return the disks to Available Storage and remove the temporary empty roles.

12. Once satisfied, remove the test virtual machine. Add any real test virtual machines needed for further evaluation to a proposed source node.

13. Configure stretch cluster site awareness so that servers **SR-SRV01** and **SR-SRV02** are in site **Redmond**, **SR-SRV03** and **SR-SRV04** are in site **Bellevue**, and **Redmond** is preferred for node ownership of the source storage and VMs:

```
New-ClusterFaultDomain -Name Seattle -Type Site -Description "Primary" -Location "Seattle Datacenter"

New-ClusterFaultDomain -Name Bellevue -Type Site -Description "Secondary" -Location "Bellevue
Datacenter"

Set-ClusterFaultDomain -Name sr-srv01 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv02 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv03 -Parent Bellevue
Set-ClusterFaultDomain -Name sr-srv04 -Parent Bellevue

(Get-Cluster).PreferredSite="Seattle"
```

> **NOTE**
> There is no option to configure site awareness using Failover Cluster Manager in Windows Server 2016.

14. **(Optional)** Configure cluster networking and Active Directory for faster DNS site failover. You can utilize Hyper-V software defined networking, stretched VLANs, network abstraction devices, lowered DNS TTL, and other common techniques.

    For more information, review the Microsoft Ignite session: Stretching Failover Clusters and Using Storage Replica in Windows Server vNext and the Enable Change Notifications between Sites - How and Why? blog post.

15. **(Optional)** Configure VM resiliency so that guests do not pause for long during node failures. Instead, they failover to the new replication source storage within 10 seconds.

```
(Get-Cluster).ResiliencyDefaultPeriod=10
```

> **NOTE**
> There is no option to configure VM resiliency using Failover Cluster Manager in Windows Server 2016.

**Windows PowerShell method**

1. Test the proposed cluster and analyze the results to ensure you can continue:

```
Test-Cluster SR-SRV01, SR-SRV02, SR-SRV03, SR-SRV04
```

> **NOTE**
> You should expect storage errors from cluster validation, due to the use of asymmetric storage.

2. Create the File Server for General Use storage cluster (you must specify your own static IP address the cluster will use). Ensure that the cluster name is 15 characters or fewer. If the nodes reside in different subnets, than an IP Address for the additional site must be created using the "OR" dependency. More information can be found at Configuring IP Addresses and Dependencies for Multi-Subnet Clusters – Part III.

```
New-Cluster -Name SR-SRVCLUS -Node SR-SRV01, SR-SRV02, SR-SRV03, SR-SRV04 -StaticAddress <your IP here>
Add-ClusterResource -Name NewIPAddress -ResourceType "IP Address" -Group "Cluster Group"
Set-ClusterResourceDependency -Resource "Cluster Name" -Dependency "[Cluster IP Address] or
[NewIPAddress]"
```

3. Configure a File Share Witness or Cloud (Azure) witness in the cluster that points to a share hosted on the domain controller or some other independent server. For example:

```
Set-ClusterQuorum -FileShareWitness \\someserver\someshare
```

> **NOTE**
> WIndows Server now includes an option for Cloud (Azure)-based Witness. You can choose this quorum option instead of the file share witness.

For more information about quorum configuration, see the Configure and Manage the Quorum in a Windows Server 2012 Failover Cluster guide's Witness Configuration. For more information on the `Set-ClusterQuorum` cmdlet, see Set-ClusterQuorum.

4. Review Network Recommendations for a Hyper-V Cluster in Windows Server 2012 and ensure that you have optimally configured cluster networking.

5. If you're creating a two-node stretch cluster, you must add all storage before continuing. To do so, open a PowerShell session with administrative permissions on the cluster nodes, and run the following command: `Get-ClusterAvailableDisk -All | Add-ClusterDisk`.

   This is by-design behavior in Windows Server 2016.

6. Using the Deploy a Hyper-V Cluster guide, follow steps 7-10 within **Redmond** site to create a test virtual machine only to ensure the cluster is working normally within the two nodes sharing the storage in the first test site.

7. Once satisfied, remove the test VM. Add any real test virtual machines needed for further evaluation to a proposed source node.

8. Configure stretch cluster site awareness so that servers **SR-SRV01** and **SR-SRV02** are in site **Redmond**, **SR-SRV03** and **SR-SRV04** are in site **Bellevue**, and **Redmond** is preferred for node ownership of the source storage and virtual machines:

   ```
   New-ClusterFaultDomain -Name Seattle -Type Site -Description "Primary" -Location "Seattle Datacenter"

   New-ClusterFaultDomain -Name Bellevue -Type Site -Description "Secondary" -Location "Bellevue
   Datacenter"

   Set-ClusterFaultDomain -Name sr-srv01 -Parent Seattle
   Set-ClusterFaultDomain -Name sr-srv02 -Parent Seattle
   Set-ClusterFaultDomain -Name sr-srv03 -Parent Bellevue
   Set-ClusterFaultDomain -Name sr-srv04 -Parent Bellevue

   (Get-Cluster).PreferredSite="Seattle"
   ```

9. **(Optional)** Configure cluster networking and Active Directory for faster DNS site failover. You can utilize Hyper-V software defined networking, stretched VLANs, network abstraction devices, lowered DNS TTL, and other common techniques.

   For more information, review the Microsoft Ignite session: Stretching Failover Clusters and Using Storage Replica in Windows Server vNext and Enable Change Notifications between Sites - How and Why.

10. **(Optional)** Configure VM resiliency so that guests do not pause for long periods during node failures. Instead, they failover to the new replication source storage within 10 seconds.

    ```
    (Get-Cluster).ResiliencyDefaultPeriod=10
    ```

> **NOTE**
> There is no option to VM Resiliency using Failover Cluster Manager in Windows Server 2016.

### Configure a File Server for General Use Cluster

> **NOTE**
> Skip this section if you have already configured a Hyper-V Failover cluster as described in Configure a Hyper-V Failover Cluster.

You will now create a normal failover cluster. After configuration, validation, and testing, you will stretch it using Storage Replica. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

#### Graphical method

1. Run cluadmin.msc.
2. Validate the proposed cluster and analyze the results to ensure you can continue.

   > **NOTE**
   > You should expect storage errors from cluster validation, due to the use of asymmetric storage.

3. Create the File Server for General Use storage cluster. Ensure that the cluster name is 15 characters or fewer. The example used below is SR-SRVCLUS. If the nodes are going to reside in different subnets, you must create an IP Address for the Cluster Name for each subnet and use the "OR" dependency. More information can be found at Configuring IP Addresses and Dependencies for Multi-Subnet Clusters – Part III.
4. Configure a File Share Witness or Cloud Witness to provide quorum in the event of site loss.

   > **NOTE**
   > WIndows Server now includes an option for Cloud (Azure)-based Witness. You can choose this quorum option instead of the file share witness.

   > **NOTE**
   > For more information about quorum configuration, see the Configure and Manage the Quorum in a Windows Server 2012 Failover Cluster guide's Witness Configuration. For more information on the Set-ClusterQuorum cmdlet, see Set-ClusterQuorum.

5. If you're creating a two-node stretch cluster, you must add all storage before continuing. To do so, open a PowerShell session with administrative permissions on the cluster nodes, and run the following command: `Get-ClusterAvailableDisk -All | Add-ClusterDisk`.

   This is by-design behavior in Windows Server 2016.

6. Ensure that you have optimally configured cluster networking.

   > **NOTE**
   > The File Server role must be installed on all nodes prior to continuing to the next step. |

7. Under **Roles**, click **Configure Role**. Review **Before you Begin** and click **Next**.
8. Select **File Server** and click **Next**.
9. Leave **File Server for general use** selected and click **Next**.
10. Provide a **Client Access Point** name (15 characters or fewer) and click **Next**.
11. Select a disk to be your data volume and click **Next**.
12. Review your settings and click **Next**. Click **Finish**.
13. Right click your new File Server role and click **Add File Share**. Proceed through the wizard to configure shares.
14. Optional: Add another File Server role that uses the other storage in this site.
15. Configure stretch cluster site awareness so that servers SR-SRV01 and SR-SRV02 are in site Redmond, SR-SRV03 and SR-SRV04 are in site Bellevue, and Redmond is preferred for node ownership of the source storage and VMs:

```
New-ClusterFaultDomain -Name Seattle -Type Site -Description "Primary" -Location "Seattle Datacenter"

New-ClusterFaultDomain -Name Bellevue -Type Site -Description "Secondary" -Location "Bellevue
Datacenter"

Set-ClusterFaultDomain -Name sr-srv01 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv02 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv03 -Parent Bellevue
Set-ClusterFaultDomain -Name sr-srv04 -Parent Bellevue

(Get-Cluster).PreferredSite="Seattle"
```

> **NOTE**
> There is no option to configure site awareness using Failover Cluster Manager in Windows Server 2016.

16. (Optional) Configure cluster networking and Active Directory for faster DNS site failover. You can utilize stretched VLANs, network abstraction devices, lowered DNS TTL, and other common techniques.

For more information, review the Microsoft Ignite session Stretching Failover Clusters and Using Storage Replica in Windows Server vNext and the blog post Enable Change Notifications between Sites - How and Why.

**PowerShell Method**

1. Test the proposed cluster and analyze the results to ensure you can continue:

```
Test-Cluster SR-SRV01, SR-SRV02, SR-SRV03, SR-SRV04
```

> **NOTE**
> You should expect storage errors from cluster validation, due to the use of asymmetric storage.

2. Create the Hyper-V compute cluster (you must specify your own static IP address the cluster will use). Ensure that the cluster name is 15 characters or fewer. If the nodes reside in different subnets, than an IP Address for the additional site must be created using the "OR" dependency. More information can be found at Configuring IP Addresses and Dependencies for Multi-Subnet Clusters – Part III.

```
New-Cluster -Name SR-SRVCLUS -Node SR-SRV01, SR-SRV02, SR-SRV03, SR-SRV04 -StaticAddress <your IP here>

Add-ClusterResource -Name NewIPAddress -ResourceType “IP Address” -Group “Cluster Group”

Set-ClusterResourceDependency -Resource “Cluster Name” -Dependency “[Cluster IP Address] or
[NewIPAddress]”
```

3. Configure a File Share Witness or Cloud (Azure) witness in the cluster that points to a share hosted on the domain controller or some other independent server. For example:

```
Set-ClusterQuorum -FileShareWitness \\someserver\someshare
```

> **NOTE**
> Windows Server now includes an option for cloud witness using Azure. You can choose this quorum option instead of the file share witness.

   For more information about quorum configuration, see the Understanding cluster and pool quorum. For more information on the Set-ClusterQuorum cmdlet, see Set-ClusterQuorum.

4. If you're creating a two-node stretch cluster, you must add all storage before continuing. To do so, open a PowerShell session with administrative permissions on the cluster nodes, and run the following command: `Get-ClusterAvailableDisk -All | Add-ClusterDisk`.

   This is by-design behavior in Windows Server 2016.

5. Ensure that you have optimally configured cluster networking.

6. Configure a File Server role. For example:

```
Get-ClusterResource
Add-ClusterFileServerRole -Name SR-CLU-FS2 -Storage "Cluster Disk 4"

MD e:\share01

New-SmbShare -Name Share01 -Path f:\share01 -ContinuouslyAvailable $false
```

7. Configure stretch cluster site awareness so that servers SR-SRV01 and SR-SRV02 are in site Redmond, SR-SRV03 and SR-SRV04 are in site Bellevue, and Redmond is preferred for node ownership of the source storage and virtual machines:

```
New-ClusterFaultDomain -Name Seattle -Type Site -Description "Primary" -Location "Seattle Datacenter"

New-ClusterFaultDomain -Name Bellevue -Type Site -Description "Secondary" -Location "Bellevue
Datacenter"

Set-ClusterFaultDomain -Name sr-srv01 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv02 -Parent Seattle
Set-ClusterFaultDomain -Name sr-srv03 -Parent Bellevue
Set-ClusterFaultDomain -Name sr-srv04 -Parent Bellevue

(Get-Cluster).PreferredSite="Seattle"
```

8. (Optional) Configure cluster networking and Active Directory for faster DNS site failover. You can utilize stretched VLANs, network abstraction devices, lowered DNS TTL, and other common techniques.

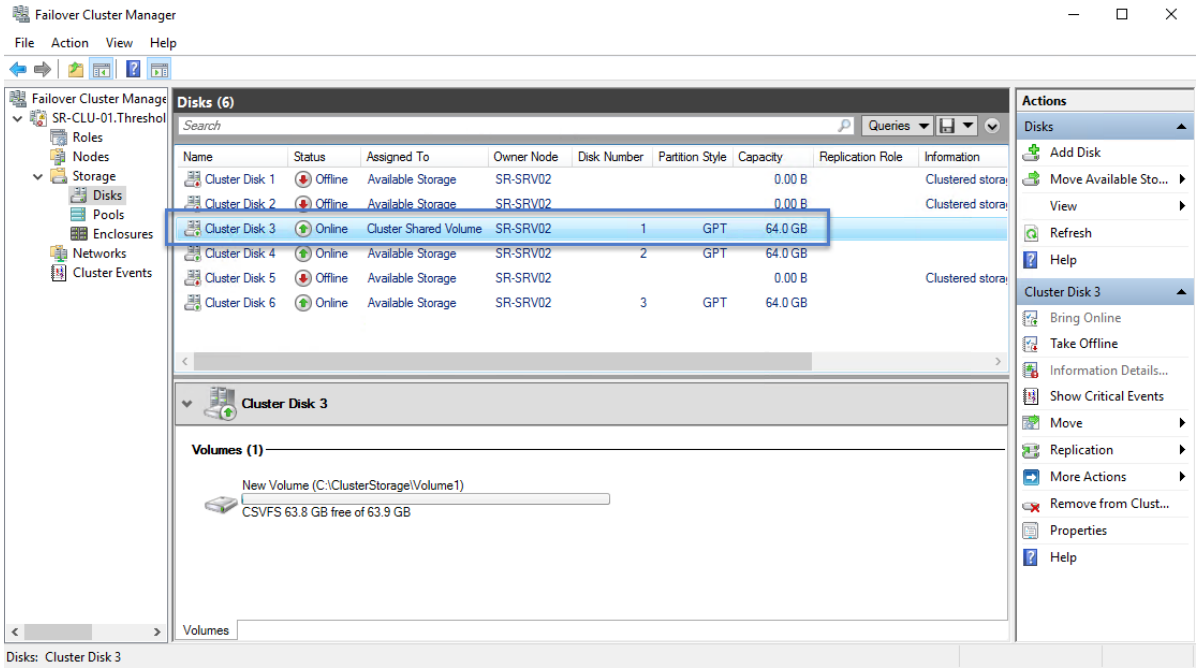
For more information, review the Microsoft Ignite session Stretching Failover Clusters and Using Storage Replica in Windows Server vNext and the blog post Enable Change Notifications between Sites - How and Why.

### Configure a stretch cluster

Now you will configure the stretch cluster, using either Failover Cluster Manager or Windows PowerShell. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

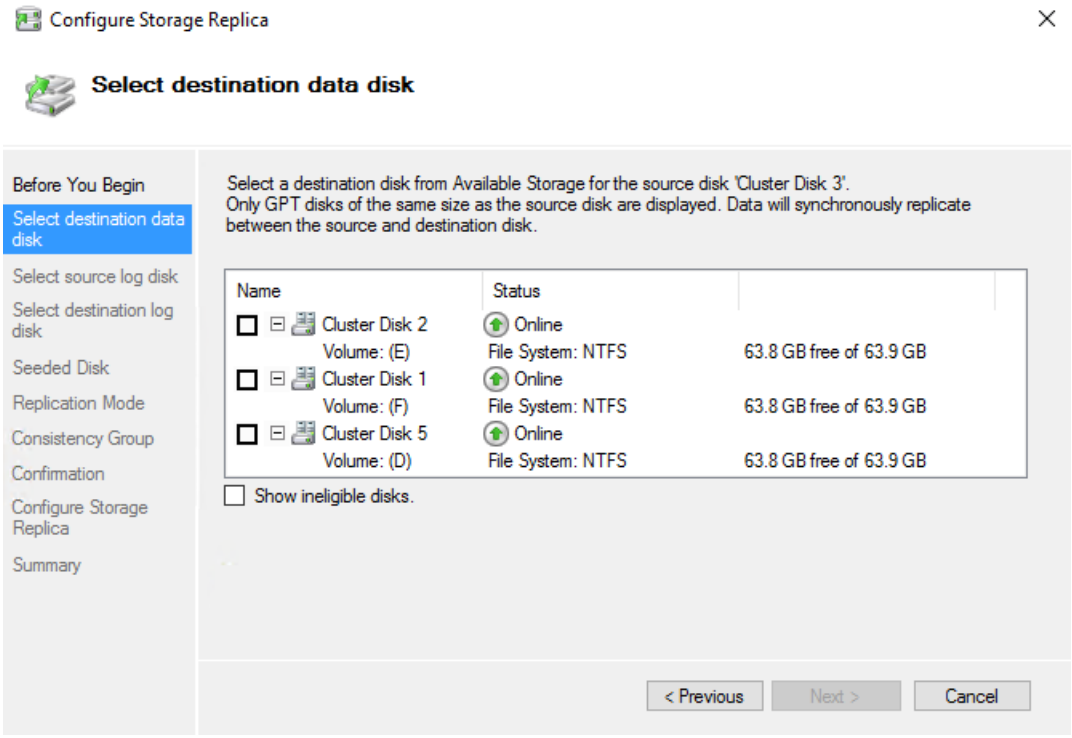
#### Failover Cluster Manager Method

1. For Hyper-V workloads, on one node where you have the data you wish to replicate out, add the source data disk from your available disks to cluster shared volumes if not already configured. Do not add all the disks; just add the single disk. At this point, half the disks will show offline because this is asymmetric storage. If replicating a physical disk resource (PDR) workload like File Server for general use, you already have a role-attached disk ready to go.

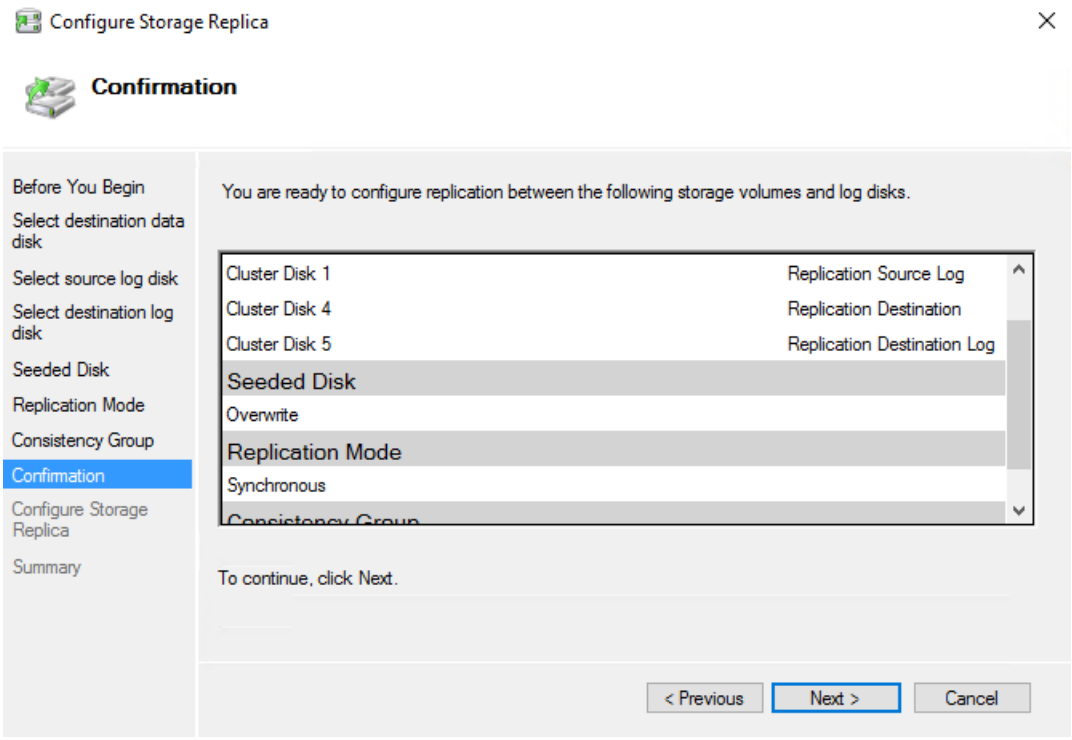



2. Right-click the CSV disk or role-attached disk, click **Replication**, and then click **Enable**.

3. Select the appropriate destination data volume and click **Next**. The destination disks shown will have a volume the same size as the selected source disk. When moving between these wizard dialogs, the available storage will automatically move and come online in the background as needed.



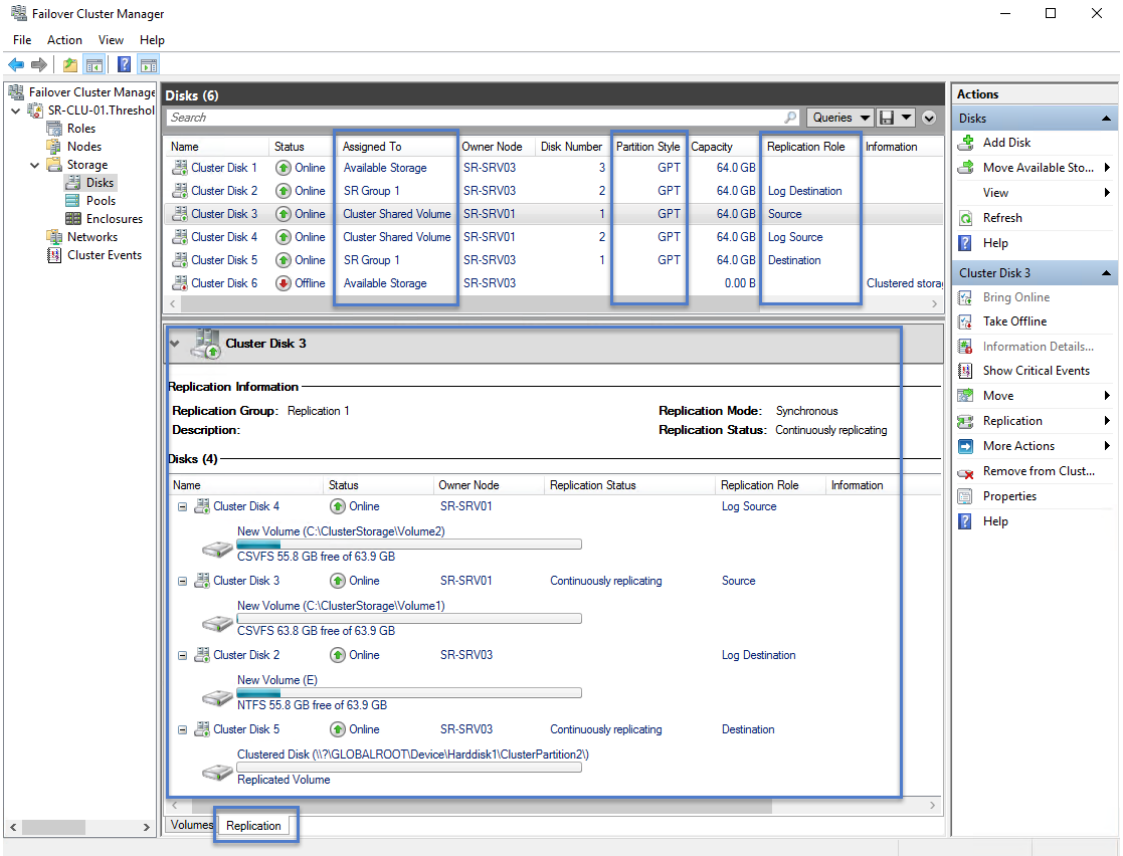

4. Select the appropriate source log disk and click **Next**. The source log volume should be on a disk that uses SSD or similarly fast media, not spinning disks.
5. Select the appropriate destination log volume and click Next. The destination log disks shown will have a volume the same size as the selected source log disk volume.
6. Leave the **Overwrite Volume** value at **Overwrite destination Volume** if the destination volume does not contain a previous copy of the data from the source server. If the destination does contain similar data, from a recent backup or previous replication, select **Seeded destination disk**, and then click **Next**.
7. Leave the **Replication Mode** value at **Synchronous Replication** if you plan to use zero RPO replication. Change it to **Asynchronous Replication** if you plan to stretch your cluster over higher latency networks or need lower IO latency on the primary site nodes.
8. Leave the **Consistency Group** value at **Highest Performance** if you do not plan to use write ordering later with additional disk pairs in the replication group. If you plan to add further disks to this replication group and you require guaranteed write ordering, select **Enable Write Ordering**, and then click **Next**.
9. Click **Next** to configure replication and the stretch cluster formation.




10. On the Summary screen, note the completion dialog results. You can view the report in a web browser.

11. At this point, you have configured a Storage Replica partnership between the two halves of the cluster but replication is ongoing. There are several ways to see the state of replication via a graphical tool.

    a. Use the **Replication Role** column and the **Replication** tab. When done with initial synchronization, the source and destination disks will have a Replication Status of **Continuously Replicating**.




    b. Start **eventvwr.exe**.

        a. On the source server, navigate to **Applications and Services \ Microsoft \ Windows \ StorageReplica \ Admin** and examine events 5015, 5002, 5004, 1237, 5001, and 2200.

b. On the destination server, navigate to **Applications and Services \ Microsoft \ Windows \ StorageReplica \ Operational** and wait for event 1215. This event states the number of copied bytes and the time taken. Example:

```
Log Name:      Microsoft-Windows-StorageReplica/Operational
Source:        Microsoft-Windows-StorageReplica
Date:          4/6/2016 4:52:23 PM
Event ID:      1215
Task Category: (1)
Level:         Information
Keywords:      (1)
User:          SYSTEM
Computer:      SR-SRV03.Threshold.nttest.microsoft.com
Description:
Block copy completed for replica.

ReplicationGroupName: Replication 2
ReplicationGroupId: {c6683340-0eea-4abc-ab95-c7d0026bc054}
ReplicaName: \\?\Volume{43a5aa94-317f-47cb-a335-2a5d543ad536}\
ReplicaId: {00000000-0000-0000-0000-000000000000}
End LSN in bitmap:
LogGeneration: {00000000-0000-0000-0000-000000000000}
LogFileId: 0
CLSFLsn: 0xFFFFFFFF
Number of Bytes Recovered: 68583161856
Elapsed Time (ms): 140
```

c. On the destination server, navigate to **Applications and Services \ Microsoft \ Windows \ StorageReplica \ Admin** and examine events 5009, 1237, 5001, 5015, 5005, and 2200 to understand the processing progress. There should be no warnings of errors in this sequence. There will be many 1237 events; these indicate progress.

> **WARNING**
> CPU and memory usage are likely to be higher than normal until initial synchronization completes.

#### Windows PowerShell method

1. Ensure your Powershell console is running with an elevated administrator account.
2. Add the source data storage only to the cluster as CSV. To get the size, partition, and volume layout of the available disks, use the following commands:

```
Move-ClusterGroup -Name "available storage" -Node sr-srv01

$DiskResources = Get-ClusterResource | Where-Object { $_.ResourceType -eq 'Physical Disk' -and $_.State
-eq 'Online' }
$DiskResources | foreach {
    $resource = $_
    $DiskGuidValue = $resource | Get-ClusterParameter DiskIdGuid

    Get-Disk | where { $_.Guid -eq $DiskGuidValue.Value } | Get-Partition | Get-Volume |
        Select @{N="Name"; E={$resource.Name}}, @{N="Status"; E={$resource.State}}, DriveLetter,
FileSystemLabel, Size, SizeRemaining
} | FT -AutoSize

Move-ClusterGroup -Name "available storage" -Node sr-srv03

$DiskResources = Get-ClusterResource | Where-Object { $_.ResourceType -eq 'Physical Disk' -and $_.State
-eq 'Online' }
$DiskResources | foreach {
    $resource = $_
    $DiskGuidValue = $resource | Get-ClusterParameter DiskIdGuid

    Get-Disk | where { $_.Guid -eq $DiskGuidValue.Value } | Get-Partition | Get-Volume |
        Select @{N="Name"; E={$resource.Name}}, @{N="Status"; E={$resource.State}}, DriveLetter,
FileSystemLabel, Size, SizeRemaining
} | FT -AutoSize
```

3. Set the correct disk to CSV with:

```
Add-ClusterSharedVolume -Name "Cluster Disk 4"
Get-ClusterSharedVolume
Move-ClusterSharedVolume -Name "Cluster Disk 4" -Node sr-srv01
```

4. Configure the stretch cluster, specifying the following:

   - Source and destination nodes (where the source data is a CSV disk and all other disks are not).
   - Source and Destination replication group names.
   - Source and destination disks, where the partition sizes match.
   - Source and destination log volumes, where there is enough free space to contain the log size on both disks and the storage is SSD or similar fast media.
   - Source and destination log volumes, where there is enough free space to contain the log size on both disks and the storage is SSD or similar fast media.
   - Log size.
   - The source log volume should be on a disk that uses SSD or similarly fast media, not spinning disks.

```
New-SRPartnership -SourceComputerName sr-srv01 -SourceRGName rg01 -SourceVolumeName
"C:\ClusterStorage\Volume1" -SourceLogVolumeName e: -DestinationComputerName sr-srv03 -
DestinationRGName rg02 -DestinationVolumeName d: -DestinationLogVolumeName e:
```

> **NOTE**
>
> You can also use `New-SRGroup` on one node in each site and `New-SRPartnership` to create replication in stages, rather than all at once.

5. Determine the replication progress.

a. On the source server, run the following command and examine events 5015, 5002, 5004, 1237, 5001, and 2200:

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica -max 20
```

b. On the destination server, run the following command to see the Storage Replica events that show creation of the partnership. This event states the number of copied bytes and the time taken. Example:

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | Where-Object {$_.ID -eq "1215"} |
fl

TimeCreated  : 4/6/2016 4:52:23 PM
ProviderName : Microsoft-Windows-StorageReplica
Id           : 1215
Message      : Block copy completed for replica.

       ReplicationGroupName: Replication 2
       ReplicationGroupId: {c6683340-0eea-4abc-ab95-c7d0026bc054}
       ReplicaName: ?Volume{43a5aa94-317f-47cb-a335-2a5d543ad536}
       ReplicaId: {00000000-0000-0000-0000-000000000000}
       End LSN in bitmap:
       LogGeneration: {00000000-0000-0000-0000-000000000000}
       LogFileId: 0
       CLSFLsn: 0xFFFFFFFF
       Number of Bytes Recovered: 68583161856
       Elapsed Time (ms): 140
```

c. On the destination server, run the following command and examine events 5009, 1237, 5001, 5015, 5005, and 2200 to understand the processing progress. There should be no warnings of errors in this sequence. There will be many 1237 events; these indicate progress.

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | FL
```

d. Alternately, the destination server group for the replica states the number of byte remaining to copy at all times, and can be queried through PowerShell. For example:

```
(Get-SRGroup).Replicas | Select-Object numofbytesremaining
```

As a progress sample (that will not terminate):

```
while($true) {

 $v = (Get-SRGroup -Name "Replication 2").replicas | Select-Object numofbytesremaining
 [System.Console]::Write("Number of bytes remaining: {0}`r", $v.numofbytesremaining)
 Start-Sleep -s 5
}
```

6. To get replication source and destination state within the stretch cluster, use `Get-SRGroup` and `Get-SRPartnership` to see the configured state of replication in the stretch cluster.

```
Get-SRGroup
Get-SRPartnership
(Get-SRGroup).replicas
```

### Manage stretched cluster replication

Now you will manage and operate your stretch cluster. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

#### Graphical Tools Method

1. Use Failover Cluster Manager to determine the current source and destination of replication and their status.
2. To measure replication performance, run **Perfmon.exe** on both the source and destination nodes.
    a. On the destination node:
        a. Add the **Storage Replica Statistics** objects with all their performance counters for the data volume.
        b. Examine the results.
    b. On the source node:
        a. Add the **Storage Replica Statistics** and **Storage Replica Partition I/O Statistics** objects with all their performance counters for the data volume (the latter is only available with data on the current source server).
        b. Examine the results.
3. To alter replication source and destination within the stretch cluster, use the following methods:
    a. To move the source replication between nodes in the same site: right-click the source CSV, click **Move Storage**, click **Select Node**, and then select a node in the same site. If using non-CSV storage for a role assigned disk, you move the role.
    b. To move the source replication from one site to another: right-click the source CSV, click **Move Storage**, click **Select Node**, and then select a node in another site. If you configured a preferred site, you can use best possible node to always move the source storage to a node in the preferred site. If using non-CSV storage for a role assigned disk, you move the role.
    c. To perform planned failover the replication direction from one site to another: shutdown both nodes in one site using **ServerManager.exe** or **SConfig**.
    d. To perform unplanned failover the replication direction from one site to another: cut power to both nodes in one site.

    > **NOTE**
    > In Windows Server 2016, you may need to use Failover Cluster Manager or Move-ClusterGroup to move the destination disks back to the other site manually after the nodes come back online.

    > **NOTE**
    > Storage Replica dismounts the destination volumes. This is by design.

4. To change the log size from the default 8GB, right-click both the source and destination log disks, click the **Replication Log** tab, then change the sizes on both the disks to match.

> **NOTE**
> The default log size is 8GB. Depending on the results of the `Test-SRTopology` cmdlet, you may decide to use `-LogSizeInBytes` with a higher or lower value.

5. To add another pair of replicated disks to the existing replication group, you must ensure that there is at least one extra disk in available storage. You can then right-click the Source disk and select **Add replication partnership**.

> **NOTE**
> This need for an additional 'dummy' disk in available storage is due to a regression and not intentional. Failover Cluster Manager previously support adding more disks normally and will again in a later release.

6. To remove the existing replication:
   a. Start **cluadmin.msc**.
   b. Right-click the source CSV disk and click **Replication**, then click **Remove**. Accept the warning prompt.
   c. Optionally, remove the storage from CSV to return it to available storage for further testing.

> **NOTE**
> You may need to use **DiskMgmt.msc** or **ServerManager.exe** to add back drive letters to volumes after return to available storage.

#### Windows PowerShell Method

1. Use **Get-SRGroup** and **(Get-SRGroup).Replicas** to determine the current source and destination of replication and their status.
2. To measure replication performance, use the `Get-Counter` cmdlet on both the source and destination nodes. The counter names are:
   - \Storage Replica Partition I/O Statistics(*)\Number of times flush paused
   - \Storage Replica Partition I/O Statistics(*)\Number of pending flush I/O
   - \Storage Replica Partition I/O Statistics(*)\Number of requests for last log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Current Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Number of Application Write Requests
   - \Storage Replica Partition I/O Statistics(*)\Avg. Number of requests per log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Write Latency
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Read Latency
   - \Storage Replica Statistics(*)\Target RPO
   - \Storage Replica Statistics(*)\Current RPO
   - \Storage Replica Statistics(*)\Avg. Log Queue Length

- \Storage Replica Statistics(*)\Current Log Queue Length
- \Storage Replica Statistics(*)\Total Bytes Received
- \Storage Replica Statistics(*)\Total Bytes Sent
- \Storage Replica Statistics(*)\Avg. Network Send Latency
- \Storage Replica Statistics(*)\Replication State
- \Storage Replica Statistics(*)\Avg. Message Round Trip Latency
- \Storage Replica Statistics(*)\Last Recovery Elapsed Time
- \Storage Replica Statistics(*)\Number of Flushed Recovery Transactions
- \Storage Replica Statistics(*)\Number of Recovery Transactions
- \Storage Replica Statistics(*)\Number of Flushed Replication Transactions
- \Storage Replica Statistics(*)\Number of Replication Transactions
- \Storage Replica Statistics(*)\Max Log Sequence Number
- \Storage Replica Statistics(*)\Number of Messages Received
- \Storage Replica Statistics(*)\Number of Messages Sent

For more information on performance counters in Windows PowerShell, see Get-Counter.

3. To alter replication source and destination within the stretch cluster, use the following methods:

   a. To move the replication source from one node to another in the **Redmond** site, move the CSV resource using the Move-ClusterSharedVolume cmdlet.

   ```
   Get-ClusterSharedVolume | fl *
   Move-ClusterSharedVolume -Name "cluster disk 4" -Node sr-srv02
   ```

   b. To move the replication direction from one site to another "planned", move the CSV resource using the **Move-ClusterSharedVolume** cmdlet.

   ```
   Get-ClusterSharedVolume | fl *
   Move-ClusterSharedVolume -Name "cluster disk 4" -Node sr-srv04
   ```

   This will also move the logs and data appropriately for the other site and nodes.

   c. To perform unplanned failover the replication direction from one site to another: cut power to both nodes in one site.

   > **NOTE**
   > Storage Replica dismounts the destination volumes. This is by design.

4. To change the log size from the default 8GB, use **Set-SRGroup** on both the source and destination Storage Replica Groups. For example, to set all logs to 2GB:

   ```
   Get-SRGroup | Set-SRGroup -LogSizeInBytes 2GB
   Get-SRGroup
   ```

5. To add another pair of replicated disks to the existing replication group, you must ensure that there is at least one extra disk in available storage. You can then right click the Source disk and select add replication partnership.

   > **NOTE**
   > This need for an additional 'dummy' disk in available storage is due to a regression and not intentional. Failover Cluster Manager previously support adding more disks normally and will again in a later release.

   Use the **Set-SRPartnership** cmdlet with the **-SourceAddVolumePartnership** and **-DestinationAddVolumePartnership** parameters.

6. To remove replication, use `Get-SRGroup`, Get-`SRPartnership`, `Remove-SRGroup`, and `Remove-SRPartnership` on any node.

   ```
   Get-SRPartnership | Remove-SRPartnership
   Get-SRGroup | Remove-SRGroup
   ```

   > **NOTE**
   > If using a remote management computer you will need to specify the cluster name to these cmdlets and provide the two RG names.

**Related Topics**

- Storage Replica Overview
- Server to Server Storage Replication
- Cluster to Cluster Storage Replication
- Storage Replica: Known Issues
- Storage Replica: Frequently Asked Questions

## See Also

- Windows Server 2016
- Storage Spaces Direct in Windows Server 2016

# Server-to-server storage replication with Storage Replica

11/2/2020 • 17 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

You can use Storage Replica to configure two servers to sync data so that each has an identical copy of the same volume. This topic provides some background of this server-to-server replication configuration, as well as how to set it up and manage the environment.

To manage Storage Replica you can use Windows Admin Center or PowerShell.

Here's an overview video of using Storage Replica in Windows Admin Center.

## Prerequisites

- Active Directory Domain Services forest (doesn't need to run Windows Server 2016).
- Two servers running Windows Server 2019 or Windows Server 2016, Datacenter Edition. If you're running Windows Server 2019, you can instead use Standard Edition if you're OK replicating only a single volume up to 2 TB in size.
- Two sets of storage, using SAS JBODs, fibre channel SAN, iSCSI target, or local SCSI/SATA storage. The storage should contain a mix of HDD and SSD media. You will make each storage set available only to each of the servers, with no shared access.
- Each set of storage must allow creation of at least two virtual disks, one for replicated data and one for logs. The physical storage must have the same sector sizes on all the data disks. The physical storage must have the same sector sizes on all the log disks.
- At least one ethernet/TCP connection on each server for synchronous replication, but preferably RDMA.
- Appropriate firewall and router rules to allow ICMP, SMB (port 445, plus 5445 for SMB Direct) and WS-MAN (port 5985) bi-directional traffic between all nodes.
- A network between servers with enough bandwidth to contain your IO write workload and an average of =5ms round trip latency, for synchronous replication. Asynchronous replication doesn't have a latency recommendation.
  If you're replicating between on-premises servers and Azure VMs, you must create a network link between the on-premises servers and the Azure VMs. To do so, use Express Route, a Site-to-Site VPN gateway connection, or install VPN software in your Azure VMs to connect them with your on-premises network.
- The replicated storage cannot be located on the drive containing the Windows operating system folder.

> **IMPORTANT**
> In this scenario, each server should be in a different physical or logical site. Each server must be able to communicate with the other via a network.

Many of these requirements can be determined by using the `Test-SRTopology cmdlet`. You get access to this tool if you install Storage Replica or the Storage Replica Management Tools features on at least one server. There is no need to configure Storage Replica to use this tool, only to install the cmdlet. More information is included in the steps below.

## Windows Admin Center requirements

To use Storage Replica and Windows Admin Center together, you need the following:

| SYSTEM | OPERATING SYSTEM | REQUIRED FOR |
|---|---|---|
| Two servers<br>(any mix of on-premises hardware, VMs, and cloud VMs including Azure VMs) | Windows Server 2019, Windows Server 2016, or Windows Server (Semi-Annual Channel) | Storage Replica |
| One PC | Windows 10 | Windows Admin Center |

> **NOTE**
> Right now you can't use Windows Admin Center on a server to manage Storage Replica.

## Terms

This walkthrough uses the following environment as an example:

- Two servers, named **SR-SRV05** and **SR-SRV06**.
- A pair of logical "sites" that represent two different data centers, with one called **Redmond** and one called **Bellevue**.

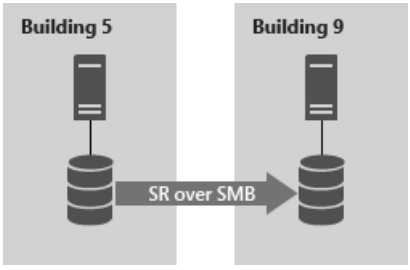



**Figure 1: Server to server replication**

## Step 1: Install and configure Windows Admin Center on your PC

If you're using Windows Admin Center to manage Storage Replica, use the following steps to prep your PC to manage Storage Replica.

1. Download and install Windows Admin Center.
2. Download and install the Remote Server Administration Tools.
   - If you're using Windows 10, version 1809 or later, install the "RSAT: Storage Replica Module for Windows PowerShell" from Features on Demand.
3. Open a PowerShell session as administrator by selecting the **Start** button, typing **PowerShell**, right-clicking **Windows PowerShell,** and then selecting **Run as administrator**.
4. Enter the following command to enable the WS-Management protocol on the local computer and set up the default configuration for remote management on the client.

   ```
   winrm quickconfig
   ```

5. Type **Y** to enable WinRM services and enable WinRM Firewall Exception.

## Step 2: Provision operating system, features, roles, storage, and network

1. Install Windows Server on both server nodes with an installation type of Windows Server **(Desktop Experience)**.

   To use an Azure VM connected to your network via an ExpressRoute, see Adding an Azure VM connected to your network via ExpressRoute.

   > **NOTE**
   > Starting in Windows Admin Center version 1910, you can configure a destination server automatically in Azure. If you choose that option, install Windows Server on the source server and then skip to Step 3: Set up server-to-server replication.

2. Add network information, join the servers to the same domain as your Windows 10 management PC (if you're using one), and then restart the servers.

   > **NOTE**
   > From this point on, always logon as a domain user who is a member of the built-in administrator group on all servers. Always remember to elevate your PowerShell and CMD prompts going forward when running on a graphical server installation or on a Windows 10 computer.

3. Connect the first set of JBOD storage enclosure, iSCSI target, FC SAN, or local fixed disk (DAS) storage to the server in site **Redmond**.

4. Connect the second set of storage to the server in site **Bellevue**.

5. As appropriate, install latest vendor storage and enclosure firmware and drivers, latest vendor HBA drivers, latest vendor BIOS/UEFI firmware, latest vendor network drivers, and latest motherboard chipset drivers on both nodes. Restart nodes as needed.

   > **NOTE**
   > Consult your hardware vendor documentation for configuring shared storage and networking hardware.

6. Ensure that BIOS/UEFI settings for servers enable high performance, such as disabling C-State, setting QPI speed, enabling NUMA, and setting highest memory frequency. Ensure power management in Windows Server is set to High Performance. Restart as required.

7. Configure roles as follows:

   - **Windows Admin Center method**

     a. In Windows Admin Center, navigate to Server Manager, and then select one of the servers.
     b. Navigate to **Roles & Features**.
     c. Select **Features** > **Storage Replica**, and then click **Install**.
     d. Repeat on the other server.

   - **Server Manager method**

     a. Run **ServerManager.exe** and create a Server Group, adding all server nodes.

     b. Install the **File Server** and **Storage Replica** roles and features on each of the nodes and

restart them.

- **Windows PowerShell method**

  On SR-SRV06 or a remote management computer, run the following command in a Windows PowerShell console to install the required features and roles and restart them:

  ```
  $Servers = 'SR-SRV05','SR-SRV06'

  $Servers | ForEach { Install-WindowsFeature -ComputerName $_ -Name Storage-Replica,FS-FileServer
  -IncludeManagementTools -restart }
  ```

  For more information on these steps, see Install or Uninstall Roles, Role Services, or Features

8. Configure storage as follows:

> **IMPORTANT**
> - You must create two volumes on each enclosure: one for data and one for logs.
> - Log and data disks must be initialized as GPT, not MBR.
> - The two data volumes must be of identical size.
> - The two log volumes should be of identical size.
> - All replicated data disks must have the same sector sizes.
> - All log disks must have the same sector sizes.
> - The log volumes should use flash-based storage, such as SSD. Microsoft recommends that the log storage be faster than the data storage. Log volumes must never be used for other workloads.
> - The data disks can use HDD, SSD, or a tiered combination and can use either mirrored or parity spaces or RAID 1 or 10, or RAID 5 or RAID 50.
> - The log volume must be at least 9GB by default and may be larger or smaller based on log requirements.
> - The File Server role is only necessary for Test-SRTopology to operate, as it opens the necessary firewall ports for testing.

- **For JBOD enclosures:**

  a. Ensure that each server can see that site's storage enclosures only and that the SAS connections are correctly configured.

  b. Provision the storage using Storage Spaces by following **Steps 1-3** provided in the Deploy Storage Spaces on a Stand-Alone Server using Windows PowerShell or Server Manager.

- **For iSCSI storage:**

  a. Ensure that each cluster can see that site's storage enclosures only. You should use more than one single network adapter if using iSCSI.

  b. Provision the storage using your vendor documentation. If using Windows-based iSCSI Targeting, consult iSCSI Target Block Storage, How To.

- **For FC SAN storage:**

  a. Ensure that each cluster can see that site's storage enclosures only and that you have properly zoned the hosts.

  b. Provision the storage using your vendor documentation.

- **For local fixed disk storage:**

  - Ensure the storage doesn't contain a system volume, page file, or dump files.

- Provision the storage using your vendor documentation.

9. Start Windows PowerShell and use the **Test-SRTopology** cmdlet to determine if you meet all the Storage Replica requirements. You can use the cmdlet in a requirements-only mode for a quick test as well as a long running performance evaluation mode.

   For example, to validate the proposed nodes that each have a **F:** and **G:** volume and run the test for 30 minutes:

   ```
   MD c:\temp

   Test-SRTopology -SourceComputerName SR-SRV05 -SourceVolumeName f: -SourceLogVolumeName g: -
   DestinationComputerName SR-SRV06 -DestinationVolumeName f: -DestinationLogVolumeName g: -
   DurationInMinutes 30 -ResultPath c:\temp
   ```

   **IMPORTANT**

   When using a test server with no write IO load on the specified source volume during the evaluation period, consider adding a workload or it will not generate a useful report. You should test with production-like workloads in order to see real numbers and recommended log sizes. Alternatively, simply copy some files into the source volume during the test or download and run DISKSPD to generate write IOs. For instance, a sample with a low write IO workload for ten minutes to the D: volume:

   ```
   Diskspd.exe -c1g -d600 -W5 -C5 -b8k -t2 -o2 -r -w5 -i100 -j100 d:\test
   ```

10. Examine the **TestSrTopologyReport.html** report shown in Figure 2 to ensure that you meet the Storage Replica requirements.

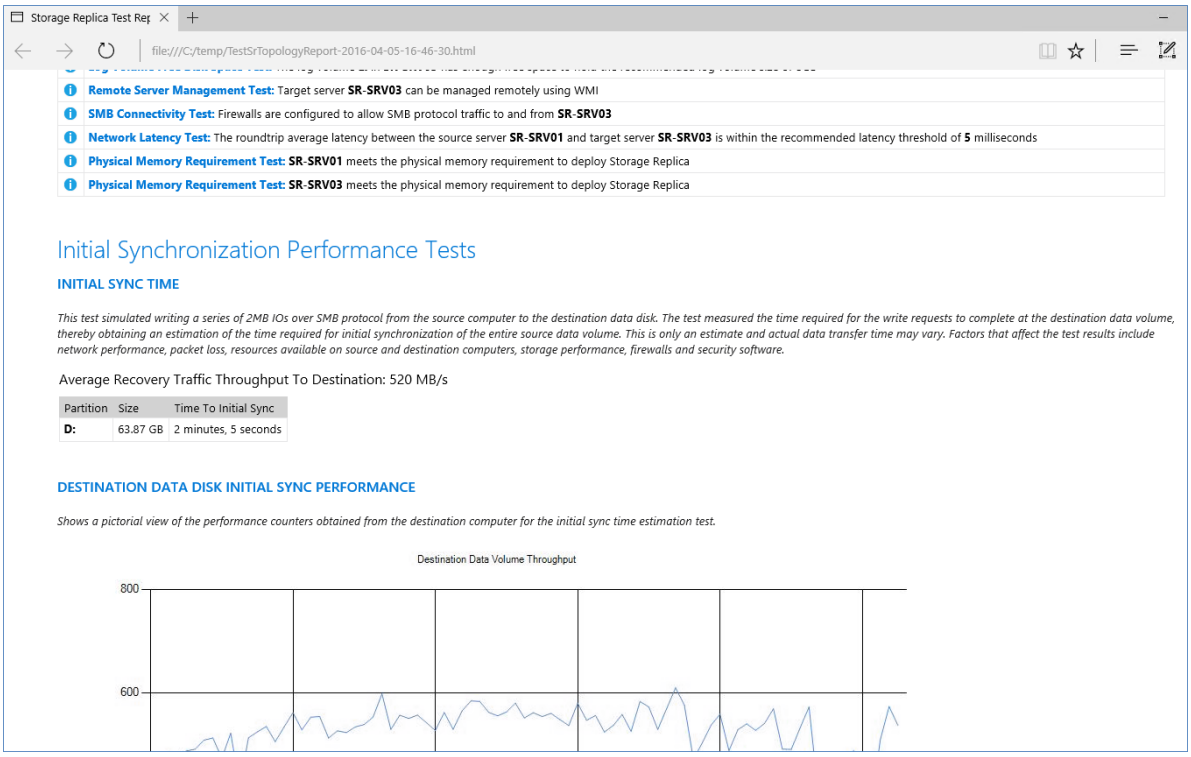



**Figure 2: Storage replication topology report**

# Step 3: Set up server-to-server replication

### Using Windows Admin Center

1. Add the source server.

a. Select the **Add** button.
b. Select **Add server connection**.
c. Type the name of the server and then select **Submit**.

2. On the **All Connections** page, select the source server.
3. Select **Storage Replica** from Tools panel.
4. Select **New** to create a new partnership. To create a new Azure VM to use as the destination for the partnership:

   a. Under **Replicate with another server** select **Use a New Azure VM** and then select **Next**. If you don't see this option, make sure that you're using Windows Admin Center version 1910 or a later version.
   b. Specify your source server information and replication group name, and then select **Next**.

      This begins a process that automatically selects a Windows Server 2019 or Windows Server 2016 Azure VM as a destination for the migration source. Storage Migration Service recommends VM sizes to match your source, but you can override this by selecting **See all sizes**. Inventory data is used to automatically configure your managed disks and their file systems, as well as join your new Azure VM to your Active Directory domain.
   c. After Windows Admin Center creates the Azure VM, provide a replication group name and then select **Create**. Windows Admin Center then begins the normal Storage Replica initial synchronization process to start protecting your data.

   Here's a video showing how to use Storage Replica to migrate to Azure VMs.

5. Provide the details of the partnership, and then select **Create** (as shown in Figure 3).

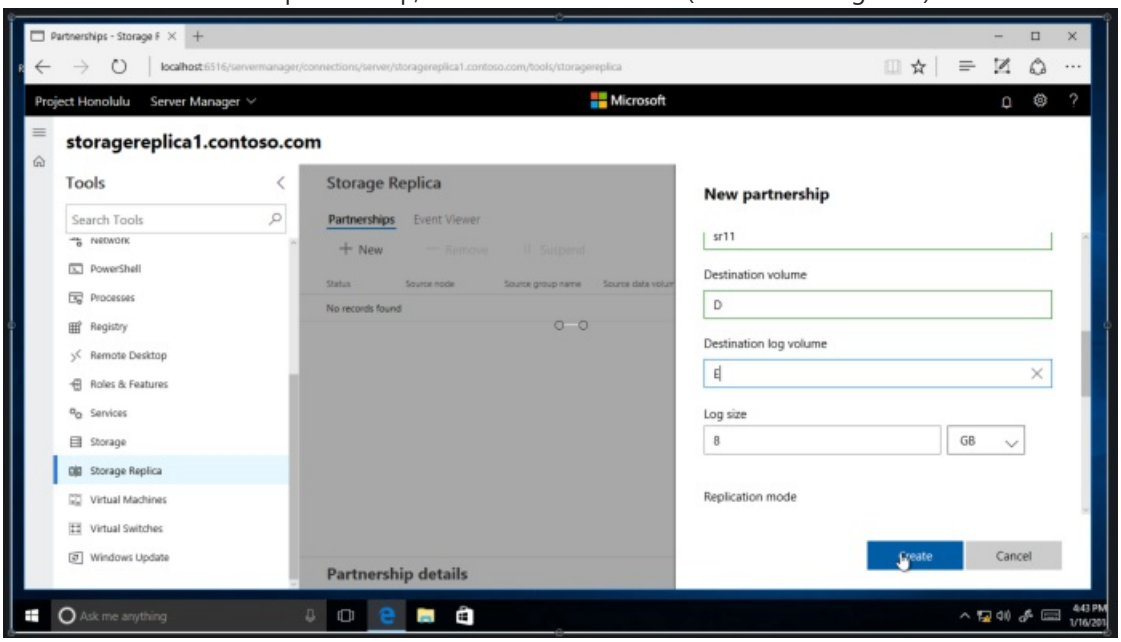



Figure 3: Creating a new partnership

> **NOTE**
> Removing the partnership from Storage Replica in Windows Admin Center doesn't remove the replication group name.

### Using Windows PowerShell

Now you will configure server-to-server replication using Windows PowerShell. You must perform all of the steps below on the nodes directly or from a remote management computer that contains the Windows Server Remote

Server Administration Tools.

1. Ensure you are using an elevated Powershell console as an administrator.
2. Configure the server-to-server replication, specifying the source and destination disks, the source and destination logs, the source and destination nodes, and the log size.

```
New-SRPartnership -SourceComputerName sr-srv05 -SourceRGName rg01 -SourceVolumeName f: -
SourceLogVolumeName g: -DestinationComputerName sr-srv06 -DestinationRGName rg02 -DestinationVolumeName
f: -DestinationLogVolumeName g:
```

   Output:

```
DestinationComputerName : SR-SRV06
DestinationRGName       : rg02
SourceComputerName      : SR-SRV05
PSComputerName          :
```

   **IMPORTANT**

   The default log size is 8GB. Depending on the results of the `Test-SRTopology` cmdlet, you may decide to use -LogSizeInBytes with a higher or lower value.

3. To get replication source and destination state, use `Get-SRGroup` and `Get-SRPartnership` as follows:

```
Get-SRGroup
Get-SRPartnership
(Get-SRGroup).replicas
```

   Output:

```
CurrentLsn             : 0
DataVolume             : F:\
LastInSyncTime         :
LastKnownPrimaryLsn    : 1
LastOutOfSyncTime      :
NumOfBytesRecovered    : 37731958784
NumOfBytesRemaining    : 30851203072
PartitionId            : c3999f10-dbc9-4a8e-8f9c-dd2ee6ef3e9f
PartitionSize          : 68583161856
ReplicationMode        : synchronous
ReplicationStatus      : InitialBlockCopy
PSComputerName         :
```

4. Determine the replication progress as follows:

   a. On the source server, run the following command and examine events 5015, 5002, 5004, 1237, 5001, and 2200:

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica -max 20
```

   b. On the destination server, run the following command to see the Storage Replica events that show creation of the partnership. This event states the number of copied bytes and the time taken. Example:

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | Where-Object {$_.ID -eq "1215"} |
fl
```

Here's some example output:

```
TimeCreated  : 4/8/2016 4:12:37 PM
ProviderName : Microsoft-Windows-StorageReplica
Id           : 1215
Message      : Block copy completed for replica.

ReplicationGroupName: rg02
ReplicationGroupId: {616F1E00-5A68-4447-830F-B0B0EFBD359C}
ReplicaName: f:\
ReplicaId: {00000000-0000-0000-0000-000000000000}
End LSN in bitmap:
LogGeneration: {00000000-0000-0000-0000-000000000000}
LogFileId: 0
CLSFLsn: 0xFFFFFFFF
Number of Bytes Recovered: 68583161856
Elapsed Time (ms): 117
```

> **NOTE**
> Storage Replica dismounts the destination volumes and their drive letters or mount points. This is by design.

c. Alternatively, the destination server group for the replica states the number of byte remaining to copy at all times, and can be queried through PowerShell. For example:

```
(Get-SRGroup).Replicas | Select-Object numofbytesremaining
```

As a progress sample (that will not terminate):

```
while($true) {

 $v = (Get-SRGroup -Name "RG02").replicas | Select-Object numofbytesremaining
 [System.Console]::Write("Number of bytes remaining: {0}`r", $v.numofbytesremaining)
 Start-Sleep -s 5
}
```

d. On the destination server, run the following command and examine events 5009, 1237, 5001, 5015, 5005, and 2200 to understand the processing progress. There should be no warnings of errors in this sequence. There will be many 1237 events; these indicate progress.

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | FL
```

## Step 4: Manage replication

Now you will manage and operate your server-to-server replicated infrastructure. You can perform all of the steps below on the nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

1. Use `Get-SRPartnership` and `Get-SRGroup` to determine the current source and destination of replication and their status.

2. To measure replication performance, use the `Get-Counter` cmdlet on both the source and destination nodes. The counter names are:

   - \Storage Replica Partition I/O Statistics(*)\Number of times flush paused
   - \Storage Replica Partition I/O Statistics(*)\Number of pending flush I/O
   - \Storage Replica Partition I/O Statistics(*)\Number of requests for last log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Current Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Number of Application Write Requests
   - \Storage Replica Partition I/O Statistics(*)\Avg. Number of requests per log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Write Latency
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Read Latency
   - \Storage Replica Statistics(*)\Target RPO
   - \Storage Replica Statistics(*)\Current RPO
   - \Storage Replica Statistics(*)\Avg. Log Queue Length
   - \Storage Replica Statistics(*)\Current Log Queue Length
   - \Storage Replica Statistics(*)\Total Bytes Received
   - \Storage Replica Statistics(*)\Total Bytes Sent
   - \Storage Replica Statistics(*)\Avg. Network Send Latency
   - \Storage Replica Statistics(*)\Replication State
   - \Storage Replica Statistics(*)\Avg. Message Round Trip Latency
   - \Storage Replica Statistics(*)\Last Recovery Elapsed Time
   - \Storage Replica Statistics(*)\Number of Flushed Recovery Transactions
   - \Storage Replica Statistics(*)\Number of Recovery Transactions
   - \Storage Replica Statistics(*)\Number of Flushed Replication Transactions
   - \Storage Replica Statistics(*)\Number of Replication Transactions
   - \Storage Replica Statistics(*)\Max Log Sequence Number
   - \Storage Replica Statistics(*)\Number of Messages Received
   - \Storage Replica Statistics(*)\Number of Messages Sent

   For more information on performance counters in Windows PowerShell, see Get-Counter.

3. To move the replication direction from one site, use the `Set-SRPartnership` cmdlet.

```
Set-SRPartnership -NewSourceComputerName sr-srv06 -SourceRGName rg02 -DestinationComputerName sr-srv05
-DestinationRGName rg01
```

> **WARNING**
> Windows Server prevents role switching when the initial sync is ongoing, as it can lead to data loss if you attempt to switch before allowing initial replication to complete. Don't force switch directions until the initial sync is complete.

Check the event logs to see the direction of replication change and recovery mode occur, and then reconcile. Write IOs can then write to the storage owned by the new source server. Changing the replication direction will block write IOs on the previous source computer.

4. To remove replication, use `Get-SRGroup`, `Get-SRPartnership`, `Remove-SRGroup`, and `Remove-SRPartnership` on each node. Ensure you run the `Remove-SRPartnership` cmdlet on the current source of replication only, not on the destination server. Run `Remove-Group` on both servers. For example, to remove all replication from two servers:

```
Get-SRPartnership
Get-SRPartnership | Remove-SRPartnership
Get-SRGroup | Remove-SRGroup
```

## Replacing DFS Replication with Storage Replica

Many Microsoft customers deploy DFS Replication as a disaster recovery solution for unstructured user data like home folders and departmental shares. DFS Replication has shipped in Windows Server 2003 R2 and all later operating systems and operates on low bandwidth networks, which makes it attractive for high latency and low change environments with many nodes. However, DFS Replication has notable limitations as a data replication solution:

- It doesn't replicate in-use or open files.
- It doesn't replicate synchronously.
- Its asynchronous replication latency can be many minutes, hours, or even days.
- It relies on a database that can require lengthy consistency checks after a power interruption.
- It's generally configured as multi-master, which allows changes to flow in both directions, possibly overwriting newer data.

Storage Replica has none of these limitations. It does, however, have several that might make it less interesting in some environments:

- It only allows one-to-one replication between volumes. It's possible to replicate different volumes between multiple servers.
- While it supports asynchronous replication, it's not designed for low bandwidth, high latency networks.
- It doesn't allow user access to the protected data on the destination while replication is ongoing

If these are not blocking factors, Storage Replica allows you to replace DFS Replication servers with this newer technology. The process is, at a high level:

1. Install Windows Server on two servers and configure your storage. This could mean upgrading an existing set of servers or cleanly installing.

2. Ensure that any data you want to replicate exists on one or more data volumes and not on the C: drive. a. You can also seed the data on the other server to save time, using a backup or file copies, as well as use thin provisioned storage. Making the metadata-like security match perfectly is unnecessary, unlike DFS Replication.

3. Share the data on your source server and make it accessible through a DFS namespace. This is important, to ensure that users can still access it if the server name changes to one in a disaster site. a. You can create

matching shares on the destination server, which will be unavailable during normal operations, b. Don't add the destination server to the DFS Namespaces namespace, or if you do, ensure that all its folder targets are disabled.

4. Enable Storage Replica replication and complete initial sync. Replication can be either synchronous or asynchronous. a. However, synchronous is recommended in order to guarantee IO data consistency on the destination server. b. We strongly recommend enabling Volume Shadow Copies and periodically taking snapshots with VSSADMIN or your other tools of choice. This will guarantee applications flush their data files to disk consistently. In the event of a disaster, you can recover files from snapshots on the destination server that might have been partially replicated asynchronously. Snapshots replicate along with files.
5. Operate normally until there is a disaster.
6. Switch the destination server to be the new source, which surfaces its replicated volumes to users.
7. If using synchronous replication, no data restore will be necessary unless the user was using an application that was writing data without transaction protection (this is irrespective of replication) during loss of the source server. If using asynchronous replication, the need for a VSS snapshot mount is higher but consider using VSS in all circumstances for application consistent snapshots.
8. Add the server and its shares as a DFS Namespaces folder target.
9. Users can then access their data.

> **NOTE**
>
> Disaster Recovery planning is a complex subject and requires great attention to detail. Creation of runbooks and the performance of annual live failover drills is highly recommended. When an actual disaster strikes, chaos will rule and experienced personnel may be unavailable.

## Adding an Azure VM connected to your network via ExpressRoute

1. Create an ExpressRoute in the Azure portal.
   After the ExpressRoute is approved, a resource group is added to the subscription - navigate to **Resource groups** to view this new group. Take note of the virtual network name.

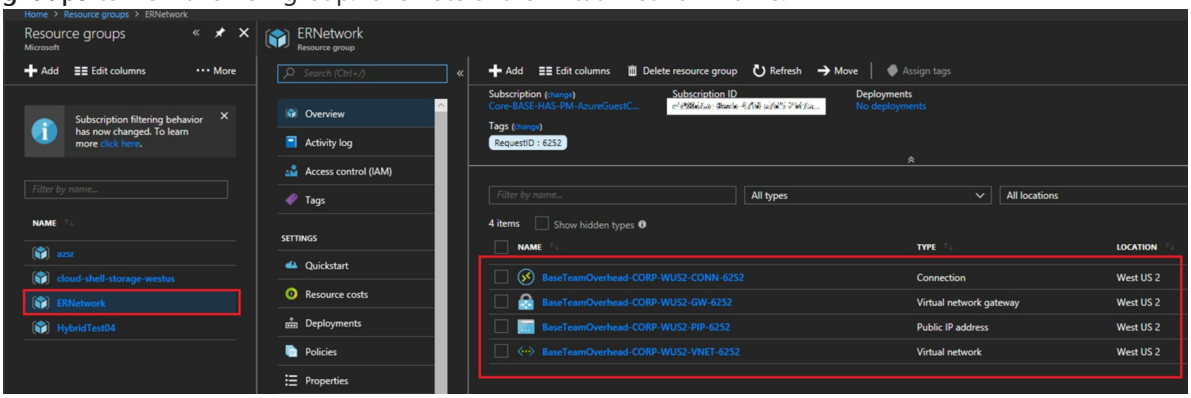



**Figure 4: The resources associated with an ExpressRoute - take note of the virtual network name**

2. Create a new resource group.
3. Add a network security group. When creating it, select the subscription ID associated with the ExpressRoute you created, and select the resource group you just created as well.

   Add any inbound and outbound security rules you need to the network security group. For example, you might want to allow Remote Desktop access to the VM.

4. Create an Azure VM with the following settings (shown in Figure 5):

   - **Public IP address**: None
   - **Virtual network**: Select the virtual network you took note of from the resource group added with the ExpressRoute.
   - **Network security group (firewall)**: Select the network security group you created previously.

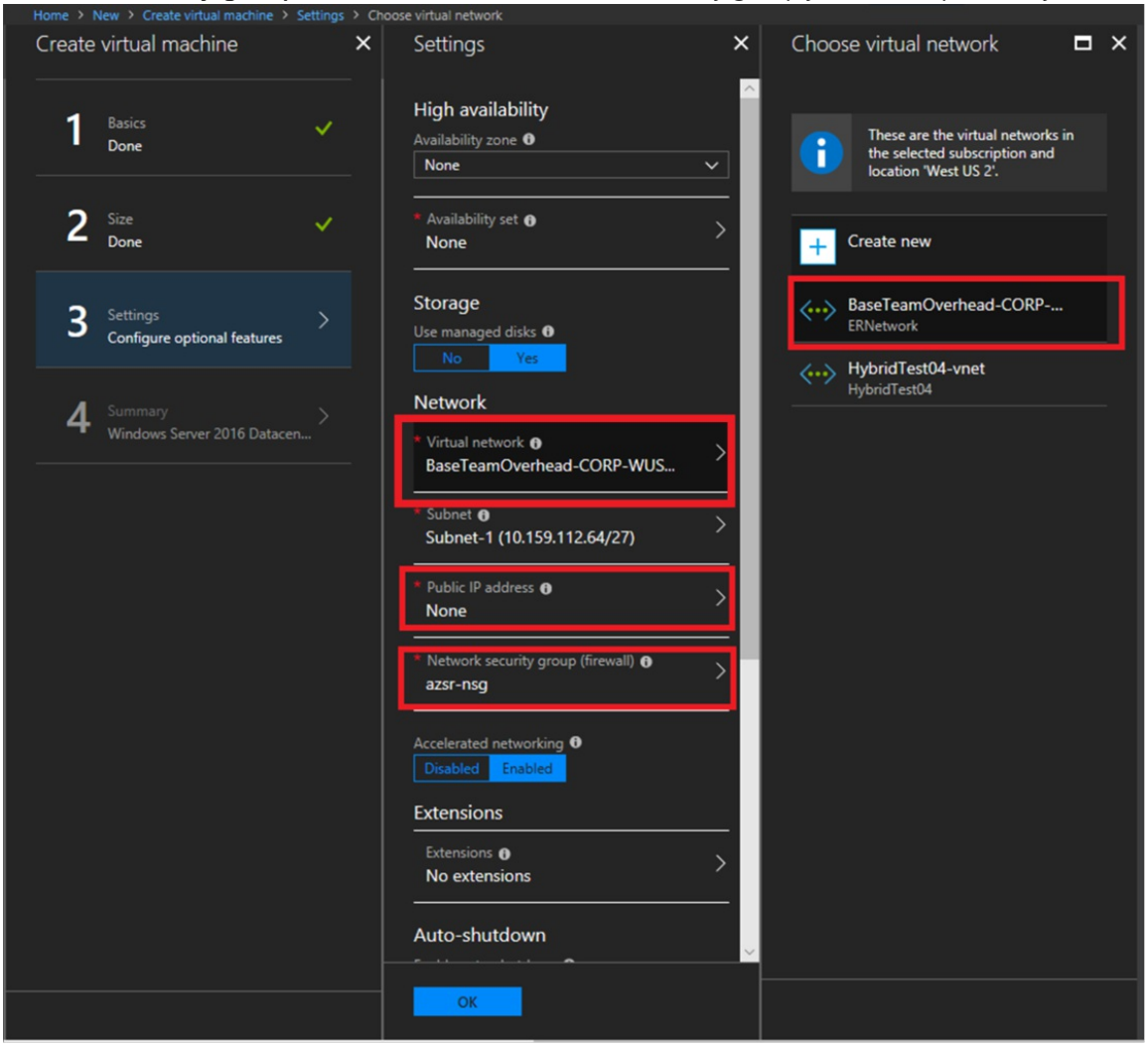



**Figure 5: Creating a VM while selecting ExpressRoute network settings**

5. After the VM is created, see Step 2: Provision operating system, features, roles, storage, and network.

# Related Topics

- Storage Replica Overview
- Stretch Cluster Replication Using Shared Storage
- Cluster to Cluster Storage Replication
- Storage Replica: Known Issues
- Storage Replica: Frequently Asked Questions
- Storage Spaces Direct in Windows Server 2016

# Cluster to cluster Storage Replication

11/2/2020 • 14 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

Storage Replica can replicate volumes between clusters, including the replication of clusters using Storage Spaces Direct. The management and configuration is similar to server-to-server replication.

You will configure these computers and storage in a cluster-to-cluster configuration, where one cluster replicates its own set of storage with another cluster and its set of storage. These nodes and their storage should be located in separate physical sites, although it is not required.

> **IMPORTANT**
>
> In this test, the four servers are an example. You can use any number of servers supported by Microsoft in each cluster, which is currently 8 for a Storage Spaces Direct cluster and 64 for a shared storage cluster.
>
> This guide does not cover configuring Storage Spaces Direct. For information about configuring Storage Spaces Direct, see Storage Spaces Direct overview.

This walkthrough uses the following environment as an example:

- Two member servers, named **SR-SRV01** and **SR-SRV02** that are later formed into a cluster named **SR-SRVCLUSA**.
- Two member servers named **SR-SRV03** and **SR-SRV04** that are later formed into a cluster named **SR-SRVCLUSB**.
- A pair of logical "sites" that represent two different data centers, with one called **Redmond** and one called **Bellevue**.

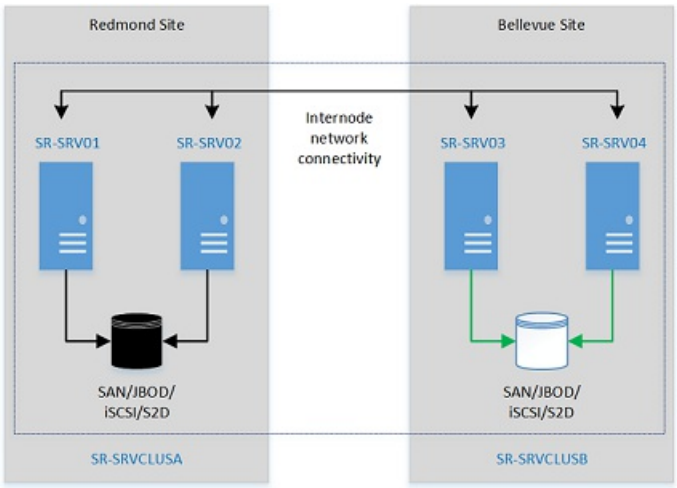



FIGURE 1: Cluster to cluster Replication

## Prerequisites

- Active Directory Domain Services forest (does not need to run Windows Server 2016).
- 4-128 servers (two clusters of 2-64 servers) running Windows Server 2019 or Windows Server 2016, Datacenter Edition. If you're running Windows Server 2019, you can instead use Standard Edition if you're OK

replicating only a single volume up to 2 TB in size.

- Two sets of storage, using SAS JBODs, fibre channel SAN, Shared VHDX, Storage Spaces Direct, or iSCSI target. The storage should contain a mix of HDD and SSD media. You will make each storage set available only to each of the clusters, with no shared access between clusters.
- Each set of storage must allow creation of at least two virtual disks, one for replicated data and one for logs. The physical storage must have the same sector sizes on all the data disks. The physical storage must have the same sector sizes on all the log disks.
- At least one ethernet/TCP connection on each server for synchronous replication, but preferably RDMA.
- Appropriate firewall and router rules to allow ICMP, SMB (port 445, plus 5445 for SMB Direct) and WS-MAN (port 5985) bi-directional traffic between all nodes.
- A network between servers with enough bandwidth to contain your IO write workload and an average of =5ms round trip latency, for synchronous replication. Asynchronous replication does not have a latency recommendation.
- The replicated storage cannot be located on the drive containing the Windows operating system folder.
- There are important considerations & limitations for Storage Spaces Direct replication - please review the detailed information below.

Many of these requirements can be determined by using the `Test-SRTopology` cmdlet. You get access to this tool if you install Storage Replica or the Storage Replica Management Tools features on at least one server. There is no need to configure Storage Replica to use this tool, only to install the cmdlet. More information is included in the steps below.

## Step 1: Provision operating system, features, roles, storage, and network

1. Install Windows Server on all four server nodes with an installation type of Windows Server **(Desktop Experience)**.

2. Add network information and join them to the domain, then restart them.

   > **IMPORTANT**
   > From this point on, always logon as a domain user who is a member of the built-in administrator group on all servers. Always remember to elevate your Windows PowerShell and CMD prompts going forward when running on a graphical server installation or on a Windows 10 computer.

3. Connect first set of JBOD storage enclosure, iSCSI target, FC SAN, or local fixed disk (DAS) storage to the server in site **Redmond**.

4. Connect second set of storage to the server in site **Bellevue**.

5. As appropriate, install latest vendor storage and enclosure firmware and drivers, latest vendor HBA drivers, latest vendor BIOS/UEFI firmware, latest vendor network drivers, and latest motherboard chipset drivers on all four nodes. Restart nodes as needed.

   > **NOTE**
   > Consult your hardware vendor documentation for configuring shared storage and networking hardware.

6. Ensure that BIOS/UEFI settings for servers enable high performance, such as disabling C-State, setting QPI speed, enabling NUMA, and setting highest memory frequency. Ensure power management in Windows Server is set to high performance. Restart as required.

7. Configure roles as follows:

   - **Graphical method**

     a. Run **ServerManager.exe** and create a server group, adding all server nodes.

     b. Install the **File Server** and **Storage Replica** roles and features on each of the nodes and restart them.

   - **Windows PowerShell method**

     On SR-SRV04 or a remote management computer, run the following command in a Windows PowerShell console to install the required features and roles for a stretch cluster on the four nodes and restart them:

     ```
     $Servers = 'SR-SRV01','SR-SRV02','SR-SRV03','SR-SRV04'

     $Servers | ForEach { Install-WindowsFeature -ComputerName $_ -Name Storage-Replica,Failover-Clustering,FS-FileServer -IncludeManagementTools -restart }
     ```

     For more information on these steps, see Install or Uninstall Roles, Role Services, or Features

8. Configure storage as follows:

   **IMPORTANT**

   - You must create two volumes on each enclosure: one for data and one for logs.
   - Log and data disks must be initialized as **GPT**, not **MBR**.
   - The two data volumes must be of identical size.
   - The two log volumes should be of identical size.
   - All replicated data disks must have the same sector sizes.
   - All log disks must have the same sector sizes.
   - The log volumes should use flash-based storage, such as SSD. Microsoft recommends that the log storage be faster than the data storage. Log volumes must never be used for other workloads.
   - The data disks can use HDD, SSD, or a tiered combination and can use either mirrored or parity spaces or RAID 1 or 10, or RAID 5 or RAID 50.
   - The log volume must be at least 8GB by default and may be larger or smaller based on log requirements.
   - When using Storage Spaces Direct (Storage Spaces Direct) with an NVME or SSD cache, you see a greater than expected increase in latency when configuring Storage Replica replication between Storage Spaces Direct clusters. The change in latency is proportionally much higher than you see when using NVME and SSD in a performance + capacity configuration and no HDD tier nor capacity tier.

   This issue occurs due to architectural limitations within SR's log mechanism combined with the extremely low latency of NVME when compared to slower media. When using Storage Spaces Direct Storage Spaces Direct cache, all IO of SR logs, along with all recent read/write IO of applications, will occur in the cache and never on the performance or capacity tiers. This means that all SR activity happens on the same speed media - this configuration is not supported not recommended (see https://aka.ms/srfaq for log recommendations).

   When using Storage Spaces Direct with HDDs, you cannot disable or avoid the cache. As a workaround, if using just SSD and NVME, you can configure just performance and capacity tiers. If using that configuration, and by placing the SR logs on the performance tier only with the data volumes they service being on the capacity tier only, you will avoid the high latency issue described above. The same could be done with a mix of faster and slower SSDs and no NVME.

   This workaround is of course not ideal and some customers may not be able to make use of it. The SR team

is working on optimizations and updated log mechanism for the future to reduce these artificial bottlenecks that occur. There is no ETA for this, but when available to TAP customers for testing, this FAQ will be updated.

- **For JBOD enclosures:**

1. Ensure that each cluster can see that site's storage enclosures only and that the SAS connections are correctly configured.
2. Provision the storage using Storage Spaces by following **Steps 1-3** provided in the Deploy Storage Spaces on a Stand-Alone Server using Windows PowerShell or Server Manager.

- **For iSCSI Target storage:**

1. Ensure that each cluster can see that site's storage enclosures only. You should use more than one single network adapter if using iSCSI.
2. Provision the storage using your vendor documentation. If using Windows-based iSCSI Targeting, consult iSCSI Target Block Storage, How To.

- **For FC SAN storage:**

1. Ensure that each cluster can see that site's storage enclosures only and that you have properly zoned the hosts.
2. Provision the storage using your vendor documentation.

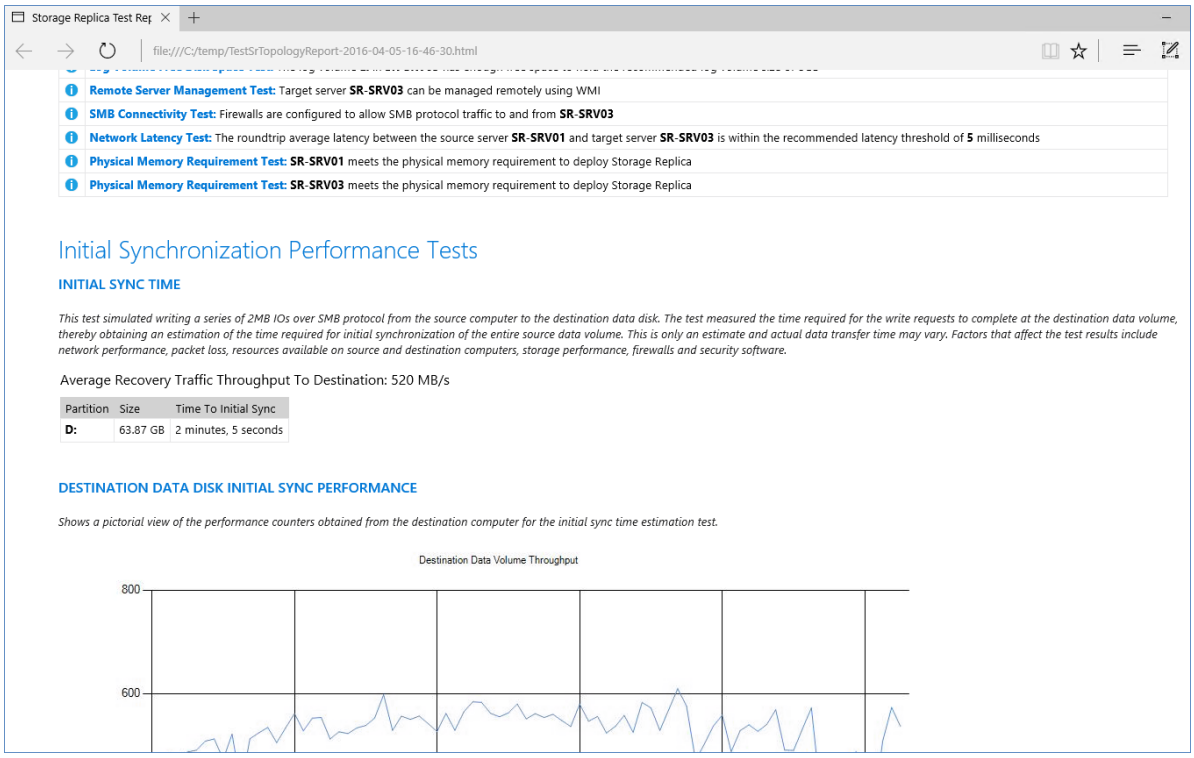
- **For Storage Spaces Direct:**

1. Ensure that each cluster can see that site's storage enclosures only by deploying Storage Spaces Direct. (https://docs.microsoft.com/windows-server/storage/storage-spaces/hyper-converged-solution-using-storage-spaces-direct)
2. Ensure that the SR log volumes will always be on the fastest flash storage and the data volumes on slower high capacity storage.
3. Start Windows PowerShell and use the `Test-SRTopology` cmdlet to determine if you meet all the Storage Replica requirements. You can use the cmdlet in a requirements-only mode for a quick test as well as a long running performance evaluation mode. For example,

```
MD c:\temp

Test-SRTopology -SourceComputerName SR-SRV01 -SourceVolumeName f: -SourceLogVolumeName g: -
DestinationComputerName SR-SRV03 -DestinationVolumeName f: -DestinationLogVolumeName g: -
DurationInMinutes 30 -ResultPath c:\temp
```

> **IMPORTANT**
> When using a test server with no write IO load on the specified source volume during the evaluation period, consider adding a workload or it will not generate a useful report. You should test with production-like workloads in order to see real numbers and recommended log sizes. Alternatively, simply copy some files into the source volume during the test or download and run DISKSPD to generate write IOs. For instance, a sample with a low write IO workload for five minutes to the D: volume:
> `Diskspd.exe -c1g -d300 -W5 -C5 -b8k -t2 -o2 -r -w5 -h d:\test.dat`

4. Examine the **TestSrTopologyReport.html** report to ensure that you meet the Storage Replica requirements.




# Step 2: Configure two Scale-Out File Server Failover Clusters

You will now create two normal failover clusters. After configuration, validation, and testing, you will replicate them using Storage Replica. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

### Graphical method

1. Run **cluadmin.msc** against a node in each site.
2. Validate the proposed cluster and analyze the results to ensure you can continue. The example used below are **SR-SRVCLUSA** and **SR-SRVCLUSB**.
3. Create the two clusters. Ensure that the cluster names are 15 characters or fewer.
4. Configure a File Share Witness or Cloud Witness.

> **NOTE**
>
> WIndows Server now includes an option for Cloud (Azure)-based Witness. You can choose this quorum option instead of the file share witness.

> **WARNING**
>
> For more information about quorum configuration, see the **Witness Configuration** section in Configure and Manage Quorum. For more information on the `Set-ClusterQuorum` cmdlet, see Set-ClusterQuorum.

5. Add one disk in the **Redmond** site to the cluster CSV. To do so, right click a source disk in the **Disks** node of the **Storage** section, and then click **Add to Cluster Shared Volumes**.
6. Create the clustered Scale-Out File Servers on both clusters using the instructions in Configure Scale-Out File Server

### Windows PowerShell method

1. Test the proposed cluster and analyze the results to ensure you can continue:

```
Test-Cluster SR-SRV01,SR-SRV02
Test-Cluster SR-SRV03,SR-SRV04
```

2. Create the clusters (you must specify your own static IP addresses for the clusters). Ensure that each cluster name is 15 characters or fewer:

```
New-Cluster -Name SR-SRVCLUSA -Node SR-SRV01,SR-SRV02 -StaticAddress <your IP here>
New-Cluster -Name SR-SRVCLUSB -Node SR-SRV03,SR-SRV04 -StaticAddress <your IP here>
```

3. Configure a File Share Witness or Cloud (Azure) witness in each cluster that points to a share hosted on the domain controller or some other independent server. For example:

```
Set-ClusterQuorum -FileShareWitness \\someserver\someshare
```

> **NOTE**
> WIndows Server now includes an option for Cloud (Azure)-based Witness. You can choose this quorum option instead of the file share witness.

> **WARNING**
> For more information about quorum configuration, see the **Witness Configuration** section in Configure and Manage Quorum. For more information on the `Set-ClusterQuorum` cmdlet, see Set-ClusterQuorum.

4. Create the clustered Scale-Out File Servers on both clusters using the instructions in Configure Scale-Out File Server

## Step 3: Set up Cluster to Cluster Replication using Windows PowerShell

Now you will set up cluster-to-cluster replication using Windows PowerShell. You can perform all of the steps below on the nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools

1. Grant the first cluster full access to the other cluster by running the **Grant-SRAccess** cmdlet on any node in the first cluster, or remotely. Windows Server Remote Server Administration Tools

```
Grant-SRAccess -ComputerName SR-SRV01 -Cluster SR-SRVCLUSB
```

2. Grant the second cluster full access to the other cluster by running the **Grant-SRAccess** cmdlet on any node in the second cluster, or remotely.

```
Grant-SRAccess -ComputerName SR-SRV03 -Cluster SR-SRVCLUSA
```

3. Configure the cluster-to-cluster replication, specifying the source and destination disks, the source and destination logs, the source and destination cluster names, and the log size. You can perform this command locally on the server or using a remote management computer.

```
New-SRPartnership -SourceComputerName SR-SRVCLUSA -SourceRGName rg01 -SourceVolumeName
c:\ClusterStorage\Volume2 -SourceLogVolumeName f: -DestinationComputerName SR-SRVCLUSB -
DestinationRGName rg02 -DestinationVolumeName c:\ClusterStorage\Volume2 -DestinationLogVolumeName f:
```

**WARNING**

The default log size is 8GB. Depending on the results of the **Test-SRTopology** cmdlet, you may decide to use -**LogSizeInBytes** with a higher or lower value.

4. To get replication source and destination state, use **Get-SRGroup** and **Get-SRPartnership** as follows:

```
Get-SRGroup
Get-SRPartnership
(Get-SRGroup).replicas
```

5. Determine the replication progress as follows:

   a. On the source server, run the following command and examine events 5015, 5002, 5004, 1237, 5001, and 2200:

   ```
   Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica -max 20
   ```

   b. On the destination server, run the following command to see the Storage Replica events that show creation of the partnership. This event states the number of copied bytes and the time taken. Example:

   ```
   Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | Where-Object {$_.ID -eq "1215"} |
   Format-List
   ```

   Here's an example of the output:

   ```
   TimeCreated  : 4/8/2016 4:12:37 PM
   ProviderName : Microsoft-Windows-StorageReplica
   Id           : 1215
   Message      : Block copy completed for replica.
       ReplicationGroupName: rg02
       ReplicationGroupId:
       {616F1E00-5A68-4447-830F-B0B0EFBD359C}
       ReplicaName: f:\
       ReplicaId: {00000000-0000-0000-0000-000000000000}
       End LSN in bitmap:
       LogGeneration: {00000000-0000-0000-0000-000000000000}
       LogFileId: 0
       CLSFLsn: 0xFFFFFFFF
       Number of Bytes Recovered: 68583161856
       Elapsed Time (seconds): 117
   ```

   c. Alternately, the destination server group for the replica states the number of byte remaining to copy at all times, and can be queried through PowerShell. For example:

   ```
   (Get-SRGroup).Replicas | Select-Object numofbytesremaining
   ```

   As a progress sample (that will not terminate):

```
while($true) {
$v = (Get-SRGroup -Name "Replication 2").replicas | Select-Object numofbytesremaining
[System.Console]::Write("Number of bytes remaining: {0}`n", $v.numofbytesremaining)
Start-Sleep -s 5
}
```

6. On the destination server in the destination cluster, run the following command and examine events 5009, 1237, 5001, 5015, 5005, and 2200 to understand the processing progress. There should be no warnings of errors in this sequence. There will be many 1237 events; these indicate progress.

```
Get-WinEvent -ProviderName Microsoft-Windows-StorageReplica | FL
```

> **NOTE**
> The destination cluster disk will always show as **Online (No Access)** when replicated.

## Step 4: Manage replication

Now you will manage and operate your cluster-to-cluster replication. You can perform all of the steps below on the cluster nodes directly or from a remote management computer that contains the Windows Server Remote Server Administration Tools.

1. Use **Get-ClusterGroup** or **Failover Cluster Manager** to determine the current source and destination of replication and their status. Windows Server Remote Server Administration Tools
2. To measure replication performance, use the **Get-Counter** cmdlet on both the source and destination nodes. The counter names are:
   - \Storage Replica Partition I/O Statistics(*)\Number of times flush paused
   - \Storage Replica Partition I/O Statistics(*)\Number of pending flush I/O
   - \Storage Replica Partition I/O Statistics(*)\Number of requests for last log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Current Flush Queue Length
   - \Storage Replica Partition I/O Statistics(*)\Number of Application Write Requests
   - \Storage Replica Partition I/O Statistics(*)\Avg. Number of requests per log write
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Write Latency
   - \Storage Replica Partition I/O Statistics(*)\Avg. App Read Latency
   - \Storage Replica Statistics(*)\Target RPO
   - \Storage Replica Statistics(*)\Current RPO
   - \Storage Replica Statistics(*)\Avg. Log Queue Length
   - \Storage Replica Statistics(*)\Current Log Queue Length
   - \Storage Replica Statistics(*)\Total Bytes Received
   - \Storage Replica Statistics(*)\Total Bytes Sent
   - \Storage Replica Statistics(*)\Avg. Network Send Latency

- \Storage Replica Statistics(*)\Replication State
- \Storage Replica Statistics(*)\Avg. Message Round Trip Latency
- \Storage Replica Statistics(*)\Last Recovery Elapsed Time
- \Storage Replica Statistics(*)\Number of Flushed Recovery Transactions
- \Storage Replica Statistics(*)\Number of Recovery Transactions
- \Storage Replica Statistics(*)\Number of Flushed Replication Transactions
- \Storage Replica Statistics(*)\Number of Replication Transactions
- \Storage Replica Statistics(*)\Max Log Sequence Number
- \Storage Replica Statistics(*)\Number of Messages Received
- \Storage Replica Statistics(*)\Number of Messages Sent

For more information on performance counters in Windows PowerShell, see Get-Counter.

3. To move the replication direction from one site, use the **Set-SRPartnership** cmdlet.

```
Set-SRPartnership -NewSourceComputerName SR-SRVCLUSB -SourceRGName rg02 -DestinationComputerName SR-SRVCLUSA -DestinationRGName rg01
```

> **NOTE**
> Windows Server prevents role switching when initial sync is ongoing, as it can lead to data loss if you attempt to switch before allowing initial replication to complete. Do not force switch directions until initial sync is complete.

Check the event logs to see the direction of replication change and recovery mode occur, and then reconcile. Write IOs can then write to the storage owned by the new source server. Changing the replication direction will block write IOs on the previous source computer.

> **NOTE**
> The destination cluster disk will always show as **Online (No Access)** when replicated.

4. To change the log size from the default 8GB, use **Set-SRGroup** on both the source and destination Storage Replica groups.

> **IMPORTANT**
> The default log size is 8GB. Depending on the results of the **Test-SRTopology** cmdlet, you may decide to use -LogSizeInBytes with a higher or lower value.

5. To remove replication, use **Get-SRGroup**, **Get-SRPartnership**, **Remove-SRGroup**, and **Remove-SRPartnership** on each cluster.

```
Get-SRPartnership | Remove-SRPartnership
Get-SRGroup | Remove-SRGroup
```

> **NOTE**
>
> Storage Replica dismounts the destination volumes. This is by design.

## Additional References

- Storage Replica Overview
- Stretch Cluster Replication Using Shared Storage
- Server to Server Storage Replication
- Storage Replica: Known Issues
- Storage Replica: Frequently Asked Questions
- Storage Spaces Direct in Windows Server 2016

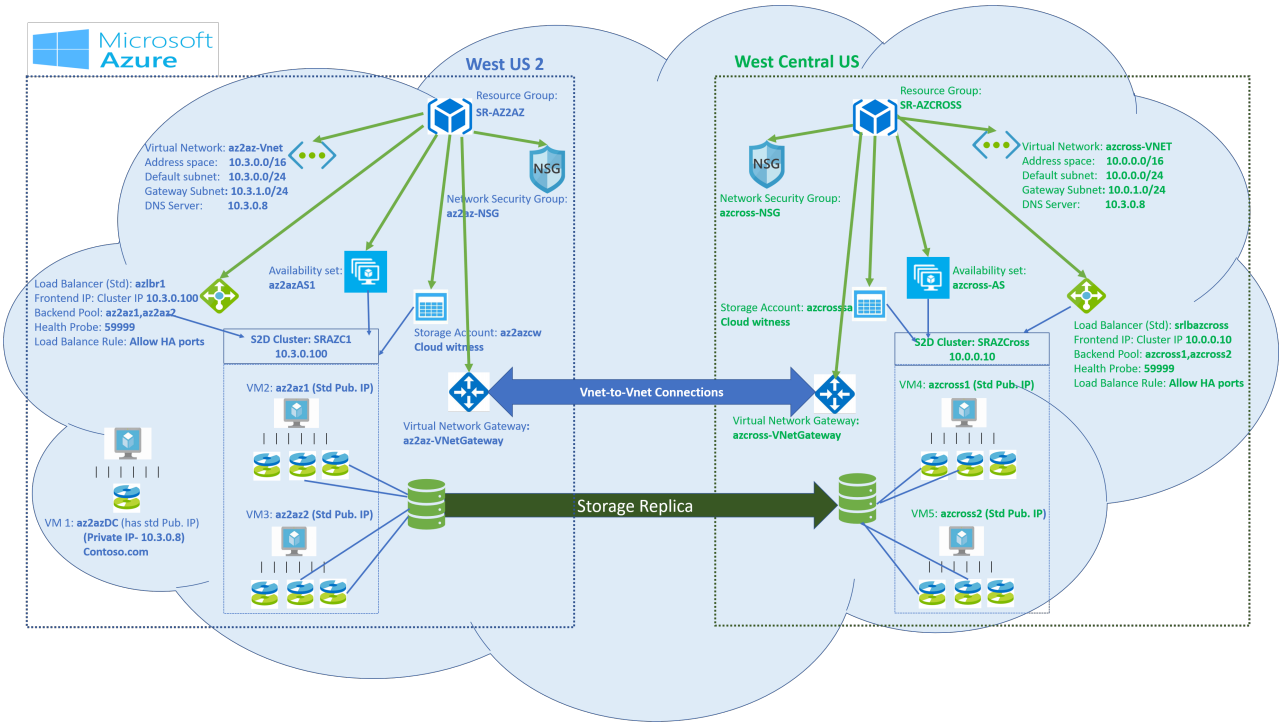
# Cluster to Cluster Storage Replica cross region in Azure

12/16/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

You can configure Cluster to Cluster Storage Replicas for cross-region applications in Azure. In the examples below, we use a two-node cluster, but Cluster to Cluster storage replica isn't restricted to a two-node cluster. The illustration below is a two-node Storage Space Direct cluster that can communicate with each other, are in the same domain, and are cross-region.

Watch the video below for a complete walk-through of the process.




**IMPORTANT**

All referenced examples are specific to the illustration above.

1. In the Azure portal, create resource groups in two different regions.

   For example, **SR-AZ2AZ** in **West US 2** and **SR-AZCROSS** in **West Central US**, as shown above.

2. Create two availability sets, one in each resource group for each cluster.

   - Availability set (**az2azAS1**) in (**SR-AZ2AZ**)
   - Availability set (**azcross-AS**) in (**SR-AZCROSS**)

3. Create two virtual networks

   - Create the virtual network (**az2az-Vnet**) in the first resource group (**SR-AZ2AZ**), having one subnet and one Gateway subnet.

- Create the virtual network (**azcross-VNET**) in the second resource group (**SR-AZCROSS**), having one subnet and one Gateway subnet.

4. Create two network security groups

   - Create the network security group (**az2az-NSG**) in the first resource group (**SR-AZ2AZ**).
   - Create the network security group (**azcross-NSG**) in the second resource group (**SR-AZCROSS**).

   Add one Inbound security rule for RDP:3389 to both Network Security Groups. You can choose to remove this rule once you finish your setup.

5. Create Windows Server virtual machines in the previously created resource groups.

   Domain Controller (**az2azDC**). You can choose to create a 3rd availability set for your domain controller or add the domain controller in one of the two availability set. If you are adding this to the availability set created for the two clusters, assign it a Standard public IP address during VM creation.

   - Install Active Directory Domain Service.
   - Create a domain (contoso.com)
   - Create a user with administrator privileges (contosoadmin)

   Create two virtual machines (**az2az1**, **az2az2**) in the resource group (**SR-AZ2AZ**) using virtual network (**az2az-Vnet**) and network security group (**az2az-NSG**) in availability set (**az2azAS1**). Assign a standard public IP address to each virtual machine during the creation itself.

   - Add at-least two managed disks to each machine
   - Install Failover Clustering and the Storage Replica feature

   Create two virtual machines (**azcross1**, **azcross2**) in the resource group (**SR-AZCROSS**) using virtual network (**azcross-VNET**) and network security group (**azcross-NSG**) in availability set (**azcross-AS**). Assign standard Public IP address to each virtual machine during the creation itself

   - Add at least two managed disks to each machine
   - Install Failover Clustering and the Storage Replica feature

   Connect all the nodes to the domain and provide administrator privileges to the previously created user.

   Change the DNS Server of the virtual network to domain controller private IP address.

   - In the example, the domain controller **az2azDC** has private IP address (10.3.0.8). In the Virtual Network (**az2az-Vnet** and **azcross-VNET**) change DNS Server 10.3.0.8.

     In the example, connect all the nodes to "contoso.com" and provide administrator privileges to "contosoadmin".

   - Login as contosoadmin from all the nodes.

6. Create the clusters (**SRAZC1**, **SRAZCross**).

   Below is the PowerShell commands for the example

   ```
   New-Cluster -Name SRAZC1 -Node az2az1,az2az2 –StaticAddress 10.3.0.100
   ```

   ```
   New-Cluster -Name SRAZCross -Node azcross1,azcross2 –StaticAddress 10.0.0.10
   ```

7. Enable storage spaces direct.

   ```
   Enable-clusterS2D
   ```

> **NOTE**
> For each cluster create virtual disk and volume. One for the data and another for the log.

8. Create an internal Standard SKU Load Balancer for each cluster (**azlbr1**, **azlbazcross**).

   Provide the Cluster IP address as static private IP address for the load balancer.

   - azlbr1 => Frontend IP: 10.3.0.100 (Pick up an unused IP address from the Virtual network (**az2az-Vnet**) subnet)
   - Create Backend Pool for each load balancer. Add the associated cluster nodes.
   - Create Health Probe: port 59999
   - Create Load Balance Rule: Allow HA ports, with enabled Floating IP.

   Provide the Cluster IP address as static private IP address for the load balancer.

   - azlbazcross => Frontend IP: 10.0.0.10 (Pick up an unused IP address from the Virtual network (**azcross-VNET**) subnet)
   - Create Backend Pool for each load balancer. Add the associated cluster nodes.
   - Create Health Probe: port 59999
   - Create Load Balance Rule: Allow HA ports, with enabled Floating IP.

9. Create Virtual network gateway for Vnet-to-Vnet connectivity.

   - Create the first virtual network gateway (**az2az-VNetGateway**) in the first resource group (**SR-AZ2AZ**)
   - Gateway Type = VPN, and VPN type = Route-based
   - Create the second Virtual network gateway (**azcross-VNetGateway**) in the second resource group (**SR-AZCROSS**)
   - Gateway Type = VPN, and VPN type = Route-based
   - Create a Vnet-to-Vnet connection from first Virtual network gateway to second Virtual network gateway. Provide a shared key
   - Create a Vnet-to-Vnet connection from second Virtual network gateway to first Virtual network gateway. Provide the same shared key as provided in the step above.

10. On each cluster node, open port 59999 (Health Probe).

    Run the following command on each node:

    ```
      netsh advfirewall firewall add rule name=PROBEPORT dir=in protocol=tcp action=allow localport=59999
    remoteip=any profile=any
    ```

11. Instruct the cluster to listen for Health Probe messages on Port 59999 and respond from the node that currently owns this resource.

    Run it once from any one node of the cluster, for each cluster.

    In our example, make sure to change the "ILBIP" according to your configuration values. Run the following command from any one node **az2az1/az2az2**

```
 $ClusterNetworkName = "Cluster Network 1" # Cluster network name (Use Get-ClusterNetwork on Windows
Server 2012 or higher to find the name. And use Get-ClusterResource to find the IPResourceName).
 $IPResourceName = "Cluster IP Address" # IP Address cluster resource name.
 $ILBIP = "10.3.0.100" # IP Address in Internal Load Balancer (ILB) - The static IP address for the load
balancer configured in the Azure portal.
 [int]$ProbePort = 59999
 Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{"Address"="$ILBIP";"ProbePort"=$ProbePort;"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkNam
e";"ProbeFailureThreshold"=5;"EnableDhcp"=0}
```

12. Run the following command from any one node **azcross1**/**azcross2**

```
 $ClusterNetworkName = "Cluster Network 1" # Cluster network name (Use Get-ClusterNetwork on Windows
Server 2012 or higher to find the name. And use Get-ClusterResource to find the IPResourceName).
 $IPResourceName = "Cluster IP Address" # IP Address cluster resource name.
 $ILBIP = "10.0.0.10" # IP Address in Internal Load Balancer (ILB) - The static IP address for the load
balancer configured in the Azure portal.
 [int]$ProbePort = 59999
 Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{"Address"="$ILBIP";"ProbePort"=$ProbePort;"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkNam
e";"ProbeFailureThreshold"=5;"EnableDhcp"=0}
```

    Make sure both clusters can connect / communicate with each other.

    Either use "Connect to Cluster" feature in Failover cluster manager to connect to the other cluster or check other cluster responds from one of the nodes of the current cluster.

    From the example we've been using:

```
  Get-Cluster -Name SRAZC1 (ran from azcross1)
```

```
  Get-Cluster -Name SRAZCross (ran from az2az1)
```

13. Create cloud witness for both clusters. Create two storage accounts (**az2azcw**,**azcrosssa**) in Azure, one for each cluster in each resource group (**SR-AZ2AZ**, **SR-AZCROSS**).

    - Copy the storage account name and key from "access keys"
    - Create the cloud witness from "failover cluster manager" and use the above account name and key to create it.

14. Run cluster validation tests before moving on to the next step

15. Start Windows PowerShell and use the Test-SRTopology cmdlet to determine if you meet all the Storage Replica requirements. You can use the cmdlet in a requirements-only mode for a quick test as well as a long running performance evaluation mode.

16. Configure cluster-to-cluster storage replica. Grant access from one cluster to another cluster in both directions:

    From our example:

```
  Grant-SRAccess -ComputerName az2az1 -Cluster SRAZCross
```

    If you're using Windows Server 2016, then also run this command:

```
Grant-SRAccess -ComputerName azcross1 -Cluster SRAZC1
```

17. Create SR-Partnership for the two clusters:

- For cluster **SRAZC1**
  - Volume location:- c:\ClusterStorage\DataDisk1
  - Log location:- g:
- For cluster **SRAZCross**
  - Volume location:- c:\ClusterStorage\DataDiskCross
  - Log location:- g:

Run the command:

```
PowerShell

New-SRPartnership -SourceComputerName SRAZC1 -SourceRGName rg01 -SourceVolumeName c:\ClusterStorage\DataDisk1 -
SourceLogVolumeName  g: -DestinationComputerName SRAZCross -DestinationRGName rg02 -DestinationVolumeName
c:\ClusterStorage\DataDiskCross -DestinationLogVolumeName  g:
```

# Cluster to cluster Storage Replica within the same region in Azure

12/16/2020 • 5 minutes to read • Edit Online

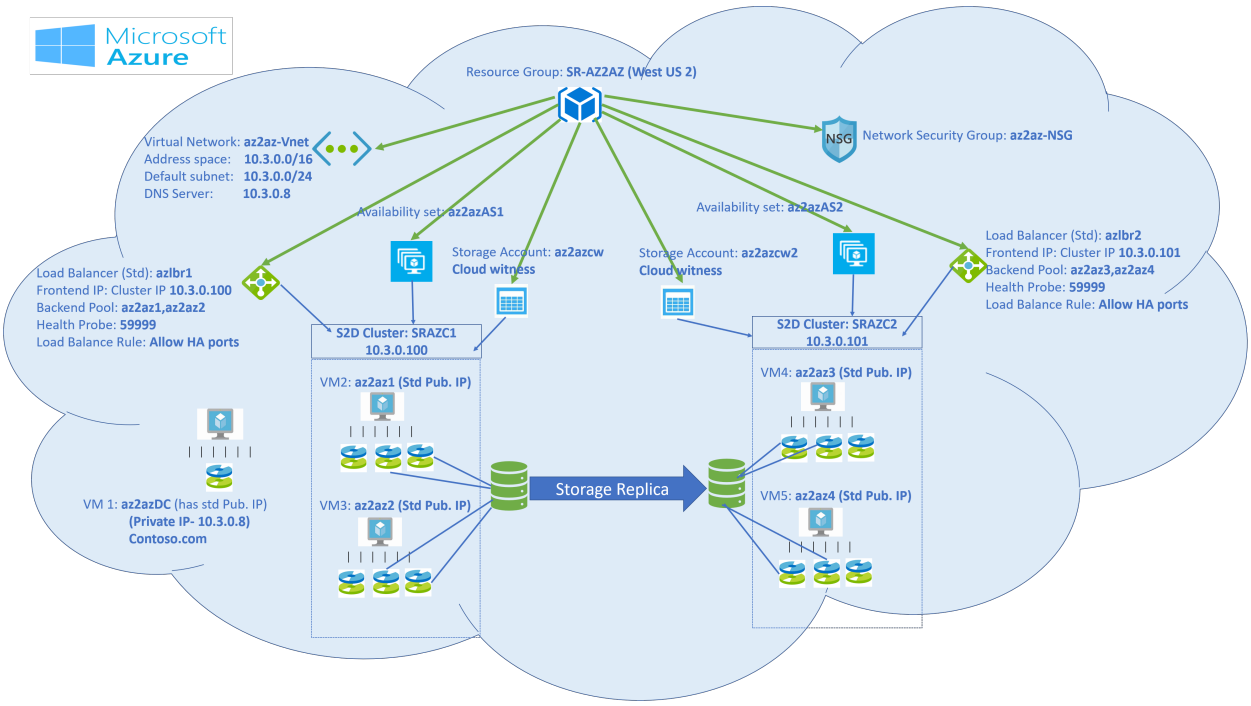
Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

You can configure cluster to cluster storage replication within the same region in Azure. In the examples below, we use a two-node cluster, but cluster to cluster storage replica isn't restricted to a two-node cluster. The illustration below is a two-node Storage Space Direct cluster that can communicate with each other, are in the same domain, and within the same region.

Watch the videos below for a complete walk-through of the process.

Part one

Part two




**IMPORTANT**

All referenced examples are specific to the illustration above.

1. Create a resource group in the Azure portal in a region (**SR-AZ2AZ** in **West US 2**).
2. Create two availability sets in the resource group (**SR-AZ2AZ**) created above, one for each cluster. a. Availability set (**az2azAS1**) b. Availability set (**az2azAS2**)
3. Create a virtual network (**az2az-Vnet**) in the previously created resource group (**SR-AZ2AZ**), having at-least one subnet.

4. Create a network security group (**az2az-NSG**), and add one Inbound security rule for RDP:3389. You can choose to remove this rule once you finish your setup.

5. Create Windows Server virtual machines in the previously created Resource group (**SR-AZ2AZ**). Use the previously created virtual network (**az2az-Vnet**) and network security group (**az2az-NSG**).

   Domain Controller (**az2azDC**). You can choose to create a third availability set for your domain controller or add the domain controller in one of the two availability sets. If you are adding this to the availability set created for the two clusters, assign it a Standard public IP address during VM creation.

   - Install Active Directory Domain Service.
   - Create a domain (Contoso.com)
   - Create a user with administrator privileges (contosoadmin)
   - Create two virtual machines (**az2az1**, **az2az2**) in the first availability set (**az2azAS1**). Assign a standard Public IP address to each virtual machine during the creation itself.
   - Add at-least 2 managed disks to each machine
   - Install Failover Clustering and Storage Replica feature
   - Create two virtual machines (**az2az3**, **az2az4**) in the second availability set (**az2azAS2**). Assign standard Public IP address to each virtual machine during the creation itself.
   - Add at-least 2 managed disks to each machine.
   - Install Failover Clustering and Storage Replica feature.
6. Connect all the nodes to the domain and provide Administrator privileges to the previously created user.

7. Change the DNS Server of the virtual network to domain controller private IP address.

8. In our example, the domain controller **az2azDC** has private IP address (10.3.0.8). In the Virtual Network (**az2az-Vnet**) change DNS Server 10.3.0.8. Connect all the nodes to "Contoso.com" and provide administrator privileges to "contosoadmin".

   - Login as contosoadmin from all the nodes.
9. Create the clusters (**SRAZC1**, **SRAZC2**). Below is the PowerShell commands for our example

   ```
   New-Cluster -Name SRAZC1 -Node az2az1,az2az2 –StaticAddress 10.3.0.100
   ```

   ```
   New-Cluster -Name SRAZC2 -Node az2az3,az2az4 –StaticAddress 10.3.0.101
   ```

10. Enable storage spaces direct

    ```
    Enable-clusterS2D
    ```

    For each cluster create virtual disk and volume. One for the data and another for the log.

11. Create an internal Standard SKU Load Balancer for each cluster (**azlbr1**,**azlbr2**).

    Provide the Cluster IP address as static private IP address for the load balancer.

    - azlbr1 => Frontend IP: 10.3.0.100 (Pick up an unused IP address from the Virtual network (**az2az-Vnet**) subnet)
    - Create Backend Pool for each load balancer. Add the associated cluster nodes.
    - Create Health Probe: port 59999
    - Create Load Balance Rule: Allow HA ports, with enabled Floating IP.

    Provide the Cluster IP address as static private IP address for the load balancer.

- azlbr2 => Frontend IP: 10.3.0.101 (Pick up an unused IP address from the Virtual network (**az2az-Vnet**) subnet)
- Create Backend Pool for each load balancer. Add the associated cluster nodes.
- Create Health Probe: port 59999
- Create Load Balance Rule: Allow HA ports, with enabled Floating IP.

12. On each cluster node, open port 59999 (Health Probe).

    Run the following command on each node:

    ```
    netsh advfirewall firewall add rule name=PROBEPORT dir=in protocol=tcp action=allow localport=59999
    remoteip=any profile=any
    ```

13. Instruct the cluster to listen for Health Probe messages on Port 59999 and respond from the node that currently owns this resource. Run it once from any one node of the cluster, for each cluster.

    In our example, make sure to change the "ILBIP" according to your configuration values. Run the following command from any one node **az2az1/az2az2**:

    ```
     $ClusterNetworkName = "Cluster Network 1" # Cluster network name (Use Get-ClusterNetwork on Windows
    Server 2012 or higher to find the name. And use Get-ClusterResource to find the IPResourceName).
     $IPResourceName = "Cluster IP Address" # IP Address cluster resource name.
     $ILBIP = "10.3.0.100" # IP Address in Internal Load Balancer (ILB) - The static IP address for the load
    balancer configured in the Azure portal.
     [int]$ProbePort = 59999
     Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
    @{"Address"="$ILBIP";"ProbePort"=$ProbePort;"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkNam
    e";"ProbeFailureThreshold"=5;"EnableDhcp"=0}
    ```

14. Run the following command from any one node **az2az3/az2az4**.

    ```
    $ClusterNetworkName = "Cluster Network 1" # Cluster network name (Use Get-ClusterNetwork on Windows
    Server 2012 or higher to find the name. And use Get-ClusterResource to find the IPResourceName).
    $IPResourceName = "Cluster IP Address" # IP Address cluster resource name.
    $ILBIP = "10.3.0.101" # IP Address in Internal Load Balancer (ILB) - The static IP address for the load
    balancer configured in the Azure portal.
    [int]$ProbePort = 59999
    Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
    @{"Address"="$ILBIP";"ProbePort"=$ProbePort;"SubnetMask"="255.255.255.255";"Network"="$ClusterNetworkNam
    e";"ProbeFailureThreshold"=5;"EnableDhcp"=0}
    ```

    Make sure both clusters can connect / communicate with each other.

    Either use "Connect to Cluster" feature in Failover cluster manager to connect to the other cluster or check other cluster responds from one of the nodes of the current cluster.

    ```
     Get-Cluster -Name SRAZC1 (ran from az2az3)
    ```

    ```
     Get-Cluster -Name SRAZC2 (ran from az2az1)
    ```

15. Create cloud witnesses for both clusters. Create two storage accounts (**az2azcw**, **az2azcw2**) in azure one for each cluster in the same resource group (**SR-AZ2AZ**).

    - Copy the storage account name and key from "access keys"
    - Create the cloud witness from "failover cluster manager" and use the above account name and key to create it.

16. Run cluster validation tests before moving on to the next step.

17. Start Windows PowerShell and use the Test-SRTopology cmdlet to determine if you meet all the Storage Replica requirements. You can use the cmdlet in a requirements-only mode for a quick test as well as a long-running performance evaluation mode.

18. Configure cluster-to-cluster Storage Replica.

    Grant access from one cluster to another cluster in both directions:

    In our example:

    ```
    Grant-SRAccess -ComputerName az2az1 -Cluster SRAZC2
    ```

    If you're using Windows Server 2016 then also run this command:

    ```
    Grant-SRAccess -ComputerName az2az3 -Cluster SRAZC1
    ```

19. Create SRPartnership for the clusters:

- For cluster **SRAZC1**.
- Volume location:- c:\ClusterStorage\DataDisk1
- Log location:- g:
- For cluster **SRAZC2**
- Volume location:- c:\ClusterStorage\DataDisk2
- Log location:- g:

Run the following command:

```
New-SRPartnership -SourceComputerName SRAZC1 -SourceRGName rg01 -SourceVolumeName c:\ClusterStorage\DataDisk1 -
SourceLogVolumeName  g: -DestinationComputerName **SRAZC2** -DestinationRGName rg02 -DestinationVolumeName
c:\ClusterStorage\DataDisk2 -DestinationLogVolumeName  g:
```

# Known issues with Storage Replica

12/16/2020 • 19 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

This topic discusses known issues with Storage Replica in Windows Server.

## After removing replication, disks are offline and you cannot configure replication again

In Windows Server 2016, you may be unable to provision replication on a volume that was previously replicated or may find un-mountable volumes. This may occur when some error condition prevents removal of replication or when you reinstall the operating system on a computer that was previously replicating data.

To fix, you must clear the hidden Storage Replica partition off the disks and return them to a writeable state using the `Clear-SRMetadata` cmdlet.

- To remove all orphaned Storage Replica partition databases slots and remount all partitions, use the `-AllPartitions` parameter as follows:

```
Clear-SRMetadata -AllPartitions
```

- To remove all orphaned Storage Replica log data, use the `-AllLogs` parameter as follows:

```
Clear-SRMetadata -AllLogs
```

- To remove all orphaned failover cluster configuration data, use the `-AllConfiguration` parameter as follows:

```
Clear-SRMetadata -AllConfiguration
```

- To remove individual replication group metadata, use the `-Name` parameter and specify a replication group as follows:

```
Clear-SRMetadata -Name RG01 -Logs -Partition
```

The server may need to restart after cleaning the partition database; you can suppress this temporarily with `-NoRestart` but you should not skip restarting the server if requested by the cmdlet. This cmdlet does not remove data volumes nor data contained within those volumes.

## During initial sync, see event log 4004 warnings

In Windows Server 2016, when configuring replication, both the source and destination servers may show multiple **StorageReplica\Admin*- event log 4004 warnings each during initial sync, with a status of "insufficient system resources exist to complete the API". You are likely to see 5014 errors as well. These indicate that the servers do not have enough available memory (RAM) to perform both initial synchronization as well as run workloads. Either add RAM or reduce the used RAM from features and applications other than Storage Replica.

## When using guest clusters with Shared VHDX and a host without a CSV, virtual machines stop responding after configuring replication

In Windows Server 2016, when using Hyper-V guest clusters for Storage Replica testing or demonstration purposes, and using Shared VHDX as the guest cluster storage, the virtual machines stop responding after you configure replication. If you restart the Hyper-V host, the virtual machines start responding but replication configuration will not be complete and no replication will occur.

This behavior occurs when you are using **fltmc.exe attach svhdxflt*- to bypass the requirement for the Hyper-V host running a CSV. Use of this command is not supported and is intended only for test and demonstration purposes.

The cause of the slowdown is a by-design interoperability issue between the Storage QoS feature in Windows Server 2016 and the manually attached Shared VHDX filter. To resolve this issue, disable the Storage QoS filter driver and restart the Hyper-V host:

```
SC config storqosflt start= disabled
```

## Cannot configure replication when using New-Volume and differing storage

When using the `New-Volume` cmdlet along with differing sets of storage on the source and destination server, such as two different SANs or two JBODs with differing disks, you may not be able to subsequently configure replication using `New-SRPartnership`. The error shown may include:

```
Data partition sizes are different in those two groups
```

Use the `New-Partition**` cmdlet to create volumes and format them instead of `New-Volume`, as the latter cmdlet may round the volume size on differing storage arrays. If you have already created an NTFS volume, you can use `Resize-Partition` to grow or shrink one of the volumes to match the other (this cannot be done with ReFS volumes). If using **Diskmgmt*- or **Server Manager**, no rounding will occur.

## Running Test-SRTopology fails with name-related errors

When attempting to use `Test-SRTopology`, you receive one of the following errors:

ERROR EXAMPLE 1:

```
WARNING: Invalid value entered for target computer name: sr-srv03. Test-SrTopology cmdlet does not accept IP
address as input for target computer name parameter. NetBIOS names and fully qualified domain names are
acceptable inputs
WARNING: System.Exception
WARNING: at Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand.BeginProcessing()
Test-SRTopology : Invalid value entered for target computer name: sr-srv03. Test-SrTopology cmdlet does not
accept IP address as input for target computer name parameter. NetBIOS names and fully qualified domain
names are acceptable inputs
At line:1 char:1
+ Test-SRTopology -SourceComputerName sr-srv01 -SourceVolumeName d: -So ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Test-SRTopology], Exception
+ FullyQualifiedErrorId : TestSRTopologyFailure,Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand
```

ERROR EXAMPLE 2:

```
WARNING: Invalid value entered for source computer name
```

ERROR EXAMPLE 3:

```
The specified volume cannot be found G: cannot be found on computer SRCLUSTERNODE1
```

This cmdlet has limited error reporting in Windows Server 2016 and will return the same output for many common issues. The error can appear for the following reasons:

- You are logged on to the source computer as a local user, not a domain user.
- The destination computer is not running or is not accessible over the network.
- You specified an incorrect name for the destination computer.
- You specified an IP address for the destination server.
- The destination computer firewall is blocking access to PowerShell and/or CIM calls.
- The destination computer is not running the WMI service.
- You did not use CREDSSP when running the `Test-SRTopology` cmdlet remotely from a management computer.
- The source or destination volume specified are local disks on a cluster node, not clustered disks.

## Configuring new Storage Replica partnership returns an error - "Failed to provision partition"

When attempting to create a new replication partnership with `New-SRPartnership`, you receive the following error:

```
New-SRPartnership : Unable to create replication group test01, detailed reason: Failed to provision
partition ed0dc93f-107c-4ab4-a785-afd687d3e734.
At line: 1 char: 1
+ New-SRPartnership -SourceComputerName srv1 -SourceRGName test01
+ Categorylnfo : ObjectNotFound: (MSFT_WvrAdminTasks : root/ Microsoft/. . s) CNew-SRPartnership],
CimException
+ FullyQua1ifiedErrorId : Windows System Error 1168 ,New-SRPartnership
```

This is caused by selecting a data volume that is on the same partition as the System Drive (i.e. the **C:- *drive with its Windows folder). For instance, on a drive that contains both the **C:-* and **D:*- volumes created from the same partition. This is not supported in Storage Replica; you must pick a different volume to replicate.

## Attempting to grow a replicated volume fails due to missing update

When attempting to grow or extend a replicated volume, you receive the following error:

```
Resize-Partition -DriveLetter d -Size 44GB
Resize-Partition : The operation failed with return code 8
At line:1 char:1
+ Resize-Partition -DriveLetter d -Size 44GB
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : NotSpecified: (StorageWMI:ROOT/Microsoft/.../MSFT_Partition
[Resize-Partition], CimException
+ FullyQualifiedErrorId : StorageWMI 8,Resize-Partition
```

If using the Disk Management MMC snapin, you receive this error:

```
Element not found
```

This occurs even if you correctly enable volume resizing on the source server using `Set-SRGroup -Name rg01 -AllowVolumeResize $TRUE`.

This issue was fixed in Cumulative Update for Windows 10, version 1607 (Anniversary Update) and Windows Server 2016: December 9, 2016 (KB3201845).

## Attempting to grow a replicated volume fails due to missing step

If you attempt to resize a replicated volume on the source server without setting `-AllowResizeVolume $TRUE` first, you will receive the following errors:

```
Resize-Partition -DriveLetter I -Size 8GB
Resize-Partition : Failed

Activity ID: {87aebbd6-4f47-4621-8aa4-5328dfa6c3be}
At line:1 char:1
+ Resize-Partition -DriveLetter I -Size 8GB
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (StorageWMI:ROOT/Microsoft/.../MSFT_Partition) [Resize-
Partition], CimException
     + FullyQualifiedErrorId : StorageWMI 4,Resize-Partition

Storage Replica Event log error 10307:

Attempted to resize a partition that is protected by Storage Replica.

DeviceName: \Device\Harddisk1\DR1
PartitionNumber: 7
PartitionId: {b71a79ca-0efe-4f9a-a2b9-3ed4084a1822}

Guidance: To grow a source data partition, set the policy on the replication group containing the data
partition.
```

```
Set-SRGroup -ComputerName [ComputerName] -Name [ReplicationGroupName] -AllowVolumeResize $true
```

Before you grow the source data partition, ensure that the destination data partition has enough space to grow to an equal size. Shrinking of data partition protected by Storage Replica is blocked.

Disk Management Snap-in Error:

```
An unexpected error has occurred
```

After resizing the volume, remember to disable resizing with `Set-SRGroup -Name rg01 -AllowVolumeResize $FALSE`. This parameter prevents admins from attempting to resize volumes prior to ensuring that there is sufficient space on the destination volume, typically because they were unaware of Storage Replica's presence.

## Attempting to move a PDR resource between sites on an asynchronous stretch cluster fails

When attempting to move a physical disk resource-attached role - such as a file server for general use - in order to move the associated storage in an asynchronous stretch cluster, you receive an error.

If using the Failover Cluster Manager snap-in:

```
Error
The operation has failed.
The action 'Move' did not complete.
Error Code: 0x80071398
The operation failed because either the specified cluster node is not the owner of the group, or the node is
not a possible owner of the group
```

If using the Cluster powershell cmdlet:

```
Move-ClusterGroup -Name sr-fs-006 -Node sr-srv07
Move-ClusterGroup : An error occurred while moving the clustered role 'sr-fs-006'.
The operation failed because either the specified cluster node is not the owner of the group, or the node is
not a possible owner of the group
At line:1 char:1
+ Move-ClusterGroup -Name sr-fs-006 -Node sr-srv07
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : NotSpecified: (:) [Move-ClusterGroup], ClusterCmdletException
+ FullyQualifiedErrorId : Move-ClusterGroup,Microsoft.FailoverClusters.PowerShell.MoveClusterGroupCommand
```

This occurs due to a by-design behavior in Windows Server 2016. Use `Set-SRPartnership` to move these PDR disks in an asynchronous stretched cluster.

This behavior has been changed in Windows Server, version 1709 to allow manual and automated failovers with asynchronous replication, based on customer feedback.

## Attempting to add disks to a two-node asymmetric cluster returns "No disks suitable for cluster disks found"

When attempting to provision a cluster with only two nodes, prior to adding Storage Replica stretch replication, you attempt to add the disks in the second site to the Available Disks. You receive the following error:

```
No disks suitable for cluster disks found. For diagnostic information about disks available to the cluster,
use the Validate a Configuration Wizard to run Storage tests.
```

This does not occur if you have at least three nodes in the cluster. This issue occurs because of a by-design code change in Windows Server 2016 for asymmetric storage clustering behaviors.

To add the storage, you can run the following command on the node in the second site:

```
Get-ClusterAvailableDisk -All | Add-ClusterDisk
```

This will not work with node local storage. You can use Storage Replica to replicate a stretch cluster between two total nodes, **each one using its own set of shared storage.**

## The SMB Bandwidth limiter fails to throttle Storage Replica bandwidth

When specifying a bandwidth limit to Storage Replica, the limit is ignored and full bandwidth used. For example:

```
Set-SmbBandwidthLimit  -Category StorageReplication -BytesPerSecond 32MB
```

This issue occurs because of an interoperability issue between Storage Replica and SMB. This issue was first fixed in the July 2017 Cumulative Update of Windows Server 2016 and in Windows Server, version 1709.

## Event 1241 warning repeated during initial sync

When specifying a replication partnership is asynchronous, the source computer repeatedly logs warning event 1241 in the Storage Replica Admin channel. For example:

```
Log Name:      Microsoft-Windows-StorageReplica/Admin
Source:        Microsoft-Windows-StorageReplica
Date:          3/21/2017 3:10:41 PM
Event ID:      1241
Task Category: (1)
Level:         Warning
Keywords:      (1)
User:          SYSTEM
Computer:      sr-srv05.corp.contoso.com
Description:
The Recovery Point Objective (RPO) of the asynchronous destination is unavailable.

LocalReplicationGroupName: rg01
LocalReplicationGroupId: {e20b6c68-1758-4ce4-bd3b-84a5b5ef2a87}
LocalReplicaName: f:\
LocalPartitionId: {27484a49-0f62-4515-8588-3755a292657f}
ReplicaSetId: {1f6446b5-d5fd-4776-b29b-f235d97d8c63}
RemoteReplicationGroupName: rg02
RemoteReplicationGroupId: {7f18e5ea-53ca-4b50-989c-9ac6afb3cc81}
TargetRPO: 30
```

Guidance: This is typically due to one of the following reasons:

- The asynchronous destination is currently disconnected. The RPO may become available after the connection is restored.
- The asynchronous destination is unable to keep pace with the source such that the most recent destination log record is no longer present in the source log. The destination will start block copying. The RPO should become available after block copying completes.

This is expected behavior during initial sync and can safely be ignored. This behavior may change in a later release. If you see this behavior during ongoing asynchronous replication, investigate the partnership to determine why replication is delayed beyond your configured RPO (30 seconds, by default).

## Event 4004 warning repeated after rebooting a replicated node

Under rare and usually unreproducable circumstances, rebooting a server that is in a partnership leads to replication failing and the rebooted node logging warning event 4004 with an access denied error.

```
Log Name:      Microsoft-Windows-StorageReplica/Admin
Source:        Microsoft-Windows-StorageReplica
Date:          3/21/2017 11:43:25 AM
Event ID:      4004
Task Category: (7)
Level:         Warning
Keywords:      (256)
User:          SYSTEM
Computer:      server.contoso.com
Description:
Failed to establish a connection to a remote computer.

RemoteComputerName: server
LocalReplicationGroupName: rg01
LocalReplicationGroupId: {a386f747-bcae-40ac-9f4b-1942eb4498a0}
RemoteReplicationGroupName: rg02
RemoteReplicationGroupId: {a386f747-bcae-40ac-9f4b-1942eb4498a0}
ReplicaSetId: {00000000-0000-0000-0000-000000000000}
RemoteShareName:{a386f747-bcae-40ac-9f4b-1942eb4498a0}.{00000000-0000-0000-0000-000000000000}
Status: {Access Denied}
A process has requested access to an object, but has not been granted those access rights.

Guidance: Possible causes include network failures, share creation failures for the remote replication
group, or firewall settings. Make sure SMB traffic is allowed and there are no connectivity issues between
the local computer and the remote computer. You should expect this event when suspending replication or
removing a replication partnership.
```

Note the `Status: "{Access Denied}"` and the message `A process has requested access to an object, but has not been granted those access rights.` This is a known issue within Storage Replica and was fixed in Quality Update September 12, 2017—KB4038782 (OS Build 14393.1715) https://support.microsoft.com/help/4038782/windows-10-update-kb4038782

## Error "Failed to bring the resource 'Cluster Disk x' online." with a stretch cluster

When attempting to bring a cluster disk online after a successful failover, where you are attempting to make the original source site primary again, you receive an error in Failover Cluster Manager. For example:

```
Error
The operation has failed.
Failed to bring the resource 'Cluster Disk 2' online.

Error Code: 0x80071397
The operation failed because either the specified cluster node is not the owner of the resource, or the node
is not a possible owner of the resource.
```

If you attempt to move the disk or CSV manually, you receive an additional error. For example:

```
Error
The operation has failed.
The action 'Move' did not complete.

Error Code: 0x8007138d
A cluster node is not available for this operation
```

This issue is caused by one or more uninitialized disks being attached to one or more cluster nodes. To resolve the issue, initialize all attached storage using DiskMgmt.msc, DISKPART.EXE, or the Initialize-Disk PowerShell cmdlet.

We are working on providing an update that permanently resolves this issue. If you are interested in assisting us and you have a Microsoft Premier Support agreement, please email SRFEED@microsoft.com so that we can work with you on filing a backport request.

## GPT error when attempting to create a new SR partnership

When running New-SRPartnership, it fails with error:

```
Disk layout type for volume \\?\Volume{GUID}\ is not a valid GPT style layout.
New-SRPartnership : Unable to create replication group SRG01, detailed reason: Disk layout type for volume
\\?\Volume{GUID}\ is not a valid GPT style layout.
At line:1 char:1
+ New-SRPartnership -SourceComputerName nodesrc01 -SourceRGName SRG01 ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (MSFT_WvrAdminTasks:root/Microsoft/...T_WvrAdminTasks) [New-SRPartnership],
CimException
+ FullyQualifiedErrorId : Windows System Error 5078,New-SRPartnership
```

In the Failover Cluster Manager GUI, there is no option to setup Replication for the disk.

When running Test-SRTopology, it fails with:

```
WARNING: Object reference not set to an instance of an object.
WARNING: System.NullReferenceException
WARNING:    at
Microsoft.FileServices.SR.Powershell.MSFTPartition.GetPartitionInStorageNodeByAccessPath(String AccessPath,
String ComputerName, MIObject StorageNode)
    at Microsoft.FileServices.SR.Powershell.Volume.GetVolume(String Path, String ComputerName)
    at Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand.BeginProcessing()
Test-SRTopology : Object reference not set to an instance of an object.
At line:1 char:1
+ Test-SRTopology -SourceComputerName nodesrc01 -SourceVolumeName U: - ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : InvalidArgument: (:) [Test-SRTopology], NullReferenceException
+ FullyQualifiedErrorId : TestSRTopologyFailure,Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand
```

This is caused by the cluster functional level still being set to Windows Server 2012 R2 (i.e. FL 8). Storage Replica is supposed to return a specific error here but instead returns an incorrect error mapping.

```
Run Get-Cluster | fl - on each node.
```

If `ClusterFunctionalLevel = 9`, that is the Windows 2016 ClusterFunctionalLevel version needed to implement Storage Replica on this node. If ClusterFunctionalLevel is not 9, the ClusterFunctionalLevel will need to be updated in order to implement Storage Replica on this node.

To resolve the issue, raise the cluster functional level by running the PowerShell cmdlet: Update-ClusterFunctionalLevel.

## Small unknown partition listed in DISKMGMT for each replicated volume

When running the Disk Management snap-in (DISKMGMT.MSC), you notice one or more volumes listed with no label or drive letter and 1MB in size. You may be able to delete the unknown volume or you may receive:

```
An Unexpected Error has Occurred
```

This behavior is by design. This not a volume, but a partition. Storage Replica creates a 512KB partition as a database slot for replication operations (the legacy DiskMgmt.msc tool rounds to the nearest MB). Having a partition like this for each replicated volume is normal and desirable. When no longer in use, you are free to delete this 512KB partition; in-use ones cannot be deleted. The partition will never grow or shrink. If you are recreating replication we recommend leaving the partition as Storage Replica will claim unused ones.

To view details, use the DISKPART tool or Get-Partition cmdlet. These partitions will have a GPT Type of `558d43c5-a1ac-43c0-aac8-d1472b2923d1`.

## A Storage Replica node hangs when creating snapshots

When creating a VSS snapshot (through backup, VSSADMIN, etc) a Storage Replica node hangs, and you must force a restart of the node to recover. There is no error, just a hard hang of the server.

This issue occurs when you create a VSS snapshot of the log volume. The underlying cause is a legacy design aspect of VSS, not Storage Replica. The resulting behavior when you snapshot the Storage Replica log volume is a VSS I/O queing mechanism deadlocks the server.

To prevent this behavior, do not snapshot Storage Replica log volumes. There is no need to snapshot Storage Replica log volumes, as these logs cannot be restored. Furthermore, the log volume should never contain any other workloads, so no snapshot is needed in general.

## High IO latency increase when using Storage Spaces Direct with Storage Replica

When using Storage Spaces Direct with an NVME or SSD cache, you see a greater than expected increase in latency when configuring Storage Replica replication between Storage Spaces Direct clusters. The change in latency is proportionally much higher than you see when using NVME and SSD in a performance + capacity configuration and no HDD tier nor capacity tier.

This issue occurs due to architectural limitations within Storage Replica's log mechanism combined with the extremely low latency of NVME when compared to slower media. When using the Storage Spaces Direct cache, all I/O of Storage Replica logs, along with all recent read/write IO of applications, will occur in the cache and never on the performance or capacity tiers. This means that all Storage Replica activity happens on the same speed media - this configuration is supported but not recommended (see https://aka.ms/srfaq for log recommendations).

When using Storage Spaces Direct with HDDs, you cannot disable or avoid the cache. As a workaround, if using just SSD and NVME, you can configure just performance and capacity tiers. If using that configuration, and by placing the SR logs on the performance tier only with the data volumes they service being on the capacity tier only, you will avoid the high latency issue described above. The same could be done with a mix of faster and slower SSDs and no NVME.

This workaround is of course not ideal and some customers may not be able to make use of it. The Storage Replica team is working on optimizations and an updated log mechanism for the future to reduce these artificial bottlenecks. This v1.1 log first became available in Windows Server 2019 and its improved performance is described in on the Server Storage Blog.

## Error "Could not find file" when running Test-SRTopology between two clusters

When running Test-SRTopology between two clusters and their CSV paths, it fails with error:

```
PS C:\Windows\system32> Test-SRTopology -SourceComputerName NedClusterA -SourceVolumeName
C:\ClusterStorage\Volume1 -SourceLogVolumeName L: -DestinationComputerName NedClusterB -
DestinationVolumeName C:\ClusterStorage\Volume1 -DestinationLogVolumeName L: -DurationInMinutes 1 -
ResultPath C:\Temp

Validating data and log volumes...
Measuring Storage Replica recovery and initial synchronization performance...
WARNING: Could not find file
'\\NedNode1\C$\CLUSTERSTORAGE\VOLUME1TestSRTopologyRecoveryTest\SRRecoveryTestFile01.txt'.
WARNING: System.IO.FileNotFoundException
WARNING:    at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
at System.IO.FileStream.Init(String path, FileMode mode, FileAccess access, Int32 rights, Boolean useRights,
FileShare share, Int32 bufferSize, FileOptions options, SECURITY_ATTRIBUTES secAttrs, String msgPath,
Boolean bFromProxy, Boolean useLongPath, Boolean checkHost) at System.IO.FileStream..ctor(String path,
FileMode mode, FileAccess access, FileShare share, Int32 bufferSize, FileOptions options) at
Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand.GenerateWriteIOWorkload(String Path, UInt32
IoSizeInBytes, UInt32 Parallel IoCount, UInt32 Duration)at
Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand.<>c__DisplayClass75_0.
<PerformRecoveryTest>b__0()at System.Threading.Tasks.Task.Execute()
Test-SRTopology : Could not find file
'\\NedNode1\C$\CLUSTERSTORAGE\VOLUME1TestSRTopologyRecoveryTest\SRRecoveryTestFile01.txt'.
At line:1 char:1
+ Test-SRTopology -SourceComputerName NedClusterA -SourceVolumeName  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : ObjectNotFound: (:) [Test-SRTopology], FileNotFoundException
+ FullyQualifiedErrorId : TestSRTopologyFailure,Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand
```

This is caused by a known code defect in Windows Server 2016. This issue was first fixed in Windows Server, version 1709 and the associated RSAT tools. For a downlevel resolution, please contact Microsoft Support and request a backport update. There is no workaround.

## Error "specified volume could not be found" when running Test-SRTopology between two clusters

When running Test-SRTopology between two clusters and their CSV paths, it fails with error:

```
PS C:\> Test-SRTopology -SourceComputerName RRN44-14-09 -SourceVolumeName C:\ClusterStorage\Volume1 -
SourceLogVolumeName L: -DestinationComputerName RRN44-14-13 -DestinationVolumeName C:\ClusterStorage\Volume1
-DestinationLogVolumeName L: -DurationInMinutes 30 -ResultPath c:\report

Test-SRTopology : The specified volume C:\ClusterStorage\Volume1 cannot be found on computer RRN44-14-09. If
this is a cluster node, the volume must be part of a role or CSV; volumes in Available Storage are not
accessible
At line:1 char:1
+ Test-SRTopology -SourceComputerName RRN44-14-09 -SourceVolumeName C:\ ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (:) [Test-SRTopology], Exception
    + FullyQualifiedErrorId :
TestSRTopologyFailure,Microsoft.FileServices.SR.Powershell.TestSRTopologyCommand
```

When specifying the source node CSV as the source volume, you must select the node that owns the CSV. You can either move the CSV to the specified node or change the node name you specified in `-SourceComputerName`. This error received an improved message in Windows Server 2019.

## Unable to access the data drive in Storage Replica after unexpected reboot when BitLocker is enabled

If BitLocker is enabled on both drives (Log Drive and Data Drive) and in both Storage replica drives, if the Primary Server reboots then you are unable to access the Primary Drive even after unlocking the Log Drive from

BitLocker.

This is an expected behavior. To recover the data or access the drive, you need to unlock the log drive first and then open Diskmgmt.msc to locate the data drive. Turn the data drive offline and online again. Locate the BitLocker icon on the drive and unlock the drive.

## Issue unlocking the Data drive on secondary server after breaking the Storage Replica partnership

After Disabling the SR Partnership and removing the Storage Replica, it is expected if you are unable to unlock the Secondary Server's Data drive with its respective password or key.

You need to use Key or Password of Primary Server's Data drive to unlock the Secondary Server's data drive.

## Test Failover doesn't mount when using asynchronous replication

When running Mount-SRDestination to bring a destination volume online as part of the Test Failover feature, it fails with error:

```
Mount-SRDestination: Unable to mount SR group <TEST>, detailed reason: The group or resource is not in the
correct state to perform the supported operation.
    At line:1 char:1
    + Mount-SRDestination -ComputerName SRV1 -Name TEST -TemporaryP . . .
    + ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
        + CategoryInfo          : NotSpecified: (MSFT WvrAdminTasks : root/Microsoft/...(MSFT WvrAdminTasks
: root/Microsoft/. T_WvrAdminTasks) (Mount-SRDestination], CimException
        + FullyQua1ifiedErrorId : Windows System Error 5823, Mount-SRDestination.
```

If using a synchronous partnership type, test failover works normally.

This is caused by a known code defect in Windows Server, version 1709. To resolve this issue, install the October 18, 2018 update. This issue isn't present in Windows Server 2019 and Windows Server, version 1809 and newer.

## Additional References

- Storage Replica
- Stretch Cluster Replication Using Shared Storage
- Server to Server Storage Replication
- Cluster to Cluster Storage Replication
- Storage Replica: Frequently Asked Questions
- Storage Spaces Direct

# Frequently Asked Questions about Storage Replica

12/16/2020 • 16 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

This topic contains answers to frequently asked questions (FAQs) about Storage Replica.

## Is Storage Replica supported on Azure?

Yes. You can use the following scenarios with Azure:

1. Server-to-server replication inside Azure (synchronously or asynchronously between IaaS VMs in one or two datacenter fault domains, or asynchronously between two separate regions)
2. Server-to-server asynchronous replication between Azure and on-premises (using VPN or Azure ExpressRoute)
3. Cluster-to-cluster replication inside Azure (synchronously or asynchronously between IaaS VMs in one or two datacenter fault domains, or asynchronously between two separate regions)
4. Cluster-to-cluster asynchronous replication between Azure and on-premises (using VPN or Azure ExpressRoute)

Further notes on guest clustering in Azure can be found at: Deploying IaaS VM Guest Clusters in Microsoft Azure.

Important notes:

1. Azure doesn't support shared VHDX guest clustering, so Windows Failover Cluster virtual machines must use iSCSI targets for classic shared-storage persistent disk reservation clustering or Storage Spaces Direct.
2. There are Azure Resource Manager templates for Storage Spaces Direct-based Storage Replica clustering at Create a Storage Spaces Direct SOFS Clusters with Storage Replica for Disaster Recovery across Azure Regions.
3. Cluster to cluster RPC communication in Azure (required by the cluster APIs for granting access between cluster) requires configuring network access for the CNO. You must allow TCP port 135 and the dynamic range above TCP port 49152. Reference Building Windows Server Failover Cluster on Azure IAAS VM – Part 2 Network and Creation.
4. It's possible to use two-node guest clusters, where each node is using loopback iSCSI for an asymmetric cluster replicated by Storage Replica. But this will likely have very poor performance and should be used only for very limited workloads or testing.

## How do I see the progress of replication during initial sync?

The Event 1237 messages shown in the Storage Replica Admin even log on the destination server show number of bytes copied and bytes remaining every 10 seconds. You can also use the Storage Replica performance counter on the destination showing **\Storage Replica Statistics\Total Bytes Received** for one or more replicated volumes. You can also query the replication group using Windows PowerShell. For instance, this sample command gets the name of the groups on the destination then queries one group named **Replication 2** every 10 seconds to show progress:

```
Get-SRGroup

do{
    $r=(Get-SRGroup -Name "Replication 2").replicas
    [System.Console]::Write("Number of remaining bytes {0}`n", $r.NumOfBytesRemaining)
    Start-Sleep 10
}until($r.ReplicationStatus -eq 'ContinuouslyReplicating')
Write-Output "Replica Status: "$r.replicationstatus
```

## Can I specify specific network interfaces to be used for replication?

Yes, using `Set-SRNetworkConstraint`. This cmdlet operates at the interface layer and be used on both cluster and non-cluster scenarios. For example, with a standalone server (on each node):

```
Get-SRPartnership

Get-NetIPConfiguration
```

Note the gateway and interface information (on both servers) and the partnership directions. Then run:

```
Set-SRNetworkConstraint -SourceComputerName sr-srv06 -SourceRGName rg02 -
SourceNWInterface 2 -DestinationComputerName sr-srv05 -DestinationNWInterface 3 -DestinationRGName rg01

Get-SRNetworkConstraint

Update-SmbMultichannelConnection
```

For configuring network constraints on a stretch cluster:

```
Set-SRNetworkConstraint -SourceComputerName sr-cluster01 -SourceRGName group1 -SourceNWInterface "Cluster
Network 1","Cluster Network 2" -DestinationComputerName sr-cluster02 -DestinationRGName group2 -
DestinationNWInterface "Cluster Network 1","Cluster Network 2"
```

## Can I configure one-to-many replication or transitive (A to B to C) replication?

No, Storage Replica supports only one to one replication of a server, cluster, or stretch cluster node. This may change in a later release. You can of course configure replication between various servers of a specific volume pair, in either direction. For instance, Server 1 can replicate its D volume to server 2, and its E volume from Server 3.

## Can I grow or shrink replicated volumes replicated by Storage Replica?

You can grow (extend) volumes, but not shrink them. By default, Storage Replica prevents administrators from extending replicated volumes; use the `Set-SRGroup -AllowVolumeResize $TRUE` option on the source group, prior to resizing. For example:

1. Use against the source computer: `Set-SRGroup -Name YourRG -AllowVolumeResize $TRUE`
2. Grow the volume using whatever technique you prefer
3. Use against the source computer: `Set-SRGroup -Name YourRG -AllowVolumeResize $FALSE`

## Can I bring a destination volume online for read-only access?

Not in Windows Server 2016. Storage Replica dismounts the destination volume when replication begins.

However, in Windows Server 2019 and Windows Server Semi-Annual Channel starting with version, 1709, the option to mount the destination storage is now possible - this feature is called "Test Failover". To do this, you must have an unused, NTFS or ReFS formatted volume that is not currently replicating on the destination. Then you can mount a snapshot of the replicated storage temporarily for testing or backup purposes.

For example, to create a test failover where you are replicating a volume "D:" in the Replication Group "RG2" on the destination server "SRV2" and have a "T:" drive on SRV2 that is not being replicated:

```
Mount-SRDestination -Name RG2 -Computername SRV2 -TemporaryPath T:\
```

The replicated volume D: is now accessible on SRV2. You can read and write to it normally, copy files off it, or run an online backup that you save elsewhere for safekeeping, under the D: path. The T: volume will only contain log data.

To remove the test failover snapshot and discard its changes:

```
Dismount-SRDestination -Name RG2 -Computername SRV2
```

You should only use the test failover feature for short-term temporary operations. It is not intended for long term usage. When in use, replication continues to the real destination volume.

## Can I configure Scale-out File Server (SOFS) in a stretch cluster?

While technically possible, this is not a recommended configuration due to the lack of site awareness in the compute nodes contacting the SOFS. If using campus-distance networking, where latencies are typically sub-millisecond, this configuration typically works without issues.

If configuring cluster-to-cluster replication, Storage Replica fully supports Scale-out File Servers, including the use of Storage Spaces Direct, when replicating between two clusters.

## Is CSV required to replicate in a stretch cluster or between clusters?

No. You can replicate with CSV or persistent disk reservation (PDR) owned by a cluster resource, such as a File Server role.

If configuring cluster-to-cluster replication, Storage Replica fully supports Scale-out File Servers, including the use of Storage Spaces Direct, when replicating between two clusters.

## Can I configure Storage Spaces Direct in a stretch cluster with Storage Replica?

This is not a supported configuration in Windows Server. This may change in a later release. If configuring cluster-to-cluster replication, Storage Replica fully supports Scale Out File Servers and Hyper-V Servers, including the use of Storage Spaces Direct.

## How do I configure asynchronous replication?

Specify `New-SRPartnership -ReplicationMode` and provide argument **Asynchronous**. By default, all replication in Storage Replica is synchronous. You can also change the mode with `Set-SRPartnership -ReplicationMode`.

## How do I prevent automatic failover of a stretch cluster?

To prevent automatic failover, you can use PowerShell to configure

`Get-ClusterNode -Name "NodeName").NodeWeight=0`. This removes the vote on each node in the disaster recovery site. Then you can use `Start-ClusterNode -PreventQuorum` on nodes in the primary site and `Start-ClusterNode -ForceQuorum` on nodes in the disaster site to force failover. There is no graphical option for preventing automatic failover, and preventing automatic failover is not recommended.

## How do I disable virtual machine resiliency?

To prevent the new Hyper-V virtual machine resiliency feature from running and therefore pausing virtual machines instead of failing them over to the disaster recovery site, run `(Get-Cluster).ResiliencyDefaultPeriod=0`

## How can I reduce time for initial synchronization?

You can use thin-provisioned storage as one way to speed up initial sync times. Storage Replica queries for and automatically uses thin-provisioned storage, including non-clustered Storage Spaces, Hyper-V dynamic disks, and SAN LUNs.

You can also use seeded data volumes to reduce bandwidth usage and sometimes time, by ensuring that the destination volume has some subset of data from the primary then using the Seeded option in Failover Cluster Manager or `New-SRPartnership`. If the volume is mostly empty, using seeded sync may reduce time and bandwidth usage. There are multiple ways to seed data, with varying degrees of efficacy:

1. Previous replication - by replicating with normal initial sync locally between nodes containing the disks and volumes, removing replication, shipping the destination disks elsewhere, then adding replication with the seeded option. This is the most effective method as Storage Replica guaranteed a block-copy mirror and the only thing to replicate is delta blocks.
2. Restored snapshot or restored snapshot-based backup - by restoring a volume-based snapshot onto the destination volume, there should be minimal differences in the block layout. This is the next most effective method as blocks are likely to match thanks to volume snapshots being mirror images.
3. Copied files - by creating a new volume on the destination that has never been used before and performing a full robocopy /MIR tree copy of the data, there are likely to be block matches. Using Windows File Explorer or copying some portion of the tree will not create many block matches. Copying files manually is the least effective method of seeding.

## Can I delegate users to administer replication?

You can use the `Grant-SRDelegation` cmdlet. This allows you to set specific users in server to server, cluster to cluster, and stretch cluster replication scenarios as having the permissions to create, modify, or remove replication, without being a member of the local administrators group. For example:

```
Grant-SRDelegation -UserName contso\tonywang
```

The cmdlet will remind you that the user needs to log off and on of the server they are planning to administer in order for the change to take effect. You can use `Get-SRDelegation` and `Revoke-SRDelegation` to further control this.

## What are my backup and restore options for replicated volumes?

Storage Replica supports backing up and restoring the source volume. It also supports creating and restoring snapshots of the source volume. You cannot backup or restore the destination volume while protected by Storage Replica, as it is not mounted nor accessible. If you experience a disaster where the source volume is lost, using `Set-SRPartnership` to promote the previous destination volume to now be a read/writable source will allow you to backup or restore that volume. You can also remove replication with `Remove-SRPartnership` and

`Remove-SRGroup` to remount that volume as read/writable.

To create periodic application consistent snapshots, you can use VSSADMIN.EXE on the source server to snapshot replicated data volumes. For example, where you are replicating the F: volume with Storage Replica:

```
vssadmin create shadow /for=F:
```

Then, after you switch replication direction, remove replication, or are simply still on the same source volume, you can restore any snapshot to its point in time. For example, still using F:

```
vssadmin list shadows
vssadmin revert shadow /shadow={shadown copy ID GUID listed previously}
```

You can also schedule this tool to run periodically using a scheduled task. For more information on using VSS, review Vssadmin. There is no need or value in backing up the log volumes. Attempting to do so will be ignored by VSS.

Use of Windows Server Backup, Microsoft Azure Backup, Microsoft DPM, or other snapshot, VSS, virtual machine, or file-based technologies are supported by Storage Replica as long as they operate within the volume layer. Storage Replica does not support block-based backup and restore.

## Can I configure replication to restrict bandwidth usage?

Yes, via the SMB bandwidth limiter. This is a global setting for all Storage Replica traffic and therefore affects all replication from this server. Typically, this is needed only with Storage Replica initial sync setup, where all the volume data must transfer. If needed after initial sync, your network bandwidth is too low for your IO workload; reduce the IO or increase the bandwidth.

This should only be used with asynchronous replication (note: initial sync is always asynchronous even if you have specified synchronous). You can also use network QoS policies to shape Storage Replica traffic. Use of highly matched seeded Storage Replica replication will also lower overall initial sync bandwidth usage considerably.

To set the bandwidth limit, use:

```
Set-SmbBandwidthLimit  -Category StorageReplication -BytesPerSecond x
```

To see the bandwidth limit, use:

```
Get-SmbBandwidthLimit -Category StorageReplication
```

To remove the bandwidth limit, use:

```
Remove-SmbBandwidthLimit -Category StorageReplication
```

## What network ports does Storage Replica require?

Storage Replica relies on SMB and WSMAN for its replication and management. This means the following ports are required:

- 445 (SMB - replication transport protocol, cluster RPC management protocol)
- 5445 (iWARP SMB - only needed when using iWARP RDMA networking)

- 5985 (WSManHTTP - Management protocol for WMI/CIM/PowerShell)

> ![NOTE] The Test-SRTopology cmdlet requires ICMPv4/ICMPv6, but not for replication or management.

## What are the log volume best practices?

The optimal size of the log varies widely per environment and workload, and is determined by how much write IO your workload performs.

1. A larger or smaller log doesn't make you any faster or slower
2. A larger or smaller log doesn't have any bearing on a 10GB data volume versus a 10TB data volume, for instance

A larger log simply collects and retains more write IOs before they are wrapped out. This allows an interruption in service between the source and destination computer – such as a network outage or the destination being offline - to go longer. If the log can hold 10 hours of writes, and the network goes down for 2 hours, when the network returns the source can simply play the delta of unsynced changes back to the destination very fast and you are protected again very quickly. If the log holds 10 hours and the outage is 2 days, the source now has to play back from a different log called the bitmap – and will likely be slower to get back into sync. Once in sync it returns to using the log.

Storage Replica relies on the log for all write performance. Log performance critical to replication performance. You must ensure that the log volume performs better than the data volume, as the log will serialize and sequentialize all write IO. You should always use flash media like SSD on log volumes. You must never allow any other workloads to run on the log volume, the same way you would never allow other workloads to run on SQL database log volumes.

Again: Microsoft strongly recommends that the log storage be faster than the data storage and that log volumes must never be used for other workloads.

You can get log sizing recommendations by running the Test-SRTopology tool. Alternatively, you can use performance counters on existing servers to make a log size judgement. The formula is simple: monitor the data disk throughput (Avg Write Bytes/Sec) under the workload and use it to calculate the amount of time it will take to fill up the log of different sizes. For example, data disk throughput of 50 MB/s will cause the log of 120GB to wrap in 120GB/50MB seconds or 2400 seconds or 40 minutes. So the amount of time that the destination server could be unreachable before the log wrapped is 40 minutes. If the log wraps but the destination becomes reachable again, the source would replay blocks via the bit map log instead of the main log. The size of the log does not have an effect on performance.

ONLY the Data disk from the Source cluster should be backed-up. The Storage Replica Log disks should NOT be backed-up since a backup can conflict with Storage Replica operations.

## Why would you choose a stretch cluster versus cluster-to-cluster versus server-to-server topology?

Storage Replica comes in three main configurations: stretch cluster, cluster-to-cluster, and server-to-server. There are different advantages to each.

The stretch cluster topology is ideal for workloads requiring automatic failover with orchestration, such as Hyper-V private cloud clusters and SQL Server FCI. It also has a built-in graphical interface using Failover Cluster Manager. It utilizes the classic asymmetric cluster shared storage architecture of Storage Spaces, SAN, iSCSI, and RAID via persistent reservation. You can run this with as few as 2 nodes.

The cluster-to-cluster topology uses two separate clusters and is ideal for administrators who want manual failover, especially when the second site is provisioned for disaster recovery and not everyday usage.

Orchestration is manual. Unlike stretch cluster, Storage Spaces Direct can be used in this configuration (with caveats - see the Storage Replica FAQ and cluster-to-cluster documentation). You can run this with as few as four nodes.

The server-to-server topology is ideal for customers running hardware that cannot be clustered. It requires manual failover and orchestration. It is ideal for inexpensive deployments between branch offices and central data centers, especially when using asynchronous replication. This configuration can often replace instances of DFSR-protected File Servers used for single-master disaster recovery scenarios.

In all cases, the topologies support both running on physical hardware as well as virtual machines. When in virtual machines, the underlying hypervisor doesn't require Hyper-V; it can be VMware, KVM, Xen, etc.

Storage Replica also has a server-to-self mode, where you point replication to two different volumes on the same computer.

## Is Data Deduplication supported with Storage Replica?

Yes, Data Deduplcation is supported with Storage Replica. Enable Data Deduplication on a volume on the source server, and during replication the destination server receives a deduplicated copy of the volume.

While you should *install* Data Deduplication on both the source and destination servers (see Installing and enabling Data Deduplication), it's important not to *enable* Data Deduplication on the destination server. Storage Replica allows writes only on the source server. Because Data Deduplication makes writes to the volume, it should run only on the source server.

## Can I replicate between Windows Server 2019 and Windows Server 2016?

Unfortunately, we don't support creating a *new* partnership between Windows Server 2019 and Windows Server 2016. You can safely upgrade a server or cluster running Windows Server 2016 to Windows Server 2019 and any *existing* partnerships will continue to work.

However, to get the improved replication performance of Windows Server 2019, all members of the partnership must run Windows Server 2019 and you must delete existing partnerships and associated replication groups and then recreate them with seeded data (either when creating the partnership in Windows Admin Center or with the New-SRPartnership cmdlet).

## How do I report an issue with Storage Replica or this guide?

For technical assistance with Storage Replica, you can post at the Microsoft forums. You can also email srfeed@microsoft.com for questions on Storage Replica or issues with this documentation. The Windows Server general feedback site is preferred for design change requests, as it allows your fellow customers to provide support and feedback for your ideas.

## Can Storage Replica be configured to replicate in both directions?

Storage Replica is a one-way replication technology. It will only replicate from the source to the destination on a per volume basis. This direction can be reversed at any time, but is still only in one direction. However, that does not mean you cannot have a set of volumes (source and destination) replicate in one direction and a different set of drives (source and destination) replicate in the opposite direction. For example, you have want to have server to server replication configured. Server1 and Server2 each have drive letters L:, M:, N:, and O: and you wish to replicate drive M: from Server1 to Server2 but drive O: replicate from Server2 to Server1. This can be done as long as there separate log drives for each of the groups. I.E.

- Server1 source drive M: with source log drive L: replicating to Server2 destination drive M: with destination

log drive L:

- Server2 source drive O: with source log drive N: replicating to Server1 destination drive O: with destination log drive N:

## Related Topics

- Storage Replica Overview
- Stretch Cluster Replication Using Shared Storage
- Server to Server Storage Replication
- Cluster to Cluster Storage Replication
- Storage Replica: Known Issues

## See Also

- Storage Overview
- Storage Spaces Direct

# Storage Spaces overview

12/16/2020 • 2 minutes to read • Edit Online

Storage Spaces is a technology in Windows and Windows Server that can help protect your data from drive failures. It is conceptually similar to RAID, implemented in software. You can use Storage Spaces to group three or more drives together into a storage pool and then use capacity from that pool to create Storage Spaces. These typically store extra copies of your data so if one of your drives fails, you still have an intact copy of your data. If you run low on capacity, just add more drives to the storage pool.

There are four major ways to use Storage Spaces:

- **On a Windows PC** - for more info, see Storage Spaces in Windows 10.
- **On a stand-alone server with all storage in a single server** - for more info, see Deploy Storage Spaces on a stand-alone server.
- **On a clustered server using Storage Spaces Direct with local, direct-attached storage in each cluster node** - for more info, see Storage Spaces Direct overview.
- **On a clustered server with one or more shared SAS storage enclosures holding all drives** - for more info, see Storage Spaces on a cluster with shared SAS overview.

# Deploy Storage Spaces on a stand-alone server

12/16/2020 • 12 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes how to deploy Storage Spaces on a stand-alone server. For information about how to create a clustered storage space, see Deploy a Storage Spaces cluster on Windows Server 2012 R2.

To create a storage space, you must first create one or more storage pools. A storage pool is a collection of physical disks. A storage pool enables storage aggregation, elastic capacity expansion, and delegated administration.

From a storage pool, you can create one or more virtual disks. These virtual disks are also referred to as *storage spaces*. A storage space appears to the Windows operating system as a regular disk from which you can create formatted volumes. When you create a virtual disk through the File and Storage Services user interface, you can configure the resiliency type (simple, mirror, or parity), the provisioning type (thin or fixed), and the size. Through Windows PowerShell, you can set additional parameters such as the number of columns, the interleave value, and which physical disks in the pool to use. For information about these additional parameters, see New-VirtualDisk and the Windows Server storage forum.

> **NOTE**
> You can't use a storage space to host the Windows operating system.

From a virtual disk, you can create one or more volumes. When you create a volume, you can configure the size, drive letter or folder, file system (NTFS file system or Resilient File System (ReFS)), allocation unit size, and an optional volume label.

The following figure illustrates the Storage Spaces workflow.

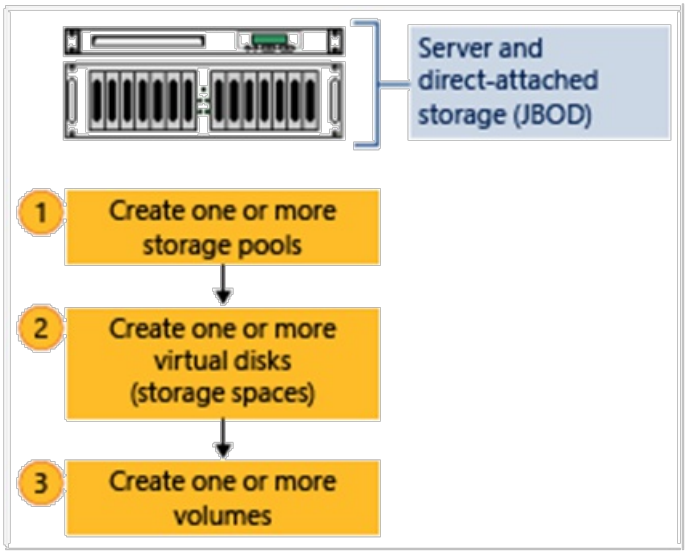



Figure 1: Storage Spaces workflow

**NOTE**

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see PowerShell.

## Prerequisites

To use Storage Spaces on a stand-alone Windows Server 2012–based server, make sure that the physical disks that you want to use meet the following prerequisites.

**IMPORTANT**

If you want to learn how to deploy Storage Spaces on a failover cluster, see Deploy a Storage Spaces cluster on Windows Server 2012 R2. A failover cluster deployment has different prerequisites, such as supported disk bus types, supported resiliency types, and the required minimum number of disks.

| AREA | REQUIREMENT | NOTES |
| --- | --- | --- |
| Disk bus types | - Serial Attached SCSI (SAS)<br>- Serial Advanced Technology Attachment (SATA)<br>- iSCSI and Fibre Channel Controllers. | You can also use USB drives. However, it's not optimal to use USB drives in a server environment.<br>Storage Spaces is supported on iSCSI and Fibre Channel (FC) controllers as long as the virtual disks created on top of them are non-resilient (Simple with any number of columns). |
| Disk configuration | - Physical disks must be at least 4 GB<br>- Disks must be blank and not formatted. Do not create volumes. | |
| HBA considerations | - Simple host bus adapters (HBAs) that do not support RAID functionality are recommended<br>- If RAID-capable, HBAs must be in non-RAID mode with all RAID functionality disabled<br>- Adapters must not abstract the physical disks, cache data, or obscure any attached devices. This includes enclosure services that are provided by attached just-a-bunch-of-disks (JBOD) devices. | Storage Spaces is compatible only with HBAs where you can completely disable all RAID functionality. |

| AREA | REQUIREMENT | NOTES |
| --- | --- | --- |
| JBOD enclosures | - JBOD enclosures are optional<br>- Recommended to use Storage Spaces certified enclosures listed on the Windows Server Catalog<br>- If you're using a JBOD enclosure, verify with your storage vendor that the enclosure supports Storage Spaces to ensure full functionality<br>- To determine whether the JBOD enclosure supports enclosure and slot identification, run the following Windows PowerShell cmdlet:<br><br>Get-PhysicalDisk \| ? {$_.BusType –eq "SAS"} \| fc | If the **EnclosureNumber** and **SlotNumber** fields contain values, then the enclosure supports these features. |

To plan for the number of physical disks and the desired resiliency type for a stand-alone server deployment, use the following guidelines.

| RESILIENCY TYPE | DISK REQUIREMENTS | WHEN TO USE |
| --- | --- | --- |
| **Simple**<br><br>- Stripes data across physical disks<br>- Maximizes disk capacity and increases throughput<br>- No resiliency (does not protect from disk failure) | Requires at least one physical disk. | Do not use to host irreplaceable data. Simple spaces do not protect against disk failure.<br><br>Use to host temporary or easily recreated data at a reduced cost.<br><br>Suited for high-performance workloads where resiliency is not required or is already provided by the application. |
| **Mirror**<br><br>- Stores two or three copies of the data across the set of physical disks<br>- Increases reliability, but reduces capacity. Duplication occurs with every write. A mirror space also stripes the data across multiple physical drives.<br>- Greater data throughput and lower access latency than parity<br>- Uses dirty region tracking (DRT) to track modifications to the disks in the pool. When the system resumes from an unplanned shutdown and the spaces are brought back online, DRT makes disks in the pool consistent with each other. | Requires at least two physical disks to protect from single disk failure.<br><br>Requires at least five physical disks to protect from two simultaneous disk failures. | Use for most deployments. For example, mirror spaces are suited for a general-purpose file share or a virtual hard disk (VHD) library. |

| RESILIENCY TYPE | DISK REQUIREMENTS | WHEN TO USE |
| --- | --- | --- |
| **Parity**<br><br>- Stripes data and parity information across physical disks<br>- Increases reliability when it is compared to a simple space, but somewhat reduces capacity<br>- Increases resiliency through journaling. This helps prevent data corruption if an unplanned shutdown occurs. | Requires at least three physical disks to protect from single disk failure. | Use for workloads that are highly sequential, such as archive or backup. |

## Step 1: Create a storage pool

You must first group available physical disks into one or more storage pools.

1. In the Server Manager navigation pane, select **File and Storage Services**.
2. In the navigation pane, select the **Storage Pools** page.

   By default, available disks are included in a pool that is named the *primordial* pool. If no primordial pool is listed under **STORAGE POOLS**, this indicates that the storage does not meet the requirements for Storage Spaces. Make sure that the disks meet the requirements that are outlined in the Prerequisites section.

   > **TIP**
   > If you select the **Primordial** storage pool, the available physical disks are listed under **PHYSICAL DISKS**.

3. Under **STORAGE POOLS**, select the **TASKS** list, and then select **New Storage Pool**. The New Storage Pool Wizard will open.
4. On the **Before you begin** page, select **Next**.
5. On the **Specify a storage pool name and subsystem** page, enter a name and optional description for the storage pool, select the group of available physical disks that you want to use, and then select **Next**.
6. On the **Select physical disks for the storage pool** page, do the following, and then select **Next**:

   a. Select the check box next to each physical disk that you want to include in the storage pool.

   b. If you want to designate one or more disks as hot spares, under **Allocation**, select the drop-down arrow, then select **Hot Spare**.

7. On the **Confirm selections** page, verify that the settings are correct, and then select **Create**.
8. On the **View results** page, verify that all tasks completed, and then select **Close**.

   > **NOTE**
   > Optionally, to continue directly to the next step, you can select the **Create a virtual disk when this wizard closes** check box.

9. Under **STORAGE POOLS**, verify that the new storage pool is listed.

**Windows PowerShell equivalent commands for creating storage pools**

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure.

Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

The following example shows which physical disks are available in the primordial pool.

```
Get-StoragePool -IsPrimordial $true | Get-PhysicalDisk -CanPool $True
```

The following example creates a new storage pool named *StoragePool1* that uses all available disks.

```
New-StoragePool –FriendlyName StoragePool1 –StorageSubsystemFriendlyName "Windows Storage*" –PhysicalDisks
(Get-PhysicalDisk –CanPool $True)
```

The following example creates a new storage pool, *StoragePool1*, that uses four of the available disks.

```
New-StoragePool –FriendlyName StoragePool1 –StorageSubsystemFriendlyName "Windows Storage*" –PhysicalDisks
(Get-PhysicalDisk PhysicalDisk1, PhysicalDisk2, PhysicalDisk3, PhysicalDisk4)
```

The following example sequence of cmdlets shows how to add an available physical disk *PhysicalDisk5* as a hot spare to the storage pool *StoragePool1*.

```
$PDToAdd = Get-PhysicalDisk –FriendlyName PhysicalDisk5
Add-PhysicalDisk –StoragePoolFriendlyName StoragePool1 –PhysicalDisks $PDToAdd –Usage HotSpare
```

## Step 2: Create a virtual disk

Next, you must create one or more virtual disks from the storage pool. When you create a virtual disk, you can select how the data is laid out across the physical disks. This affects both reliability and performance. You can also select whether to create thin- or fixed-provisioned disks.

1. If the New Virtual Disk Wizard is not already open, on the **Storage Pools** page in Server Manager, under **STORAGE POOLS**, make sure that the desired storage pool is selected.
2. Under **VIRTUAL DISKS**, select the **TASKS** list, and then select **New Virtual Disk**. The New Virtual Disk Wizard will open.
3. On the **Before you begin** page, select **Next**.
4. On the **Select the storage pool** page, select the desired storage pool, and then select **Next**.
5. On the **Specify the virtual disk name** page, enter a name and optional description, then select **Next**.
6. On the **Select the storage layout** page, select the desired layout, then select **Next**.

   > **NOTE**
   > If you select a layout where you do not have enough physical disks, you will receive an error message when you select **Next**. For information about which layout to use and the disk requirements, see Prerequisites).

7. If you selected **Mirror** as the storage layout, and you have five or more disks in the pool, the **Configure the resiliency settings** page will appear. Select one of the following options:
   - **Two-way mirror**
   - **Three-way mirror**
8. On the **Specify the provisioning type** page, select one of the following options, then select **Next**.

- **Thin**

  With thin provisioning, space is allocated on an as-needed basis. This optimizes the usage of available storage. However, because this enables you to over-allocate storage, you must carefully monitor how much disk space is available.

- **Fixed**

  With fixed provisioning, the storage capacity is allocated immediately, at the time a virtual disk is created. Therefore, fixed provisioning uses space from the storage pool that is equal to the virtual disk size.

  > **TIP**
  > With Storage Spaces, you can create both thin- and fixed-provisioned virtual disks in the same storage pool. For example, you could use a thin-provisioned virtual disk to host a database and a fixed-provisioned virtual disk to host the associated log files.

9. On the **Specify the size of the virtual disk** page, do the following:

   If you selected thin provisioning in the previous step, in the **Virtual disk size** box, enter a virtual disk size, select the units (**MB**, **GB**, or **TB**), then select **Next**.

   If you selected fixed provisioning in the previous step, select one of the following:

   - **Specify size**

     To specify a size, enter a value in the **Virtual disk size** box, then select the units (**MB**, **GB**, or **TB**).

     If you use a storage layout other than simple, the virtual disk uses more free space than the size that you specify. To avoid a potential error where the size of the volume exceeds the storage pool free space, you can select the **Create the largest virtual disk possible, up to the specified size** check box.

   - **Maximum size**

     Select this option to create a virtual disk that uses the maximum capacity of the storage pool.

10. On the **Confirm selections** page, verify that the settings are correct, and then select **Create**.
11. On the **View results** page, verify that all tasks completed, and then select **Close**.

    > **TIP**
    > By default, the **Create a volume when this wizard closes** check box is selected. This takes you directly to the next step.

**Windows PowerShell equivalent commands for creating virtual disks**

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

The following example creates a 50 GB virtual disk named *VirtualDisk1* on a storage pool named *StoragePool1*.

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –Size (50GB)
```

The following example creates a mirrored virtual disk named *VirtualDisk1* on a storage pool named *StoragePool1*.

The disk uses the storage pool's maximum storage capacity.

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –ResiliencySettingName Mirror
–UseMaximumSize
```

The following example creates a 50 GB virtual disk named *VirtualDisk1* on a storage pool that is named *StoragePool1*. The disk uses the thin provisioning type.

```
New-VirtualDisk –StoragePoolFriendlyName StoragePool1 –FriendlyName VirtualDisk1 –Size (50GB) –
ProvisioningType Thin
```

The following example creates a virtual disk named *VirtualDisk1* on a storage pool named *StoragePool1*. The virtual disk uses three-way mirroring and is a fixed size of 20 GB.

> **NOTE**
> You must have at least five physical disks in the storage pool for this cmdlet to work. (This does not include any disks that are allocated as hot spares.)

```
New-VirtualDisk -StoragePoolFriendlyName StoragePool1 -FriendlyName VirtualDisk1 -ResiliencySettingName Mirror
-NumberOfDataCopies 3 -Size 20GB -ProvisioningType Fixed
```

## Step 3: Create a volume

Next, you must create a volume from the virtual disk. You can assign an optional drive letter or folder, then format the volume with a file system.

1. If the New Volume Wizard is not already open, on the **Storage Pools** page in Server Manager, under **VIRTUAL DISKS**, right-click the desired virtual disk, and then select **New Volume**.

   The New Volume Wizard opens.

2. On the **Before you begin** page, select **Next**.
3. On the **Select the server and disk** page, do the following, and then select **Next**.
   a. In the **Server** area, select the server on which you want to provision the volume.
   b. In the **Disk** area, select the virtual disk on which you want to create the volume.
4. On the **Specify the size of the volume** page, enter a volume size, specify the units (**MB**, **GB**, or **TB**), and then select **Next**.
5. On the **Assign to a drive letter or folder** page, configure the desired option, and then select **Next**.
6. On the **Select file system settings** page, do the following, and then select **Next**.
   a. In the **File system** list, select either **NTFS** or **ReFS**.
   b. In the **Allocation unit size** list, either leave the setting at **Default** or set the allocation unit size.

   > **NOTE**
   > For more information about allocation unit size, see Default cluster size for NTFS, FAT, and exFAT.

c. Optionally, in the **Volume label** box, enter a volume label name, for example **HR Data**.

7. On the **Confirm selections** page, verify that the settings are correct, and then select **Create**.
8. On the **View results** page, verify that all tasks completed, and then select **Close**.
9. To verify that the volume was created, in Server Manager, select the **Volumes** page. The volume is listed under the server where it was created. You can also verify that the volume is in Windows Explorer.

**Windows PowerShell equivalent commands for creating volumes**

The following Windows PowerShell cmdlet performs the same function as the previous procedure. Enter the command on a single line.

The following example initializes the disks for virtual disk *VirtualDisk1*, creates a partition with an assigned drive letter, and then formats the volume with the default NTFS file system.

```
Get-VirtualDisk –FriendlyName VirtualDisk1 | Get-Disk | Initialize-Disk –Passthru | New-Partition –
AssignDriveLetter –UseMaximumSize | Format-Volume
```

## Additional information

- Storage Spaces
- Storage Cmdlets in Windows PowerShell
- Deploy Clustered Storage Spaces
- Windows Server storage forum

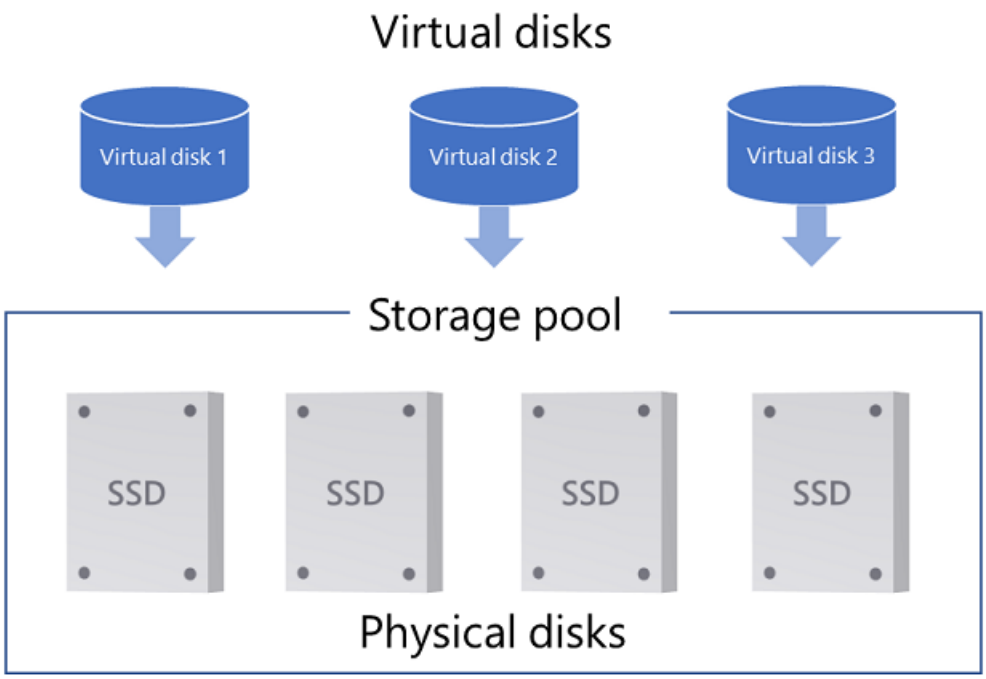
# Troubleshoot Storage Spaces and Storage Spaces Direct health and operational states

12/16/2020 • 14 minutes to read • Edit Online

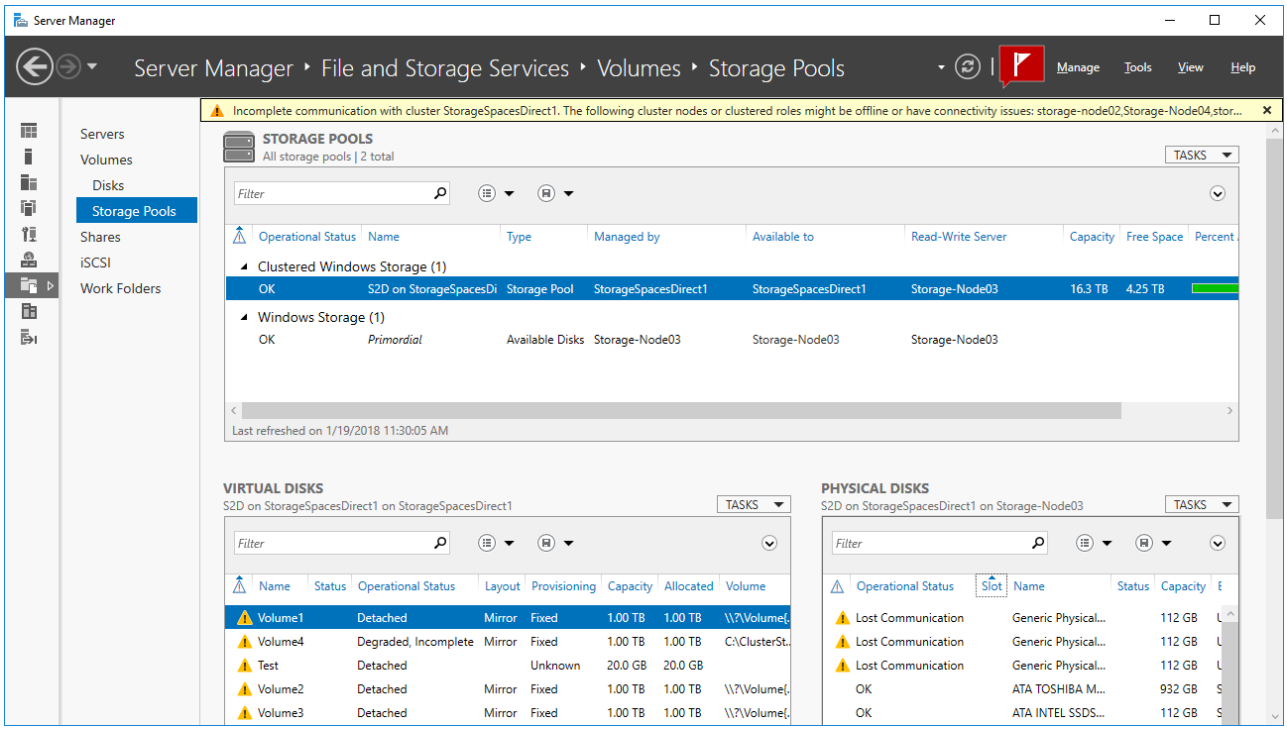
Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server (Semi-Annual Channel), Windows 10, Windows 8.1

This topic describes the health and operational states of storage pools, virtual disks (which sit underneath volumes in Storage Spaces), and drives in Storage Spaces Direct and Storage Spaces. These states can be invaluable when trying to troubleshoot various issues such as why you can't delete a virtual disk because of a read-only configuration. It also discusses why a drive can't be added to a pool (the CannotPoolReason).

Storage Spaces has three primary objects - *physical disks* (hard drives, SSDs, etc.) that are added to a *storage pool*, virtualizing the storage so that you can create *virtual disks* from free space in the pool, as shown here. Pool metadata is written to each drive in the pool. Volumes are created on top of the virtual disks and store your files, but we're not going to talk about volumes here.




You can view health and operational states in Server Manager, or with PowerShell. Here's an example of a variety of (mostly bad) health and operational states on a Storage Spaces Direct cluster that's missing most of its cluster nodes (right-click the column headers to add **Operational Status**). This isn't a happy cluster.




# Storage pool states

Every storage pool has a health status - **Healthy**, **Warning**, or **Unknown/Unhealthy**, as well as one or more operational states.

To find out what state a pool is in, use the following PowerShell commands:

```
Get-StoragePool -IsPrimordial $False | Select-Object HealthStatus, OperationalStatus, ReadOnlyReason
```

Here's an example output showing a storage pool in the Unknown health state with the Read-only operational status:

```
FriendlyName                OperationalStatus HealthStatus IsPrimordial IsReadOnly
------------                ----------------- ------------ ------------ ----------
S2D on StorageSpacesDirect1 Read-only         Unknown      False        True
```

The following sections list the health and operational states.

### Pool health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
|---|---|
| OK | The storage pool is healthy. |

### Pool health state: Warning

When the storage pool is in the **Warning** health state, it means that the pool is accessible, but one or more drives failed or are missing. As a result, your storage pool might have reduced resilience.

| OPERATIONAL STATE | DESCRIPTION |
|---|---|

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Degraded | There are failed or missing drives in the storage pool. This condition occurs only with drives hosting pool metadata.<br><br>**Action**: Check the state of your drives and replace any failed drives before there are additional failures. |

### Pool health state: Unknown or Unhealthy

When a storage pool is in the **Unknown** or **Unhealthy** health state, it means that the storage pool is read-only and can't be modified until the pool is returned to the **Warning** or **OK** health states.

| OPERATIONAL STATE | READ-ONLY REASON | DESCRIPTION |
| --- | --- | --- |
| Read-only | Incomplete | This can occur if the storage pool loses its quorum, which means that most drives in the pool have failed or are offline for some reason. When a pool loses its quorum, Storage Spaces automatically sets the pool configuration to read-only until enough drives become available again.<br><br>**Action:**<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring all servers online.<br>2. Set the pool back to read-write by opening a PowerShell session with administrative permissions and then typing:<br><br>`Get-StoragePool -IsPrimordial $False \| Set-StoragePool -IsReadOnly $false` |
| | Policy | An administrator set the storage pool to read-only.<br><br>**Action:** To set a clustered storage pool to read-write access in Failover Cluster Manager, go to **Pools**, right-click the pool and then select **Bring Online**.<br><br>For other servers and PCs, open a PowerShell session with administrative permissions and then type:<br><br>`Get-StoragePool \| Set-StoragePool -IsReadOnly $false` |

| OPERATIONAL STATE | READ-ONLY REASON | DESCRIPTION |
| --- | --- | --- |
| | Starting | Storage Spaces is starting or waiting for drives to be connected in the pool. This should be a temporary state. Once completely started, the pool should transition to a different operational state.<br><br>**Action:** If the pool stays in the *Starting* state, make sure that all drives in the pool are connected properly. |

See also, the Windows Server storage forum.

# Virtual disk states

In Storage Spaces, volumes are placed on virtual disks (storage spaces) that are carved out of free space in a pool. Every virtual disk has a health status - **Healthy**, **Warning**, **Unhealthy**, or **Unknown** as well as one or more operational states.

To find out what state virtual disks are in, use the following PowerShell commands:

```
Get-VirtualDisk | Select-Object FriendlyName,HealthStatus, OperationalStatus, DetachedReason
```

Here's an example of output showing a detached virtual disk and a degraded/incomplete virtual disk:

```
FriendlyName HealthStatus OperationalStatus      DetachedReason
------------ ------------ -----------------      --------------
Volume1      Unknown      Detached               By Policy
Volume2      Warning      {Degraded, Incomplete} None
```

The following sections list the health and operational states.

### Virtual disk health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| OK | The virtual disk is healthy. |
| Suboptimal | Data isn't written evenly across drives.<br><br>**Action**: Optimize drive usage in the storage pool by running the Optimize-StoragePool cmdlet. |

### Virtual disk health state: Warning

When the virtual disk is in a **Warning** health state, it means that one or more copies of your data are unavailable, but Storage Spaces can still read at least one copy of your data.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| In service | Windows is repairing the virtual disk, such as after adding or removing a drive. When the repair is complete, the virtual disk should return to the OK health state. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Incomplete | The resilience of the virtual disk is reduced because one or more drives failed or are missing. However, the missing drives contain up-to-date copies of your data.<br><br>**Action**:<br>1. Reconnect any missing drives, replace any failed drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive. |
| Degraded | The resilience of the virtual disk is reduced because one or more drives failed or are missing, and there are outdated copies of your data on these drives.<br><br>**Action**:<br>1. Reconnect any missing drives, replace any failed drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive. |

### Virtual disk health state: Unhealthy

When a virtual disk is in an **Unhealthy** health state, some or all of the data on the virtual disk is currently inaccessible.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| No redundancy | The virtual disk has lost data because too many drives failed.<br><br>**Action**: Replace failed drives and then restore your data from backup. |

### Virtual disk health state: Information/Unknown

The virtual disk can also be in the **Information** health state (as shown in the Storage Spaces Control Panel item) or **Unknown** health state (as shown in PowerShell) if an administrator took the virtual disk offline or the virtual disk has become detached.

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
| --- | --- | --- |

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
| --- | --- | --- |
| Detached | By Policy | An administrator took the virtual disk offline, or set the virtual disk to require manual attachment, in which case you'll have to manually attach the virtual disk every time Windows restarts.,<br><br>**Action**: Bring the virtual disk back online. To do so when the virtual disk is in a clustered storage pool, in Failover Cluster Manager select **Storage** > **Pools** > **Virtual Disks**, select the virtual disk that shows the **Offline** status and then select **Bring Online**.<br><br>To bring a virtual disk back online when not in a cluster, open a PowerShell session as an Administrator and then try using the following command:<br><br>`Get-VirtualDisk \| Where-Object -Filter { $_.OperationalStatus -eq "Detached" } \| Connect-VirtualDisk`<br><br>To automatically attach all non-clustered virtual disks after Windows restarts, open a PowerShell session as an Administrator and then use the following command:<br><br>`Get-VirtualDisk \| Set-VirtualDisk -ismanualattach $false` |
| | Majority Disks Unhealthy | Too many drives used by this virtual disk failed, are missing, or have stale data.<br><br>**Action**:<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. After all drives and servers are online, replace any failed drives. See Health Service for details.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive.<br>3. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br><br>If more disks failed than you have copies of your data and the virtual disk wasn't repaired in-between failures, all data on the virtual disk is permanently lost. In this unfortunate case, delete the virtual disk, create a new virtual disk, and then restore from a backup. |

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
| --- | --- | --- |
| | Incomplete | Not enough drives are present to read the virtual disk.<br><br>**Action**:<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. After all drives and servers are online, replace any failed drives. See Health Service for details.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive.<br>3. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br><br>If more disks failed than you have copies of your data and the virtual disk wasn't repaired in-between failures, all data on the virtual disk is permanently lost. In this unfortunate case, delete the virtual disk, create a new virtual disk, and then restore from a backup. |
| | Timeout | Attaching the virtual disk took too long<br><br>**Action:** This shouldn't happen often, so you might try see if the condition passes in time. Or you can try disconnecting the virtual disk with the Disconnect-VirtualDisk cmdlet, then using the Connect-VirtualDisk cmdlet to reconnect it. |

## Drive (physical disk) states

The following sections describe the health states a drive can be in. Drives in a pool are represented in PowerShell as *physical disk* objects.

### Drive health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| OK | The drive is healthy. |
| In service | The drive is performing some internal housekeeping operations. When the action is complete, the drive should return to the *OK* health state. |

### Drive health state: Warning

A drive in the Warning state can read and write data successfully but has an issue.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Lost communication | The drive is missing. If you're using Storage Spaces Direct, this could be because a server is down.<br><br>**Action**: If you're using Storage Spaces Direct, bring all servers back online. If that doesn't fix it, reconnect the drive, replace it, or try getting detailed diagnostic info about this drive by following the steps in Troubleshooting using Windows Error Reporting > Physical disk timed out. |
| Removing from pool | Storage Spaces is in the process of removing the drive from its storage pool.<br><br>This is a temporary state. After the removal is complete, if the drive is still attached to the system, the drive transitions to another operational state (usually OK) in a primordial pool. |
| Starting maintenance mode | Storage Spaces is in the process of putting the drive in maintenance mode after an administrator put the drive in maintenance mode. This is a temporary state - the drive should soon be in the *In maintenance mode* state. |
| In maintenance mode | An administrator placed the drive in maintenance mode, halting reads and writes from the drive. This is usually done before updating drive firmware, or when testing failures.<br><br>**Action**: To take the drive out of maintenance mode, use the Disable-StorageMaintenanceMode cmdlet. |
| Stopping maintenance mode | An administrator took the drive out of maintenance mode, and Storage Spaces is in the process of bringing the drive back online. This is a temporary state - the drive should soon be in another state - ideally *Healthy*. |
| Predictive failure | The drive reported that it's close to failing.<br><br>**Action**: Replace the drive. |
| IO error | There was a temporary error accessing the drive.<br><br>**Action**:<br>1. If the drive doesn't transition back to the **OK** state, you can try using the Reset-PhysicalDisk cmdlet to wipe the drive.<br>2. Use Repair-VirtualDisk to restore the resiliency of affected virtual disks.<br>3. If this keeps happening, replace the drive. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Transient error | There was a temporary error with the drive. This usually means the drive was unresponsive, but it could also mean that the Storage Spaces protective partition was inappropriately removed from the drive.<br><br>**Action**:<br>1. If the drive doesn't transition back to the **OK** state, you can try using the Reset-PhysicalDisk cmdlet to wipe the drive.<br>2. Use Repair-VirtualDisk to restore the resiliency of affected virtual disks.<br>3. If this keeps happening, replace the drive, or try getting detailed diagnostic info about this drive by following the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Abnormal latency | The drive is performing slowly, as measured by the Health Service in Storage Spaces Direct.<br><br>**Action**: If this keeps happening, replace the drive so it doesn't reduce the performance of Storage Spaces as a whole. |

### Drive health state: Unhealthy

A drive in the Unhealthy state can't currently be written to or accessed.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Not usable | This drive can't be used by Storage Spaces. For more info see Storage Spaces Direct hardware requirements; if you're not using Storage Spaces Direct, see Storage Spaces overview. |
| Split | The drive has become separated from the pool.<br><br>**Action**: Reset the drive, erasing all data from the drive and adding it back to the pool as an empty drive. To do so, open a PowerShell session as an administrator, run the Reset-PhysicalDisk cmdlet, and then run Repair-VirtualDisk.<br><br>To get detailed diagnostic info about this drive, follow the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Stale metadata | Storage Spaces found old metadata on the drive.<br><br>**Action**: This should be a temporary state. If the drive doesn't transition back to OK, you can run Repair-VirtualDisk to start a repair operation on affected virtual disks. If that doesn't resolve the issue, you can reset the drive with the Reset-PhysicalDisk cmdlet, wiping all data from the drive, and then run Repair-VirtualDisk. |
| Unrecognized metadata | Storage Spaces found unrecognized metadata on the drive, which usually means that the drive has metadata from a different pool on it.<br><br>**Action**: To wipe the drive and add it to the current pool, reset the drive. To reset the drive, open a PowerShell session as an administrator, run the Reset-PhysicalDisk cmdlet, and then run Repair-VirtualDisk. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Failed media | The drive failed and won't be used by Storage Spaces anymore.<br><br>**Action**: Replace the drive.<br><br>To get detailed diagnostic info about this drive, follow the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Device hardware failure | There was a hardware failure on this drive.<br><br>**Action**: Replace the drive. |
| Updating firmware | Windows is updating the firmware on the drive. This is a temporary state that usually lasts less than a minute and during which time other drives in the pool handle all reads and writes. For more info, see Update drive firmware. |
| Starting | The drive is getting ready for operation. This should be a temporary state - once complete, the drive should transition to a different operational state. |

## Reasons a drive can't be pooled

Some drives just aren't ready to be in a storage pool. You can find out why a drive isn't eligible for pooling by looking at the `CannotPoolReason` property of a physical disk. Here's an example PowerShell script to display the CannotPoolReason property:

```
Get-PhysicalDisk | Format-Table FriendlyName,MediaType,Size,CanPool,CannotPoolReason
```

Here's an example output:

```
FriendlyName          MediaType          Size CanPool CannotPoolReason
------------          ---------          ---- ------- ----------------
ATA MZ7LM120HCFD00D3  SSD        120034123776   False Insufficient Capacity
Msft Virtual Disk     SSD         10737418240    True
Generic Physical Disk SSD        119990648832   False In a Pool
```

The following table gives a little more detail on each of the reasons.

| REASON | DESCRIPTION |
| --- | --- |

| REASON | DESCRIPTION |
| --- | --- |
| In a pool | The drive already belongs to a storage pool.<br><br>Drives can belong to only a single storage pool at a time. To use this drive in another storage pool, first remove the drive from its existing pool, which tells Storage Spaces to move the data on the drive to other drives on the pool. Or reset the drive if the drive has been disconnected from its pool without notifying Storage Spaces.<br><br>To safely remove a drive from a storage pool, use Remove-PhysicalDisk, or go to Server Manager > **File and Storage Services** > **Storage Pools**, > **Physical Disks**, right-click the drive and then select **Remove Disk**.<br><br>To reset a drive, use Reset-PhysicalDisk. |
| Not healthy | The drive isn't in a healthy state and might need to be replaced. |
| Removable media | The drive is classified as a removable drive.<br><br>Storage Spaces doesn't support media that are recognized by Windows as removable, such as Blu-Ray drives. Although many fixed drives are in removable slots, in general, media that are *classified* by Windows as removable aren't suitable for use with Storage Spaces. |
| In use by cluster | The drive is currently used by a Failover Cluster. |
| Offline | The drive is offline.<br><br>To bring all offline drives online and set to read/write, open a PowerShell session as an administrator and use the following scripts:<br><br>`Get-Disk \| Where-Object -Property OperationalStatus -EQ "Offline" \| Set-Disk -IsOffline $false`<br><br>`Get-Disk \| Where-Object -Property IsReadOnly -EQ $true \| Set-Disk -IsReadOnly $false` |
| Insufficient capacity | This typically occurs when there are partitions taking up the free space on the drive.<br><br>**Action**: Delete any volumes on the drive, erasing all data on the drive. One way to do that is to use the Clear-Disk PowerShell cmdlet. |
| Verification in progress | The Health Service is checking to see if the drive or firmware on the drive is approved for use by the server administrator. |
| Verification failed | The Health Service couldn't check to see if the drive or firmware on the drive is approved for use by the server administrator. |
| Firmware not compliant | The firmware on the physical drive isn't in the list of approved firmware revisions specified by the server administrator by using the Health Service. |

| REASON | DESCRIPTION |
| --- | --- |
| Hardware not compliant | The drive isn't in the list of approved storage models specified by the server administrator by using the Health Service. |

## Additional References

- Storage Spaces Direct
- Storage Spaces Direct hardware requirements
- Understanding cluster and pool quorum

# Storage Spaces Direct overview

12/16/2020 • 7 minutes to read • Edit Online

Applies to: Azure Stack HCI, Windows Server 2019, Windows Server 2016

Storage Spaces Direct uses industry-standard servers with local-attached drives to create highly available, highly scalable software-defined storage at a fraction of the cost of traditional SAN or NAS arrays. Its converged or hyper-converged architecture radically simplifies procurement and deployment, while features such as caching, storage tiers, and erasure coding, together with the latest hardware innovations such as RDMA networking and NVMe drives, deliver unrivaled efficiency and performance.

Storage Spaces Direct is included in Azure Stack HCI, Windows Server 2019 Datacenter, Windows Server 2016 Datacenter, and Windows Server Insider Preview Builds.

For other applications of Storage Spaces, such as shared SAS clusters and stand-alone servers, see Storage Spaces overview. If you're looking for info about using Storage Spaces on a Windows 10 PC, see Storage Spaces in Windows 10.

| DESCRIPTION | DOCUMENTATION |
| --- | --- |
| **Understand**<br>• Overview (you are here)<br>• Understand the cache<br>• Fault tolerance and storage efficiency<br>• Drive symmetry considerations<br>• Understand and monitor storage resync<br>• Understanding cluster and pool quorum<br>• Cluster sets | **Plan**<br>• Hardware requirements<br>• Using the CSV in-memory read cache<br>• Choose drives<br>• Plan volumes<br>• Using guest VM clusters<br>• Disaster recovery |
| **Deploy**<br>• Deploy Storage Spaces Direct<br>• Create volumes<br>• Nested resiliency<br>• Configure quorum<br>• Upgrade a Storage Spaces Direct cluster to Windows Server 2019<br>• Understand and deploy persistent memory | **Manage**<br>• Manage with Windows Admin Center<br>• Add servers or drives<br>• Taking a server offline for maintenance<br>• Remove servers<br>• Extend volumes<br>• Delete volumes<br>• Update drive firmware<br>• Performance history<br>• Delimit the allocation of volumes<br>• Use Azure Monitor on a hyper-converged cluster |
| **Troubleshooting**<br>• Troubleshooting scenarios<br>• Troubleshoot health and operational states<br>• Collect diagnostic data with Storage Spaces Direct<br>• Storage-class memory health management | **Recent blog posts**<br>• 13.7 million IOPS with Storage Spaces Direct: the new industry record for hyper-converged infrastructure<br>• Hyper-converged infrastructure in Windows Server 2019 - the countdown clock starts now!<br>• Five big announcements from the Windows Server Summit<br>• 10,000 Storage Spaces Direct clusters and counting... |

# Videos

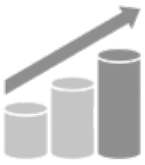
### Quick Video Overview (5 minutes)

### Storage Spaces Direct at Microsoft Ignite 2018 (1 hour)

### Storage Spaces Direct at Microsoft Ignite 2017 (1 hour)

### Launch Event at Microsoft Ignite 2016 (1 hour)

# Key benefits

| IMAGE | DESCRIPTION |
| --- | --- |
|   | **Simplicity.** Go from industry-standard servers running Windows Server 2016 to your first Storage Spaces Direct cluster in under 15 minutes. For System Center users, deployment is just one checkbox. |
|  | **Unrivaled Performance.** Whether all-flash or hybrid, Storage Spaces Direct easily exceeds 150,000 mixed 4k random IOPS per server with consistent, low latency thanks to its hypervisor-embedded architecture, its built-in read/write cache, and support for cutting-edge NVMe drives mounted directly on the PCIe bus. |
|  | **Fault Tolerance.** Built-in resiliency handles drive, server, or component failures with continuous availability. Larger deployments can also be configured for chassis and rack fault tolerance. When hardware fails, just swap it out; the software heals itself, with no complicated management steps. |
|  | **Resource Efficiency.** Erasure coding delivers up to 2.4x greater storage efficiency, with unique innovations like Local Reconstruction Codes and ReFS real-time tiers to extend these gains to hard disk drives and mixed hot/cold workloads, all while minimizing CPU consumption to give resources back to where they're needed most - the VMs. |

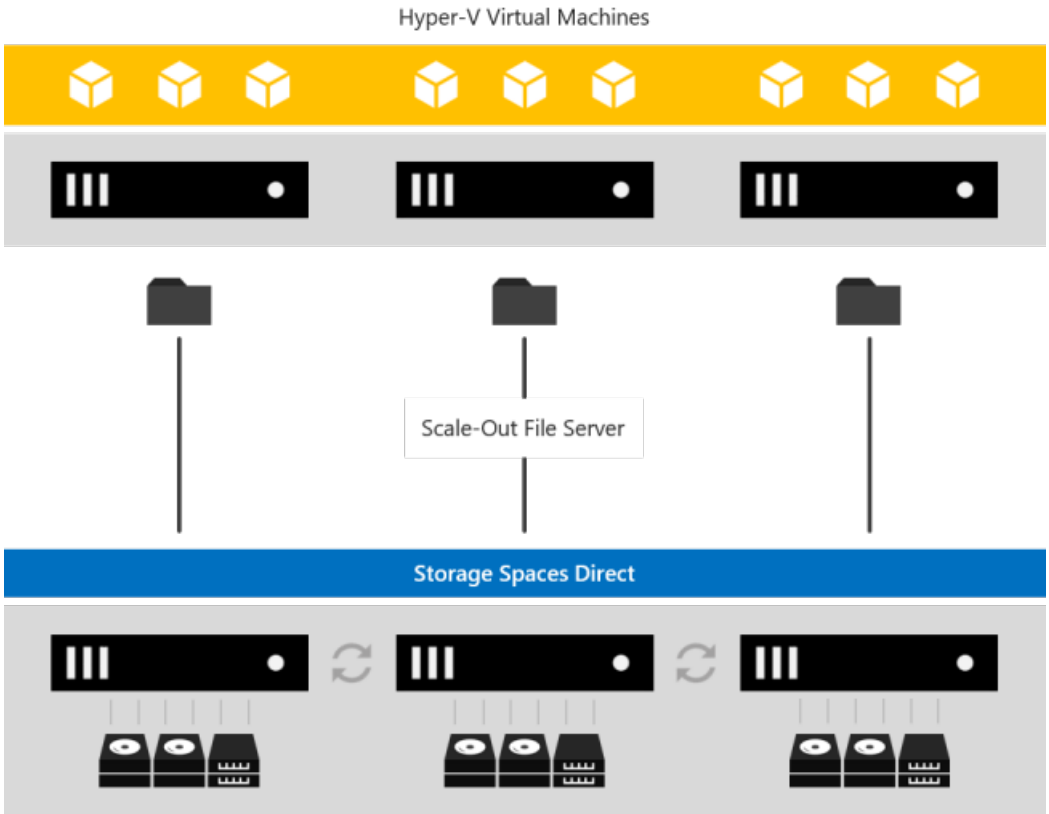
| IMAGE | DESCRIPTION |
| --- | --- |
|  | **Manageability**. Use Storage QoS Controls to keep overly busy VMs in check with minimum and maximum per-VM IOPS limits. The Health Service provides continuous built-in monitoring and alerting, and new APIs make it easy to collect rich, cluster-wide performance and capacity metrics. |
|  | **Scalability**. Go up to 16 servers and over 400 drives, for up to 1 petabyte (1,000 terabytes) of storage per cluster. To scale out, simply add drives or add more servers; Storage Spaces Direct will automatically onboard new drives and begin using them. Storage efficiency and performance improve predictably at scale. |

## Deployment options

Storage Spaces Direct was designed for two distinct deployment options:

### Converged

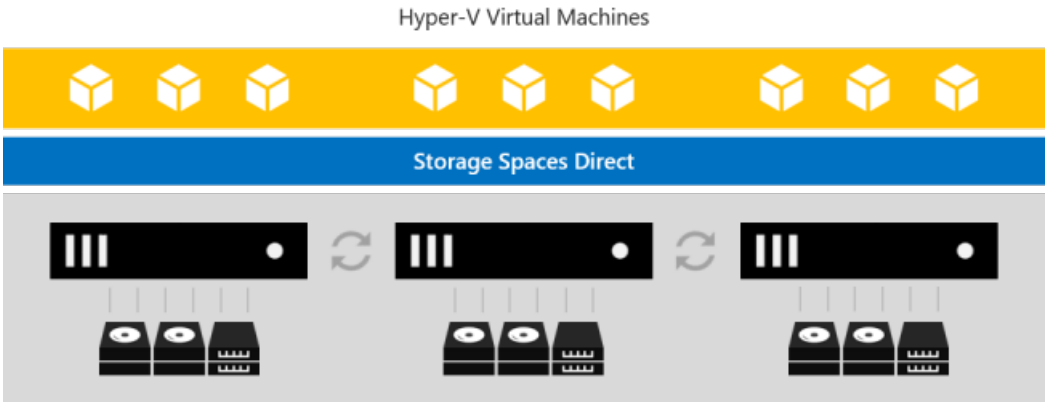
**Storage and compute in separate clusters.** The converged deployment option, also known as 'disaggregated', layers a Scale-out File Server (SoFS) atop Storage Spaces Direct to provide network-attached storage over SMB3 file shares. This allows for scaling compute/workload independently from the storage cluster, essential for larger-scale deployments such as Hyper-V IaaS (Infrastructure as a Service) for service providers and enterprises.




### Hyper-Converged

**One cluster for compute and storage.** The hyper-converged deployment option runs Hyper-V virtual machines or SQL Server databases directly on the servers providing the storage, storing their files on the

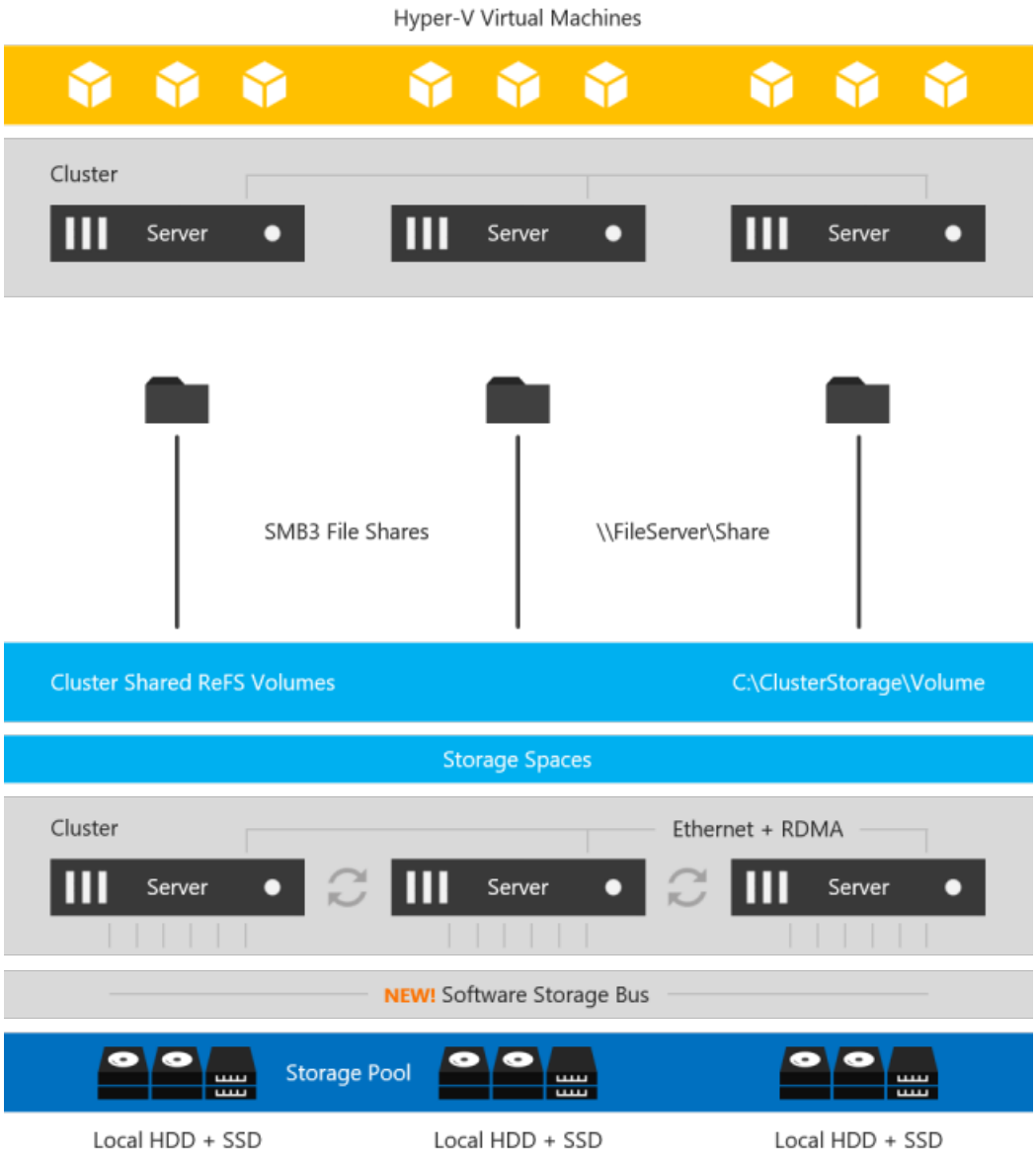
local volumes. This eliminates the need to configure file server access and permissions, and reduces hardware costs for small-to-medium business or remote office/branch office deployments. See Deploy Storage Spaces Direct.




## How it works

Storage Spaces Direct is the evolution of Storage Spaces, first introduced in Windows Server 2012. It leverages many of the features you know today in Windows Server, such as Failover Clustering, the Cluster Shared Volume (CSV) file system, Server Message Block (SMB) 3, and of course Storage Spaces. It also introduces new technology, most notably the Software Storage Bus.

Here's an overview of the Storage Spaces Direct stack:




**Networking Hardware.** Storage Spaces Direct uses SMB3, including SMB Direct and SMB Multichannel, over Ethernet to communicate between servers. We strongly recommend 10+ GbE with remote-direct memory access (RDMA), either iWARP or RoCE.

**Storage Hardware.** From 2 to 16 servers with local-attached SATA, SAS, or NVMe drives. Each server must have at least 2 solid-state drives, and at least 4 additional drives. The SATA and SAS devices should be behind a host-bus adapter (HBA) and SAS expander. We strongly recommend the meticulously engineered and extensively validated platforms from our partners (coming soon).

**Failover Clustering.** The built-in clustering feature of Windows Server is used to connect the servers.

**Software Storage Bus.** The Software Storage Bus is new in Storage Spaces Direct. It spans the cluster and establishes a software-defined storage fabric whereby all the servers can see all of each other's local drives. You can think of it as replacing costly and restrictive Fibre Channel or Shared SAS cabling.

**Storage Bus Layer Cache.** The Software Storage Bus dynamically binds the fastest drives present (e.g. SSD) to slower drives (e.g. HDDs) to provide server-side read/write caching that accelerates IO and boosts throughput.

**Storage Pool.** The collection of drives that form the basis of Storage Spaces is called the storage pool. It is automatically created, and all eligible drives are automatically discovered and added to it. We strongly recommend you use one pool per cluster, with the default settings. Read our Deep Dive into the Storage Pool to learn more.

**Storage Spaces.** Storage Spaces provides fault tolerance to virtual "disks" using mirroring, erasure coding, or both. You can think of it as distributed, software-defined RAID using the drives in the pool. In Storage Spaces Direct, these virtual disks typically have resiliency to two simultaneous drive or server failures (e.g. 3-way mirroring, with each data copy in a different server) though chassis and rack fault tolerance is also available.

**Resilient File System (ReFS).** ReFS is the premier filesystem purpose-built for virtualization. It includes dramatic accelerations for .vhdx file operations such as creation, expansion, and checkpoint merging, and built-in checksums to detect and correct bit errors. It also introduces real-time tiers that rotate data between so-called "hot" and "cold" storage tiers in real-time based on usage.

**Cluster Shared Volumes.** The CSV file system unifies all the ReFS volumes into a single namespace accessible through any server, so that to each server, every volume looks and acts like it's mounted locally.

**Scale-Out File Server.** This final layer is necessary in converged deployments only. It provides remote file access using the SMB3 access protocol to clients, such as another cluster running Hyper-V, over the network, effectively turning Storage Spaces Direct into network-attached storage (NAS).

## Customer stories

There are over 10,000 clusters worldwide running Storage Spaces Direct. Organizations of all sizes, from small businesses deploying just two nodes, to large enterprises and governments deploying hundreds of nodes, depend on Storage Spaces Direct for their critical applications and infrastructure.

Visit Microsoft.com/HCI to read their stories:


## Management tools

The following tools can be used to manage and/or monitor Storage Spaces Direct:

| NAME | GRAPHICAL OR COMMAND-LINE? | PAID OR INCLUDED? |
|---|---|---|
| Windows Admin Center | Graphical | Included |
| Server Manager & Failover Cluster Manager | Graphical | Included |

| NAME | GRAPHICAL OR COMMAND-LINE? | PAID OR INCLUDED? |
| --- | --- | --- |
| Windows PowerShell | Command-line | Included |
| System Center Virtual Machine Manager (SCVMM) & Operations Manager (SCOM) | Graphical | Paid |

## Get started

Try Storage Spaces Direct in Microsoft Azure, or download a 180-day-licensed evaluation copy of Windows Server from Windows Server Evaluations.

## Additional References

- Fault tolerance and storage efficiency
- Storage Replica
- Storage at Microsoft blog
- Storage Spaces Direct throughput with iWARP (TechNet blog)
- What's New in Failover Clustering in Windows Server
- Storage Quality of Service
- Windows IT Pro Support

# Understanding the cache in Storage Spaces Direct

12/16/2020 • 10 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Storage Spaces Direct features a built-in server-side cache to maximize storage performance. It is a large, persistent, real-time read *and* write cache. The cache is configured automatically when Storage Spaces Direct is enabled. In most cases, no manual management whatsoever is required. How the cache works depends on the types of drives present.

The following video goes into details on how caching works for Storage Spaces Direct, as well as other design considerations.

**Storage Spaces Direct design considerations**
(20 minutes)

https://channel9.msdn.com/Blogs/windowsserver/Design-Considerations-for-Storage-Spaces-Direct/player

## Drive types and deployment options

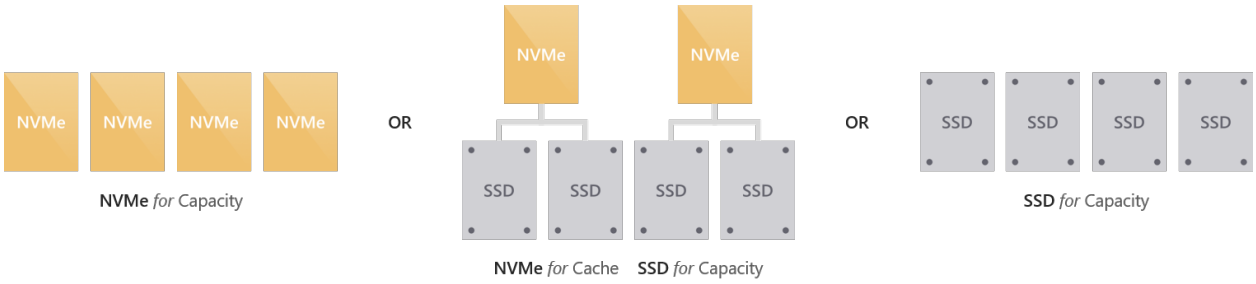
Storage Spaces Direct currently works with four types of storage devices:

| TYPE OF DRIVE | DESCRIPTION |
|---|---|
|  | **PMem** refers to persistent memory, a new type of low latency, high performance storage. |
|  | **NVMe** (Non-Volatile Memory Express) refers to solid-state drives that sit directly on the PCIe bus. Common form factors are 2.5" U.2, PCIe Add-In-Card (AIC), and M.2. NVMe offers higher IOPS and IO throughput with lower latency than any other type of drive we support today except PMem. |
|  | **SSD** refers to solid-state drives, which connect via conventional SATA or SAS. |
|  | **HDD** refers to rotational, magnetic hard disk drives, which offer vast storage capacity. |

These can be combined in various ways, which we group into two categories: "all-flash" and "hybrid".

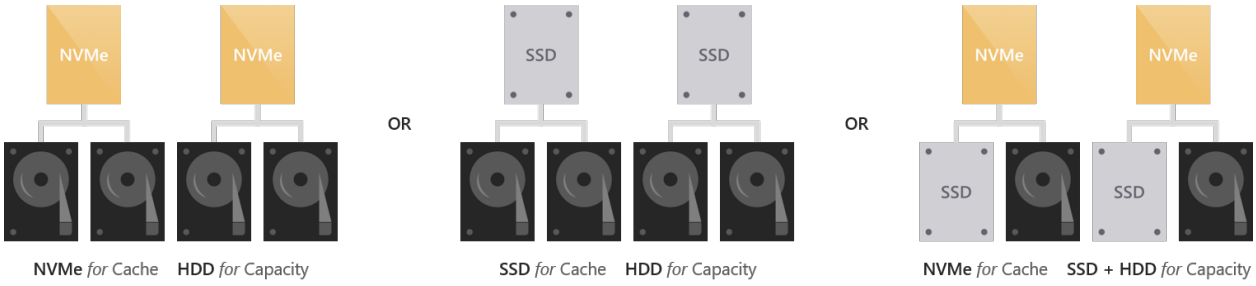
### All-flash deployment possibilities

All-flash deployments aim to maximize storage performance and do not include rotational hard disk drives (HDD).




### Hybrid deployment possibilities

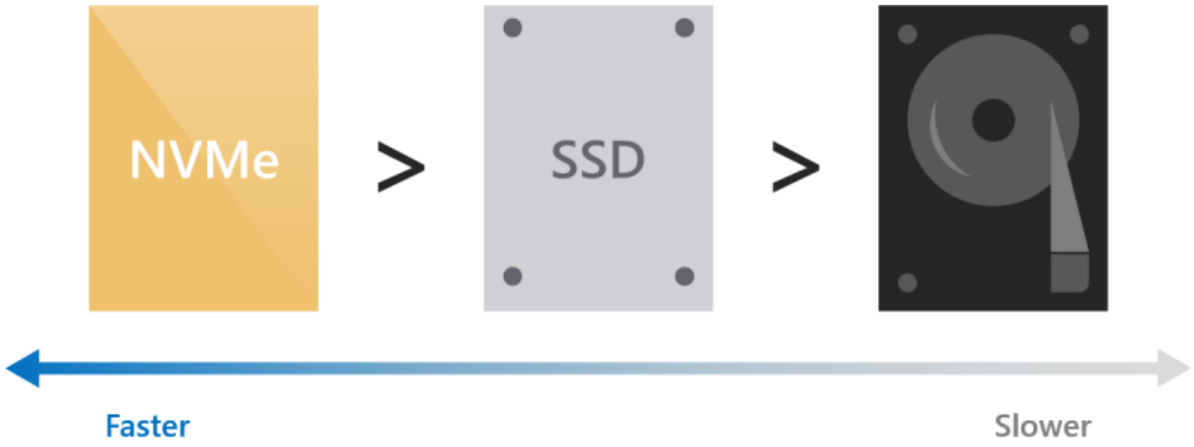
Hybrid deployments aim to balance performance and capacity or to maximize capacity and do include rotational hard disk drives (HDD).




## Cache drives are selected automatically

In deployments with multiple types of drives, Storage Spaces Direct automatically uses all drives of the "fastest" type for caching. The remaining drives are used for capacity.

Which type is "fastest" is determined according to the following hierarchy.




For example, if you have NVMe and SSDs, the NVMe will cache for the SSDs.

If you have SSDs and HDDs, the SSDs will cache for the HDDs.

> **NOTE**
> Cache drives do not contribute usable storage capacity. All data stored in the cache is also stored elsewhere, or will be once it de-stages. This means the total raw storage capacity of your deployment is the sum of your capacity drives only.

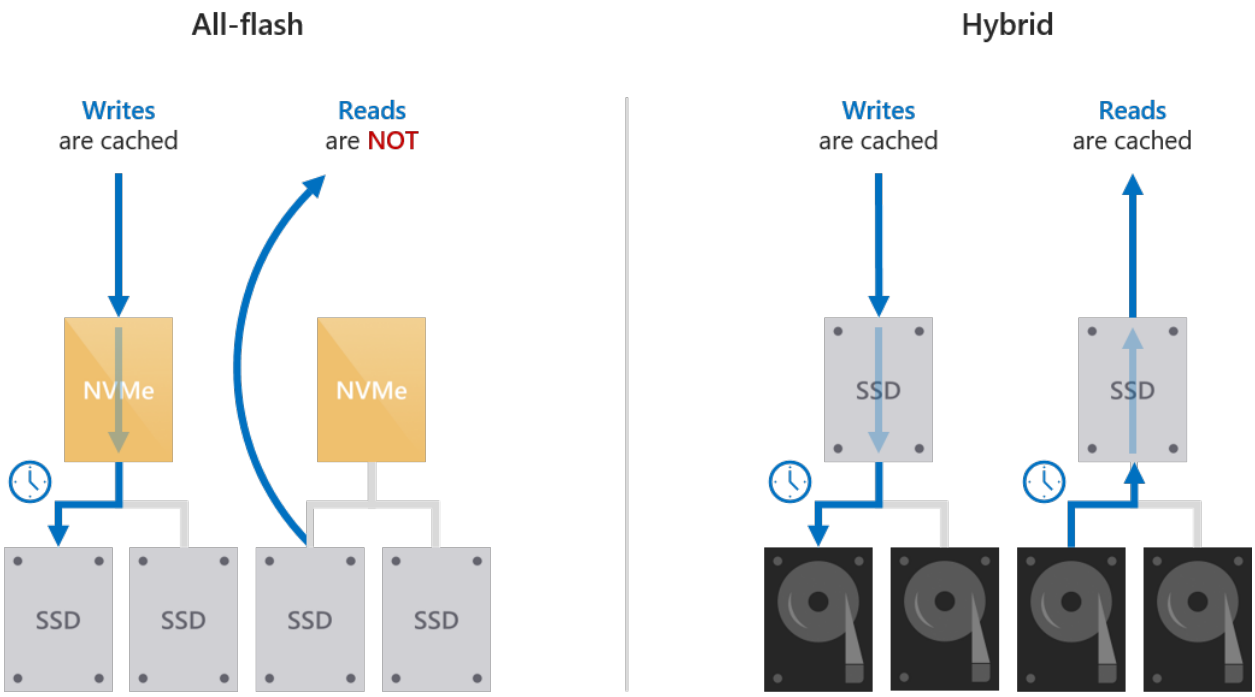
When all drives are of the same type, no cache is configured automatically. You have the option to manually configure higher-endurance drives to cache for lower-endurance drives of the same type – see the Manual configuration section to learn how.

**TIP**

In all-NVMe or all-SSD deployments, especially at very small scale, having no drives "spent" on cache can improve storage efficiency meaningfully.

## Cache behavior is set automatically

The behavior of the cache is determined automatically based on the type(s) of drives that are being cached for. When caching for solid-state drives (such as NVMe caching for SSDs), only writes are cached. When caching for hard disk drives (such as SSDs caching for HDDs), both reads and writes are cached.




**Write-only caching for all-flash deployments**

When caching for solid-state drives (NVMe or SSDs), only writes are cached. This reduces wear on the capacity drives because many writes and re-writes can coalesce in the cache and then de-stage only as needed, reducing the cumulative traffic to the capacity drives and extending their lifetime. For this reason, we recommend selecting higher-endurance, write-optimized drives for the cache. The capacity drives may reasonably have lower write endurance.

Because reads do not significantly affect the lifespan of flash, and because solid-state drives universally offer low read latency, reads are not cached: they are served directly from the capacity drives (except when the data was written so recently that it has not yet been de-staged). This allows the cache to be dedicated entirely to writes, maximizing its effectiveness.

This results in write characteristics, such as write latency, being dictated by the cache drives, while read characteristics are dictated by the capacity drives. Both are consistent, predictable, and uniform.

**Read/write caching for hybrid deployments**

When caching for hard disk drives (HDDs), both reads *and* writes are cached, to provide flash-like latency (often ~10x better) for both. The read cache stores recently and frequently read data for fast access and to minimize random traffic to the HDDs. (Because of seek and rotational delays, the latency and lost time incurred by random access to an HDD is significant.) Writes are cached to absorb bursts and, as before, to coalesce writes and re-writes and minimize the cumulative traffic to the capacity drives.

Storage Spaces Direct implements an algorithm that de-randomizes writes before de-staging them, to emulate an IO pattern to disk that seems sequential even when the actual IO coming from the workload (such as virtual

machines) is random. This maximizes the IOPS and throughput to the HDDs.

**Caching in deployments with drives of all three types**

When drives of all three types are present, the NVMe drives provides caching for both the SSDs and the HDDs. The behavior is as described above: only writes are cached for the SSDs, and both reads and writes are cached for the HDDs. The burden of caching for the HDDs is distributed evenly among the cache drives.

## Summary

This table summarizes which drives are used for caching, which are used for capacity, and what the caching behavior is for each deployment possibility.

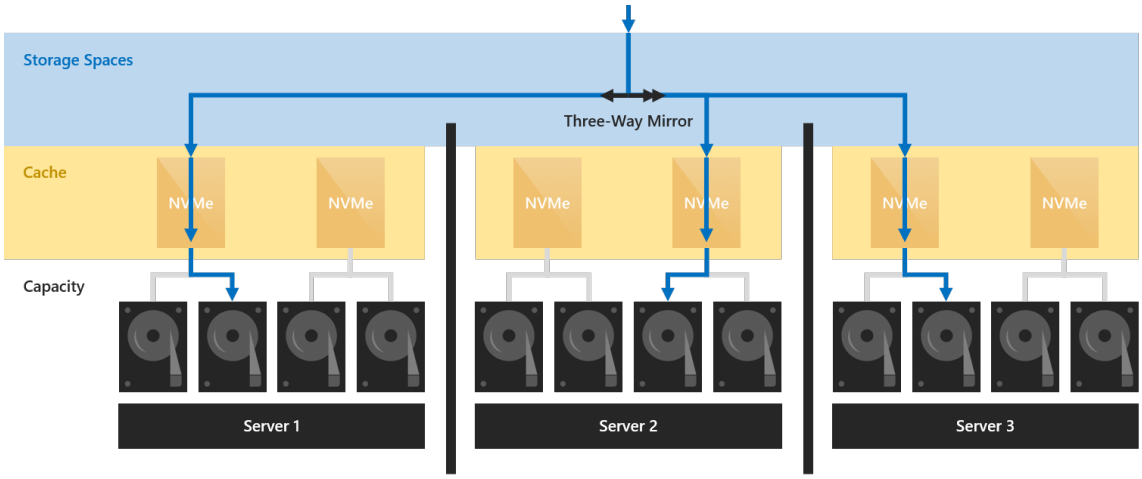
| DEPLOYMENT | CACHE DRIVES | CAPACITY DRIVES | CACHE BEHAVIOR (DEFAULT) |
|---|---|---|---|
| All NVMe | None (Optional: configure manually) | NVMe | Write-only (if configured) |
| All SSD | None (Optional: configure manually) | SSD | Write-only (if configured) |
| NVMe + SSD | NVMe | SSD | Write-only |
| NVMe + HDD | NVMe | HDD | Read + Write |
| SSD + HDD | SSD | HDD | Read + Write |
| NVMe + SSD + HDD | NVMe | SSD + HDD | Read + Write for HDD, Write-only for SSD |

## Server-side architecture

The cache is implemented at the drive level: individual cache drives within one server are bound to one or many capacity drives within the same server.

Because the cache is below the rest of the Windows software-defined storage stack, it does not have nor need any awareness of concepts such as Storage Spaces or fault tolerance. You can think of it as creating "hybrid" (part flash, part disk) drives which are then presented to Windows. As with an actual hybrid drive, the real-time movement of hot and cold data between the faster and slower portions of the physical media is nearly invisible to the outside.

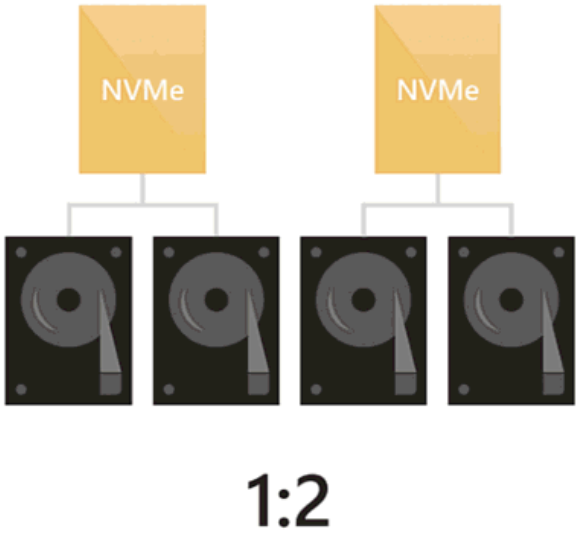
Given that resiliency in Storage Spaces Direct is at least server-level (meaning data copies are always written to different servers; at most one copy per server), data in the cache benefits from the same resiliency as data not in the cache.




For example, when using three-way mirroring, three copies of any data are written to different servers, where they land in cache. Regardless of whether they are later de-staged or not, three copies will always exist.

## Drive bindings are dynamic

The binding between cache and capacity drives can have any ratio, from 1:1 up to 1:12 and beyond. It adjusts dynamically whenever drives are added or removed, such as when scaling up or after failures. This means you can add cache drives or capacity drives independently, whenever you want.



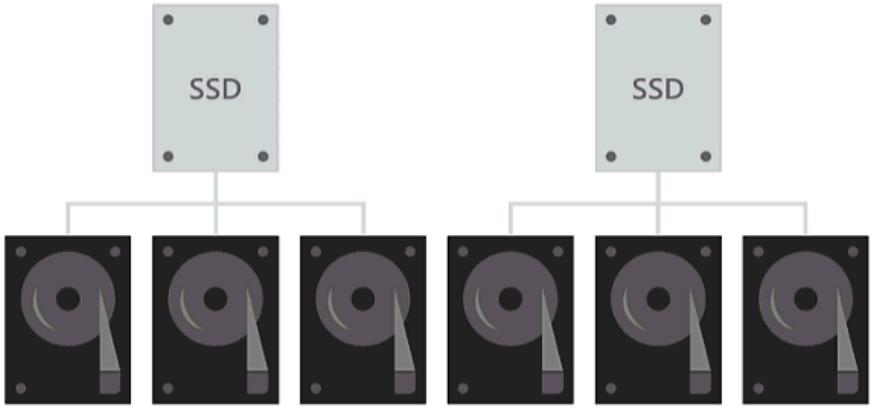

We recommend making the number of capacity drives a multiple of the number of cache drives, for symmetry. For example, if you have 4 cache drives, you will experience more even performance with 8 capacity drives (1:2 ratio) than with 7 or 9.

## Handling cache drive failures

When a cache drive fails, any writes which have not yet been de-staged are lost *to the local server*, meaning they exist only on the other copies (in other servers). Just like after any other drive failure, Storage Spaces can and does automatically recover by consulting the surviving copies.

For a brief period, the capacity drives which were bound to the lost cache drive will appear unhealthy. Once the cache rebinding has occurred (automatic) and the data repair has completed (automatic), they will resume showing as healthy.

This scenario is why at minimum two cache drives are required per server to preserve performance.




You can then replace the cache drive just like any other drive replacement.

> **NOTE**
> You may need to power down to safely replace NVMe that is Add-In Card (AIC) or M.2 form factor.

## Relationship to other caches

There are several other unrelated caches in the Windows software-defined storage stack. Examples include the Storage Spaces write-back cache and the Cluster Shared Volume (CSV) in-memory read cache.

With Storage Spaces Direct, the Storage Spaces write-back cache should not be modified from its default behavior. For example, parameters such as **-WriteCacheSize** on the **New-Volume** cmdlet should not be used.

You may choose to use the CSV cache, or not – it's up to you. It does not conflict with the cache described in this topic in any way. In certain scenarios it can provide valuable performance gains. For more information, see How to Enable CSV Cache.

## Manual configuration

For most deployments, manual configuration is not required. In case you do need it, see the following sections.

If you need to make changes to the cache device model after setup, edit the Health Service's Support Components Document, as described in Health Service overview.

### Specify cache drive model

In deployments where all drives are of the same type, such as all-NVMe or all-SSD deployments, no cache is configured because Windows cannot distinguish characteristics like write endurance automatically among drives of the same type.

To use higher-endurance drives to cache for lower-endurance drives of the same type, you can specify which drive model to use with the **-CacheDeviceModel** parameter of the **Enable-ClusterS2D** cmdlet. Once Storage Spaces Direct is enabled, all drives of that model will be used for caching.

> **TIP**
> Be sure to match the model string exactly as it appears in the output of **Get-PhysicalDisk**.

**Example**

First, get a list of physical disks:

```
Get-PhysicalDisk | Group Model -NoElement
```

Here's some example output:

```
Count Name
----- ----
    8 FABRIKAM NVME-1710
   16 CONTOSO NVME-1520
```

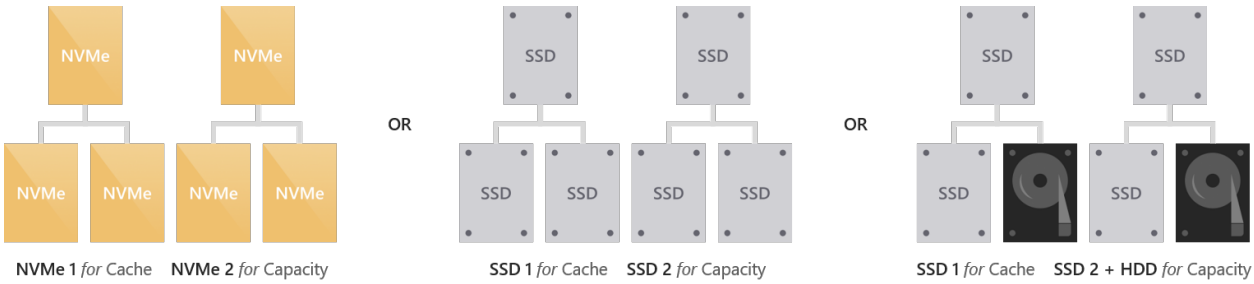
Then enter the following command, specifying the cache device model:

```
Enable-ClusterS2D -CacheDeviceModel "FABRIKAM NVME-1710"
```

You can verify that the drives you intended are being used for caching by running **Get-PhysicalDisk** in PowerShell and verifying that their **Usage** property says **"Journal"**.

### Manual deployment possibilities

Manual configuration enables the following deployment possibilities:




### Set cache behavior

It is possible to override the default behavior of the cache. For example, you can set it to cache reads even in an all-flash deployment. We discourage modifying the behavior unless you are certain the default does not suit your workload.

To override the behavior, use **Set-ClusterStorageSpacesDirect** cmdlet and its **-CacheModeSSD** and **-CacheModeHDD** parameters. The **CacheModeSSD** parameter sets the cache behavior when caching for solid-state drives. The **CacheModeHDD** parameter sets cache behavior when caching for hard disk drives. This can be done at any time after Storage Spaces Direct is enabled.

You can use **Get-ClusterStorageSpacesDirect** to verify the behavior is set.

#### Example

First, get the Storage Spaces Direct settings:

```
Get-ClusterStorageSpacesDirect
```

Here's some example output:

```
CacheModeHDD : ReadWrite
CacheModeSSD : WriteOnly
```

Then, do the following:

```
Set-ClusterStorageSpacesDirect -CacheModeSSD ReadWrite

Get-ClusterS2D
```

Here's some example output:

```
CacheModeHDD : ReadWrite
CacheModeSSD : ReadWrite
```

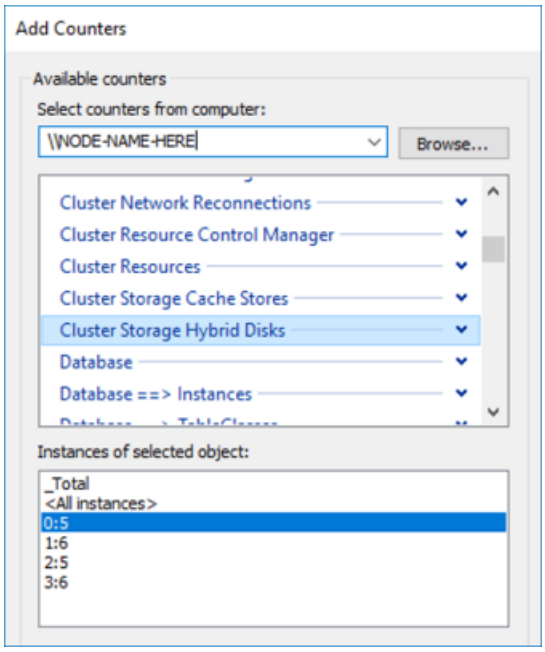
## Sizing the cache

The cache should be sized to accommodate the working set (the data being actively read or written at any given time) of your applications and workloads.

This is especially important in hybrid deployments with hard disk drives. If the active working set exceeds the size of the cache, or if the active working set drifts too quickly, read cache misses will increase and writes will need to be de-staged more aggressively, hurting overall performance.

You can use the built-in Performance Monitor (PerfMon.exe) utility in Windows to inspect the rate of cache misses. Specifically, you can compare the **Cache Miss Reads/sec** from the **Cluster Storage Hybrid Disk** counter set to the overall read IOPS of your deployment. Each "Hybrid Disk" corresponds to one capacity drive.

For example, 2 cache drives bound to 4 capacity drives results in 4 "Hybrid Disk" object instances per server.




There is no universal rule, but if too many reads are missing the cache, it may be undersized and you should consider adding cache drives to expand your cache. You can add cache drives or capacity drives independently whenever you want.

## Additional References

- Choosing drives and resiliency types
- Fault tolerance and storage efficiency
- Storage Spaces Direct hardware requirements

# Fault tolerance and storage efficiency in Storage Spaces Direct

11/2/2020 • 8 minutes to read • Edit Online

Applies to: Windows Server 2016

This topic introduces the resiliency options available in Storage Spaces Direct and outlines the scale requirements, storage efficiency, and general advantages and tradeoffs of each. It also presents some usage instructions to get you started, and references some great papers, blogs, and additional content where you can learn more.

If you are already familiar with Storage Spaces, you may want to skip to the Summary section.

## Overview

At its heart, Storage Spaces is about providing fault tolerance, often called 'resiliency', for your data. Its implementation is similar to RAID, except distributed across servers and implemented in software.

As with RAID, there are a few different ways Storage Spaces can do this, which make different tradeoffs between fault tolerance, storage efficiency, and compute complexity. These broadly fall into two categories: 'mirroring' and 'parity', the latter sometimes called 'erasure coding'.

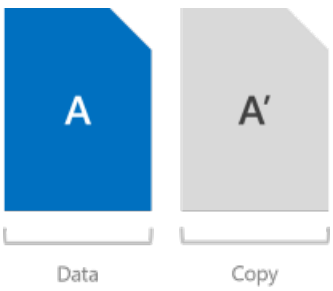
## Mirroring

Mirroring provides fault tolerance by keeping multiple copies of all data. This most closely resembles RAID-1. How that data is striped and placed is non-trivial (see this blog to learn more), but it is absolutely true to say that any data stored using mirroring is written, in its entirety, multiple times. Each copy is written to different physical hardware (different drives in different servers) that are assumed to fail independently.

In Windows Server 2016, Storage Spaces offers two flavors of mirroring – 'two-way' and 'three-way'.

#### Two-way mirror

Two-way mirroring writes two copies of everything. Its storage efficiency is 50% – to write 1 TB of data, you need at least 2 TB of physical storage capacity. Likewise, you need at least two hardware 'fault domains' – with Storage Spaces Direct, that means two servers.




> **WARNING**
> If you have more than two servers, we recommend using three-way mirorring instead.

#### Three-way mirror

Three-way mirroring writes three copies of everything. Its storage efficiency is 33.3% – to write 1 TB of data, you need at least 3 TB of physical storage capacity. Likewise, you need at least three hardware fault domains – with Storage Spaces Direct, that means three servers.

Three-way mirroring can safely tolerate at least two hardware problems (drive or server) at a time. For example, if you're rebooting one server when suddenly another drive or server fails, all data remains safe and continuously accessible.


## Parity

Parity encoding, often called 'erasure coding', provides fault tolerance using bitwise arithmetic, which can get remarkably complicated. The way this works is less obvious than mirroring, and there are many great online resources (for example, this third-party Dummies Guide to Erasure Coding) that can help you get the idea. Sufficed to say it provides better storage efficiency without compromising fault tolerance.

In Windows Server 2016, Storage Spaces offers two flavors of parity – 'single' parity and 'dual' parity, the latter employing an advanced technique called 'local reconstruction codes' at larger scales.

> **IMPORTANT**
> We recommend using mirroring for most performance-sensitive workloads. To learn more about how to balance performance and capacity depending on your workload, see Plan volumes.

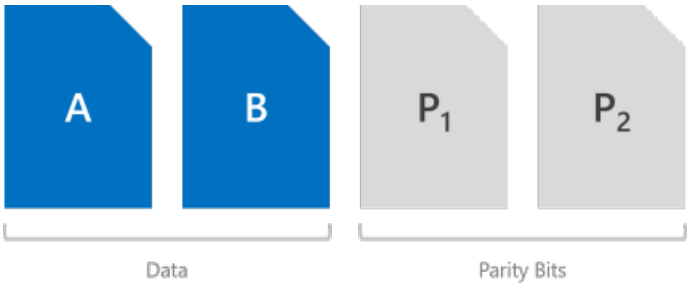
### Single parity

Single parity keeps only one bitwise parity symbol, which provides fault tolerance against only one failure at a time. It most closely resembles RAID-5. To use single parity, you need at least three hardware fault domains – with Storage Spaces Direct, that means three servers. Because three-way mirroring provides more fault tolerance at the same scale, we discourage using single parity. But, it's there if you insist on using it, and it is fully supported.

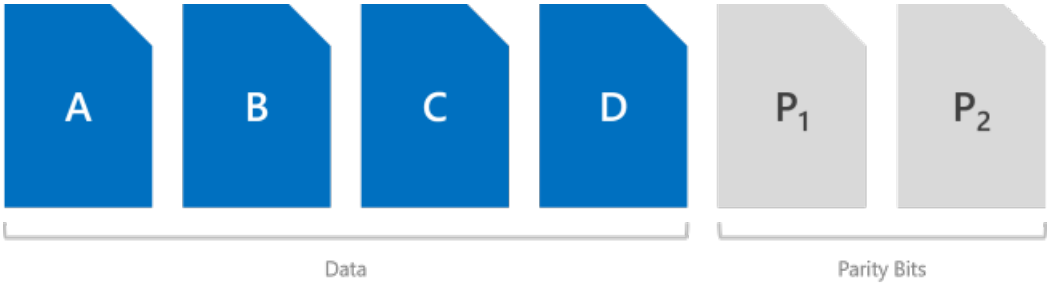
> **WARNING**
> We discourage using single parity because it can only safely tolerate one hardware failure at a time: if you're rebooting one server when suddenly another drive or server fails, you will experience downtime. If you only have three servers, we recommend using three-way mirroring. If you have four or more, see the next section.

### Dual parity

Dual parity implements Reed-Solomon error-correcting codes to keep two bitwise parity symbols, thereby providing the same fault tolerance as three-way mirroring (i.e. up to two failures at once), but with better storage efficiency. It most closely resembles RAID-6. To use dual parity, you need at least four hardware fault domains – with Storage Spaces Direct, that means four servers. At that scale, the storage efficiency is 50% – to store 2 TB of data, you need 4 TB of physical storage capacity.




The storage efficiency of dual parity increases the more hardware fault domains you have, from 50% up to 80%. For example, at seven (with Storage Spaces Direct, that means seven servers) the efficiency jumps to 66.7% – to store 4 TB of data, you need just 6 TB of physical storage capacity.




See the Summary section for the efficiency of dual party and local reconstruction codes at every scale.

**Local reconstruction codes**

Storage Spaces in Windows Server 2016 introduces an advanced technique developed by Microsoft Research called 'local reconstruction codes', or LRC. At large scale, dual parity uses LRC to split its encoding/decoding into a few smaller groups, to reduce the overhead required to make writes or recover from failures.

With hard disk drives (HDD) the group size is four symbols; with solid-state drives (SSD), the group size is six symbols. For example, here's what the layout looks like with hard disk drives and 12 hardware fault domains (meaning 12 servers) – there are two groups of four data symbols. It achieves 72.7% storage efficiency.


We recommend this in-depth yet eminently readable walk-through of how local reconstruction codes handle various failure scenarios, and why they're appealing, by our very own Claus Joergensen.

## Mirror-accelerated parity

Beginning in Windows Server 2016, a Storage Spaces Direct volume can be part mirror and part parity. Writes land first in the mirrored portion and are gradually moved into the parity portion later. Effectively, this is using mirroring to accelerate erasure coding.

To mix three-way mirror and dual parity, you need at least four fault domains, meaning four servers.

The storage efficiency of mirror-accelerated parity is in between what you'd get from using all mirror or all parity, and depends on the proportions you choose. For example, the demo at the 37-minute mark of this presentation shows various mixes achieving 46%, 54%, and 65% efficiency with 12 servers.

**IMPORTANT**

We recommend using mirroring for most performance-sensitive workloads. To learn more about how to balance performance and capacity depending on your workload, see Plan volumes.

# Summary

This section summarizes the resiliency types available in Storage Spaces Direct, the minimum scale requirements to use each type, how many failures each type can tolerate, and the corresponding storage efficiency.

### Resiliency types

| RESILIENCY | FAILURE TOLERANCE | STORAGE EFFICIENCY |
|---|---|---|
| Two-way mirror | 1 | 50.0% |
| Three-way mirror | 2 | 33.3% |
| Dual parity | 2 | 50.0% - 80.0% |
| Mixed | 2 | 33.3% - 80.0% |

### Minimum scale requirements

| RESILIENCY | MINIMUM REQUIRED FAULT DOMAINS |
|---|---|
| Two-way mirror | 2 |
| Three-way mirror | 3 |
| Dual parity | 4 |
| Mixed | 4 |

**TIP**

Unless you are using chassis or rack fault tolerance, the number of fault domains refers to the number of servers. The number of drives in each server does not affect which resiliency types you can use, as long as you meet the minimum requirements for Storage Spaces Direct.

### Dual parity efficiency for hybrid deployments

This table shows the storage efficiency of dual parity and local reconstruction codes at each scale for hybrid deployments which contain both hard disk drives (HDD) and solid-state drives (SSD).

| FAULT DOMAINS | LAYOUT | EFFICIENCY |
|---|---|---|
| 2 | – | – |
| 3 | – | – |
| 4 | RS 2+2 | 50.0% |

| FAULT DOMAINS | LAYOUT | EFFICIENCY |
|---|---|---|
| 5 | RS 2+2 | 50.0% |
| 6 | RS 2+2 | 50.0% |
| 7 | RS 4+2 | 66.7% |
| 8 | RS 4+2 | 66.7% |
| 9 | RS 4+2 | 66.7% |
| 10 | RS 4+2 | 66.7% |
| 11 | RS 4+2 | 66.7% |
| 12 | LRC (8, 2, 1) | 72.7% |
| 13 | LRC (8, 2, 1) | 72.7% |
| 14 | LRC (8, 2, 1) | 72.7% |
| 15 | LRC (8, 2, 1) | 72.7% |
| 16 | LRC (8, 2, 1) | 72.7% |

**Dual parity efficiency for all-flash deployments**

This table shows the storage efficiency of dual parity and local reconstruction codes at each scale for all-flash deployments which contain only solid-state drives (SSD). The parity layout can use larger group sizes and achieve better storage efficiency in an all-flash configuration.

| FAULT DOMAINS | LAYOUT | EFFICIENCY |
|---|---|---|
| 2 | – | – |
| 3 | – | – |
| 4 | RS 2+2 | 50.0% |
| 5 | RS 2+2 | 50.0% |
| 6 | RS 2+2 | 50.0% |
| 7 | RS 4+2 | 66.7% |
| 8 | RS 4+2 | 66.7% |
| 9 | RS 6+2 | 75.0% |
| 10 | RS 6+2 | 75.0% |
| 11 | RS 6+2 | 75.0% |

| FAULT DOMAINS | LAYOUT | EFFICIENCY |
|---|---|---|
| 12 | RS 6+2 | 75.0% |
| 13 | RS 6+2 | 75.0% |
| 14 | RS 6+2 | 75.0% |
| 15 | RS 6+2 | 75.0% |
| 16 | LRC (12, 2, 1) | 80.0% |

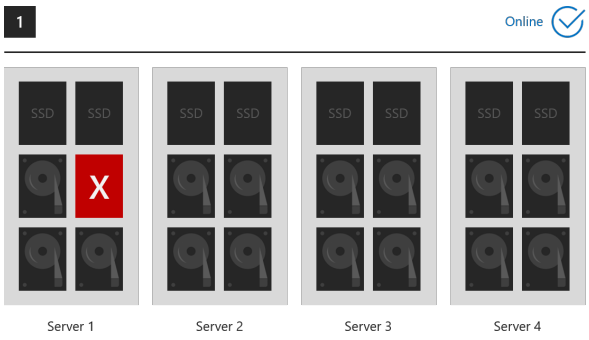
# Examples

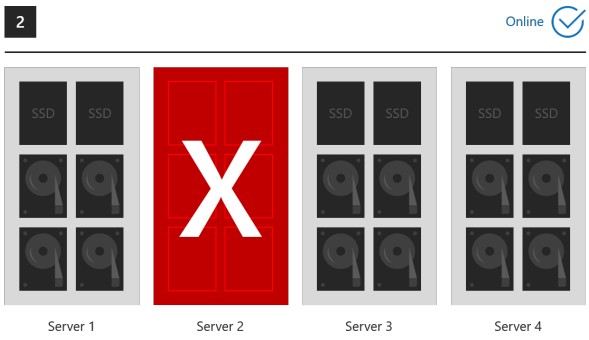
Unless you have only two servers, we recommend using three-way mirroring and/or dual parity, because they offer better fault tolerance. Specifically, they ensure that all data remains safe and continuously accessible even when two fault domains – with Storage Spaces Direct, that means two servers - are affected by simultaneous failures.

### Examples where everything stays online

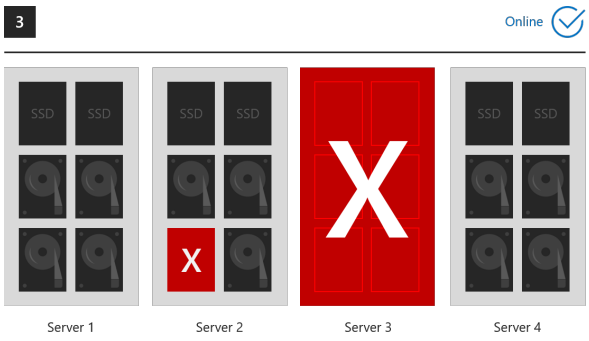
These six examples show what three-way mirroring and/or dual parity **can** tolerate.

- 1. One drive lost (includes cache drives)
- 2. One server lost



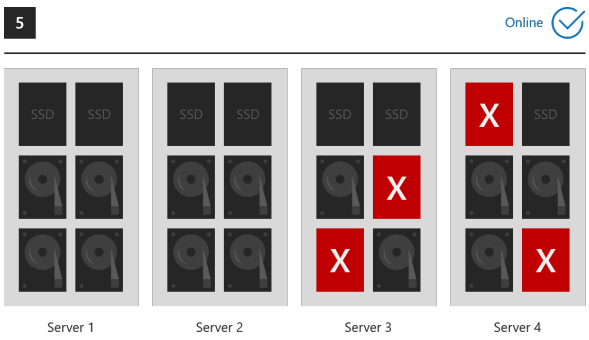



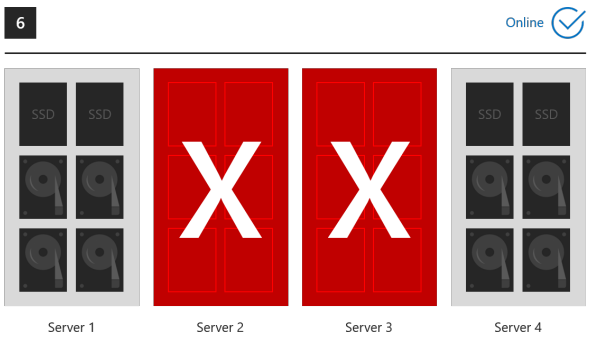

- 3. One server and one drive lost
- 4. Two drives lost in different servers





- 5. More than two drives lost, so long as at most two servers are affected
- 6. Two servers lost



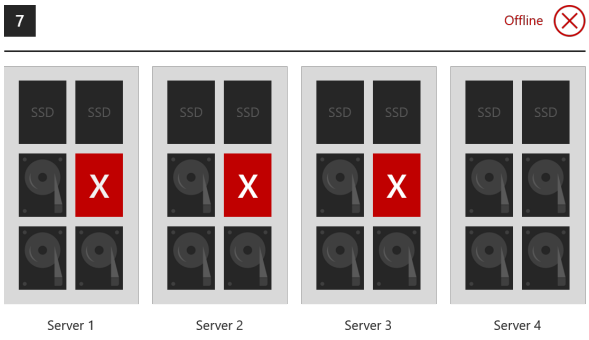



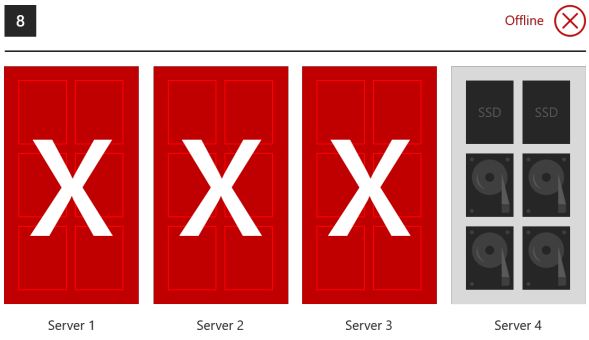

...in every case, all volumes will stay online. (Make sure your cluster maintains quorum.)

**Examples where everything goes offline**

Over its lifetime, Storage Spaces can tolerate any number of failures, because it restores to full resiliency after each one, given sufficient time. However, at most two fault domains can safely be affected by failures at any given moment. The following are therefore examples of what three-way mirroring and/or dual parity **cannot** tolerate.

- 7. Drives lost in three or more servers at once
- 8. Three or more servers lost at once




# Usage

Check out Creating volumes in Storage Spaces Direct.

# Additional References

Every link below is inline somewhere in the body of this topic.

- Storage Spaces Direct in Windows Server 2016
- Fault Domain Awareness in Windows Server 2016
- Erasure Coding in Azure by Microsoft Research
- Local Reconstruction Codes and Accelerating Parity Volumes
- Volumes in the Storage Management API
- Storage Efficiency Demo at Microsoft Ignite 2016
- Capacity Calculator PREVIEW for Storage Spaces Direct

# Drive symmetry considerations for Storage Spaces Direct

12/16/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Storage Spaces Direct works best when every server has exactly the same drives.

In reality, we recognize this is not always practical: Storage Spaces Direct is designed to run for years and to scale as the needs of your organization grow. Today, you may buy spacious 3 TB hard drives; next year, it may become impossible to find ones that small. Therefore, some amount of mixing-and-matching is supported.

This topic explains the constraints and provides examples of supported and unsupported configurations.

## Constraints

### Type

All servers should have the same types of drives.

For example, if one server has NVMe, they should *all* have NVMe.

### Number

All servers should have the same number of drives of each type.

For example, if one server has six SSD, they should *all* have six SSD.

> **NOTE**
> It is okay for the number of drives to differ temporarily during failures or while adding or removing drives.

### Model

We recommend using drives of the same model and firmware version whenever possible. If you can't, carefully select drives that are as similar as possible. We discourage mixing-and-matching drives of the same type with sharply different performance or endurance characteristics (unless one is cache and the other is capacity) because Storage Spaces Direct distributes IO evenly and doesn't discriminate based on model.

> **NOTE**
> It is okay to mix-and-match similar SATA and SAS drives.

### Size

We recommend using drives of the same sizes whenever possible. Using capacity drives of different sizes may result in some unusable capacity, and using cache drives of different sizes may not improve cache performance. See the next section for details.

> **WARNING**
> Differing capacity drives sizes across servers may result in stranded capacity.

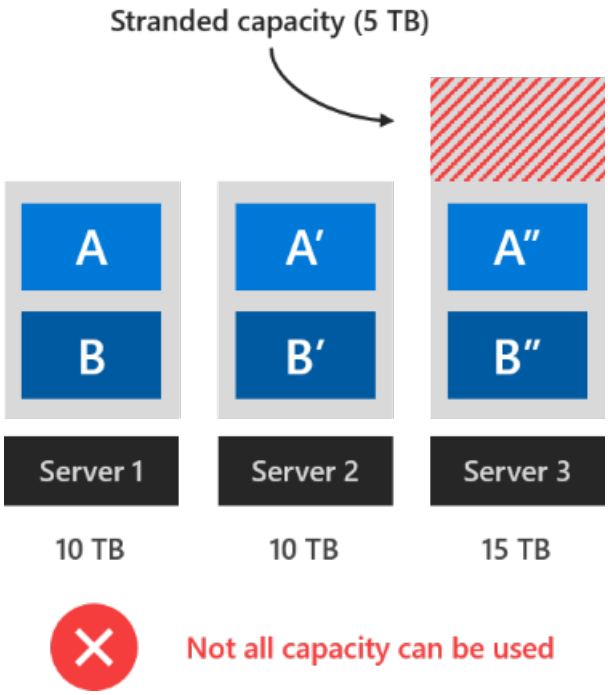
# Understand: capacity imbalance

Storage Spaces Direct is robust to capacity imbalance across drives and across servers. Even if the imbalance is severe, everything will continue to work. However, depending on several factors, capacity that isn't available in every server may not be usable.

To see why this happens, consider the simplified illustration below. Each colored box represents one copy of mirrored data. For example, the boxes marked A, A', and A'' are three copies of the same data. To honor server fault tolerance, these copies *must* be stored in different servers.

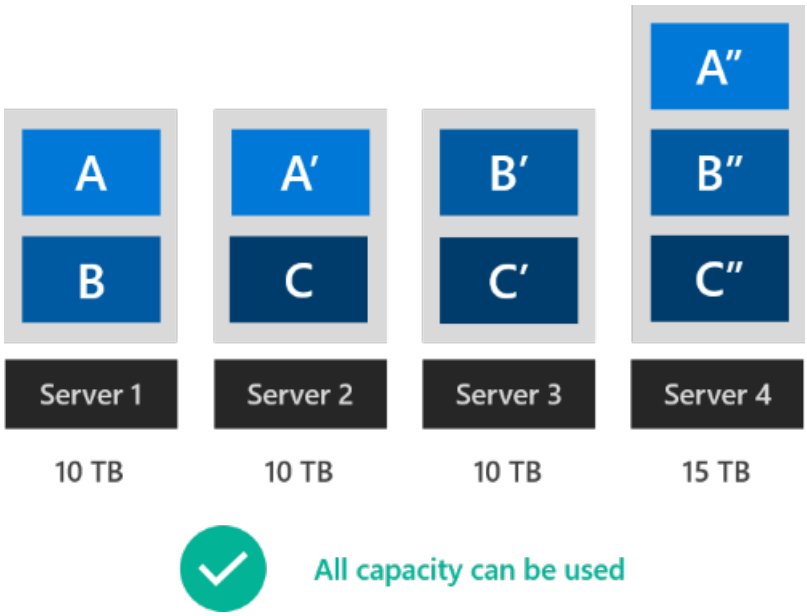
**Stranded capacity**

As drawn, Server 1 (10 TB) and Server 2 (10 TB) are full. Server 3 has larger drives, therefore its total capacity is larger (15 TB). However, to store more three-way mirror data on Server 3 would require copies on Server 1 and Server 2 too, which are already full. The remaining 5 TB capacity on Server 3 can't be used – it's *"stranded"* capacity.




**Optimal placement**

Conversely, with four servers of 10 TB, 10 TB, 10 TB, and 15 TB capacity and three-way mirror resiliency, it *is* possible to validly place copies in a way that uses all available capacity, as drawn. Whenever this is possible, the Storage Spaces Direct allocator will find and use the optimal placement, leaving no stranded capacity.

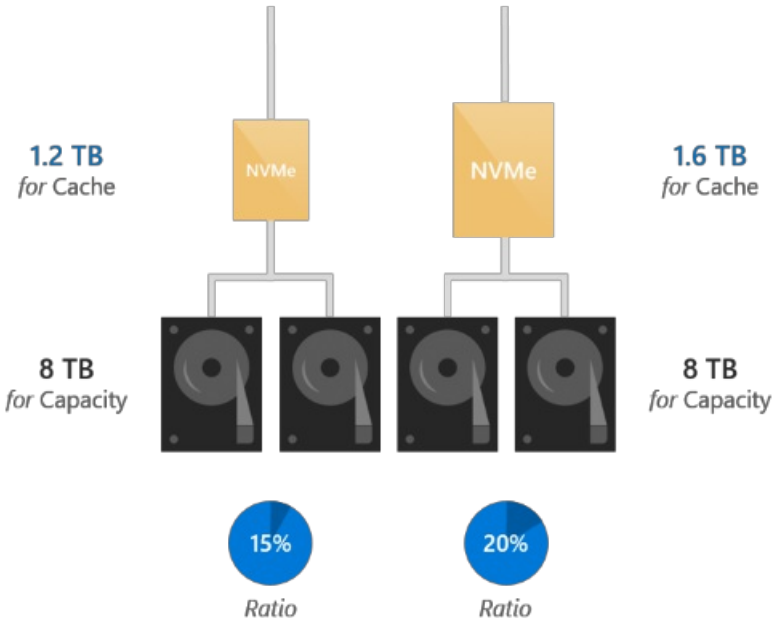



The number of servers, the resiliency, the severity of the capacity imbalance, and other factors affect whether there is stranded capacity. **The most prudent general rule is to assume that only capacity available in every server is guaranteed to be usable.**

## Understand: cache imbalance

Storage Spaces Direct is robust to cache imbalance across drives and across servers. Even if the imbalance is severe, everything will continue to work. Moreover, Storage Spaces Direct always uses all available cache to the fullest.

However, using cache drives of different sizes may not improve cache performance uniformly or predictably: only IO to drive bindings with larger cache drives may see improved performance. Storage Spaces Direct distributes IO evenly across bindings and doesn't discriminate based on cache-to-capacity ratio.




> **TIP**
> See Understanding the cache to learn more about cache bindings.

## Example configurations

Here are some supported and unsupported configurations:

### Supported: different models between servers

The first two servers use NVMe model "X" but the third server uses NVMe model "Z", which is very similar.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 2 x NVMe Model X (cache) | 2 x NVMe Model X (cache) | 2 x NVMe Model Z (cache) |
| 10 x SSD Model Y (capacity) | 10 x SSD Model Y (capacity) | 10 x SSD Model Y (capacity) |

This is supported.

### Supported: different models within server

Every server uses some different mix of HDD models "Y" and "Z", which are very similar. Every server has 10 total HDD.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 2 x SSD Model X (cache) | 2 x SSD Model X (cache) | 2 x SSD Model X (cache) |
| 7 x HDD Model Y (capacity) | 5 x HDD Model Y (capacity) | 1 x HDD Model Y (capacity) |
| 3 x HDD Model Z (capacity) | 5 x HDD Model Z (capacity) | 9 x HDD Model Z (capacity) |

This is supported.

### Supported: different sizes across servers

The first two servers use 4 TB HDD but the third server uses very similar 6 TB HDD.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 2 x 800 GB NVMe (cache) | 2 x 800 GB NVMe (cache) | 2 x 800 GB NVMe (cache) |
| 4 x 4 TB HDD (capacity) | 4 x 4 TB HDD (capacity) | 4 x 6 TB HDD (capacity) |

This is supported, although it will result in stranded capacity.

### Supported: different sizes within server

Every server uses some different mix of 1.2 TB and very similar 1.6 TB SSD. Every server has 4 total SSD.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 3 x 1.2 TB SSD (cache) | 2 x 1.2 TB SSD (cache) | 4 x 1.2 TB SSD (cache) |
| 1 x 1.6 TB SSD (cache) | 2 x 1.6 TB SSD (cache) | - |
| 20 x 4 TB HDD (capacity) | 20 x 4 TB HDD (capacity) | 20 x 4 TB HDD (capacity) |

This is supported.

### Not supported: different types of drives across servers

Server 1 has NVMe but the others don't.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 6 x NVMe (cache) | - | - |
| - | 6 x SSD (cache) | 6 x SSD (cache) |
| 18 x HDD (capacity) | 18 x HDD (capacity) | 18 x HDD (capacity) |

This isn't supported. The types of drives should be the same in every server.

**Not supported: different number of each type across servers**

Server 3 has more drives than the others.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 2 x NVMe (cache) | 2 x NVMe (cache) | 4 x NVMe (cache) |
| 10 x HDD (capacity) | 10 x HDD (capacity) | 20 x HDD (capacity) |

This isn't supported. The number of drives of each type should be the same in every server.

**Not supported: only HDD drives**

All servers have only HDD drives connected.

| SERVER 1 | SERVER 2 | SERVER 3 |
|---|---|---|
| 18 x HDD (capacity) | 18 x HDD (capacity) | 18 x HDD (capacity) |

This isn't supported. You need to add a minimum of two cache drives (NvME or SSD) attached to each of the servers.

## Summary

To recap, every server in the cluster should have the same types of drives and the same number of each type. It's supported to mix-and-match drive models and drive sizes as needed, with the considerations above.

| CONSTRAINT | STATE |
|---|---|
| Same types of drives in every server | **Required** |
| Same number of each type in every server | **Required** |
| Same drive models in every server | Recommended |
| Same drive sizes in every server | Recommended |

## Additional References

- Storage Spaces Direct hardware requirements
- Storage Spaces Direct overview

# Understand and monitor storage resync

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server 2019

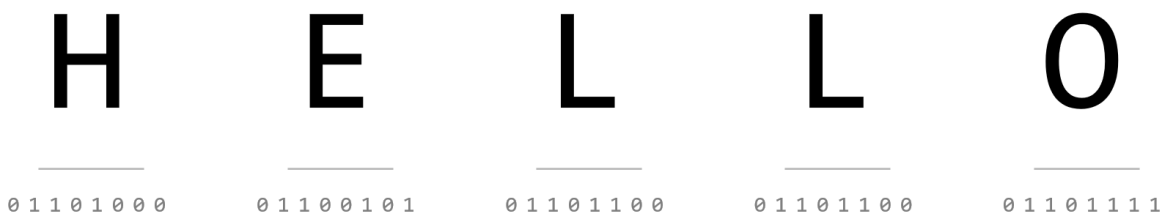
Storage resync alerts are a new capability of Storage Spaces Direct in Windows Server 2019 that allows the Health Service to throw a fault when your storage is resyncing. The alert is useful in notifying you when resync is happening, so that you don't accidentally take more servers down (which could cause multiple fault domains to be affected, resulting in your cluster going down).

This topic provides background and steps to understand and see storage resync in a Windows Server failover cluster with Storage Spaces Direct.

## Understanding resync

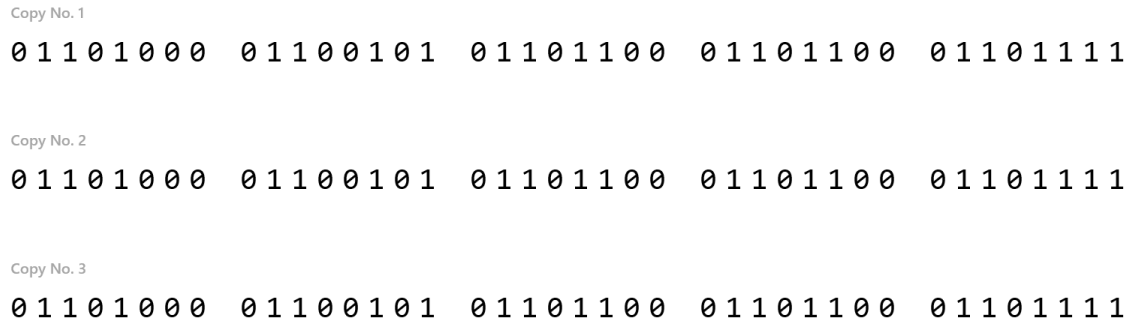
Let's start with a simple example to understand how storage gets out of sync. Keep in mind that any shared-nothing (local drives only) distributed storage solution exhibits this behavior. As you will see below, if one server node goes down, then its drives won't be updated until it comes back online - this is true for any hyper-converged architecture.

Suppose that we want to store the string "HELLO".

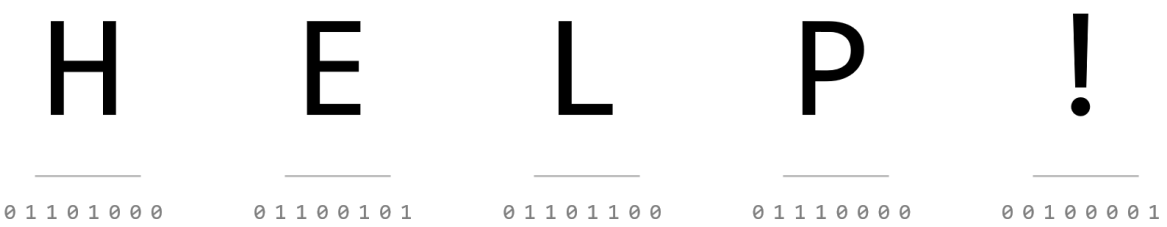



** Using standard ASCII 8-bit encodings for each letter*

Asssuming that we have three-way mirror resiliency, we have three copies of this string. Now, if we take server #1 down temporarily (for maintanence), then we cannot access copy #1.

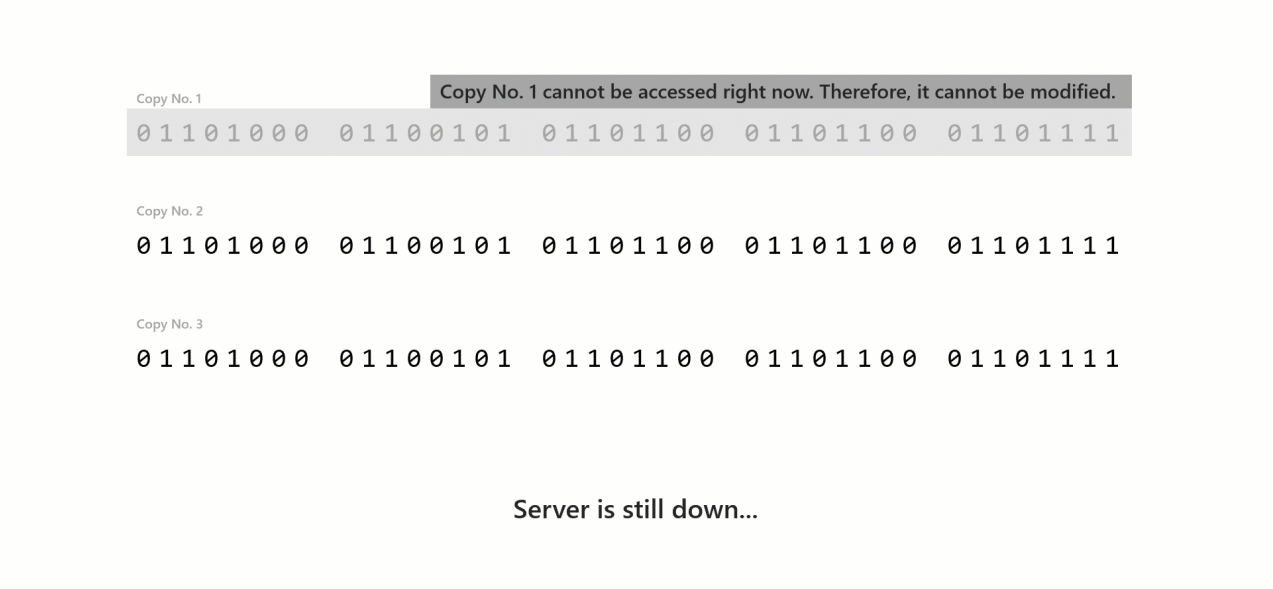



Suppose we update our string from "HELLO" to "HELP!" at this time.




** Using standard ASCII 8-bit encodings for each letter*

Once we update the string, copy #2 and #3 will be successfully updated. However, copy #1 still cannot be accessed because server #1 is down temporarily (for maintanence).




Now, we have copy #1 which has data that is out of sync. The operating system uses granular dirty region tracking to keep track of the bits that are out of sync. This way when server #1 comes back online, we can sync the changes

by reading the data from copy #2 or #3 and overwriting the data in copy #1. The advantages of this approach are that we only need to copy over the data that is stale, rather than resyncing all of the data from server #2 or server #3.


So, this explains how data gets out of sync. But what does this look like at a high level? Assume for this example that we have a three server hyper-converged cluster. When server #1 is in maintenance, you will see it as being down. When you bring server #1 back up, it will start resyncing all of its storage using the granular dirty region tracking (explained above). Once the data is all back in sync, all servers will be shown as up.


## How to monitor storage resync in Windows Server 2019

Now that you understand how storage resync works, let's look at how this shows up in Windows Server 2019. We have added a new fault to the Health Service that will show up when your storage is resyncing.

To view this fault in PowerShell, run:

```
Get-HealthFault
```

This is a new fault in Windows Server 2019, and will appear in PowerShell, in the cluster validation report, and anywhere else that builds on Health faults.

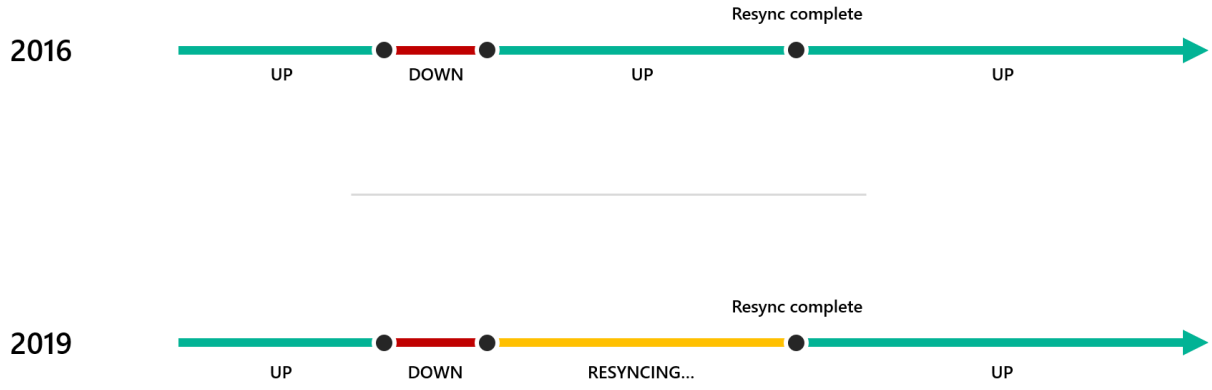
To get a deeper view, you can query the time series database in PowerShell as follows:

```
Get-ClusterNode | Get-ClusterPerf -ClusterNodeSeriesName ClusterNode.Storage.Degraded
```

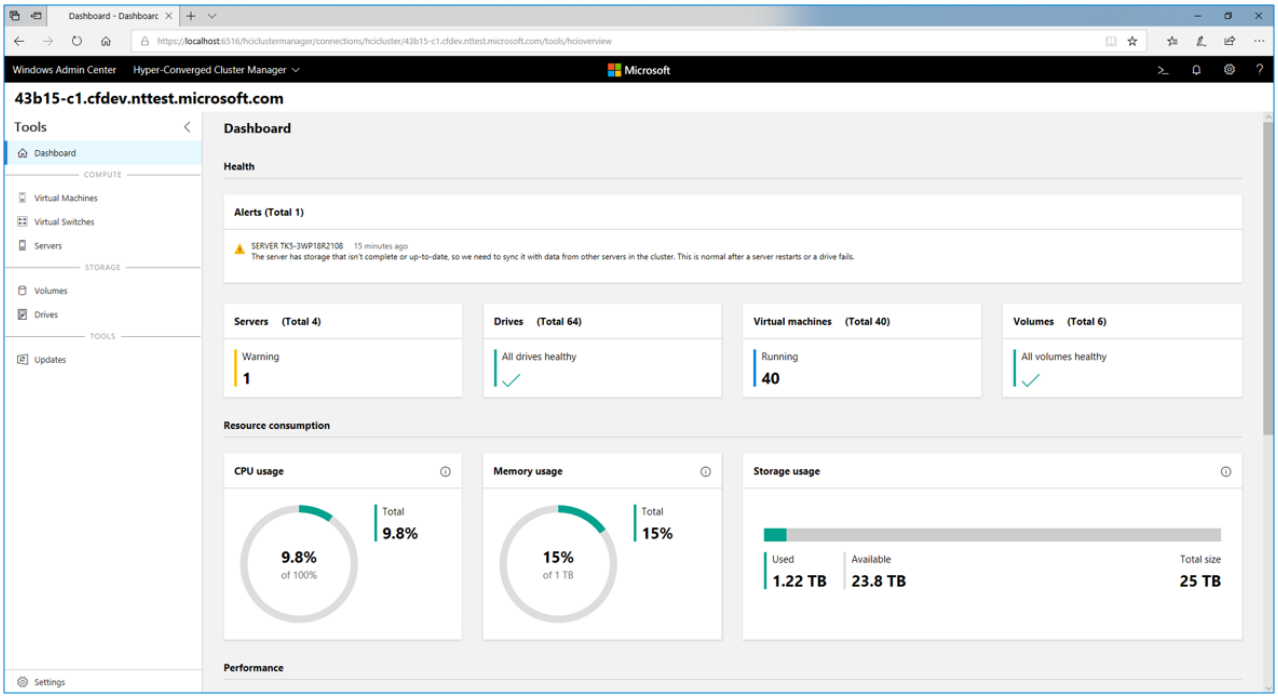
Here's some example output:

```
Object Description: ClusterNode Server1

Series                       Time                Value Unit
------                       ----                ----- ----
ClusterNode.Storage.Degraded 01/11/2019 16:26:48     214 GB
```

Notably, Windows Admin Center uses Health faults to set the status and color of cluster nodes. So, this new fault will cause cluster nodes to transition from red (down) to yellow (resyncing) to green (up), instead of going straight from red to green, on the HCI Dashboard.

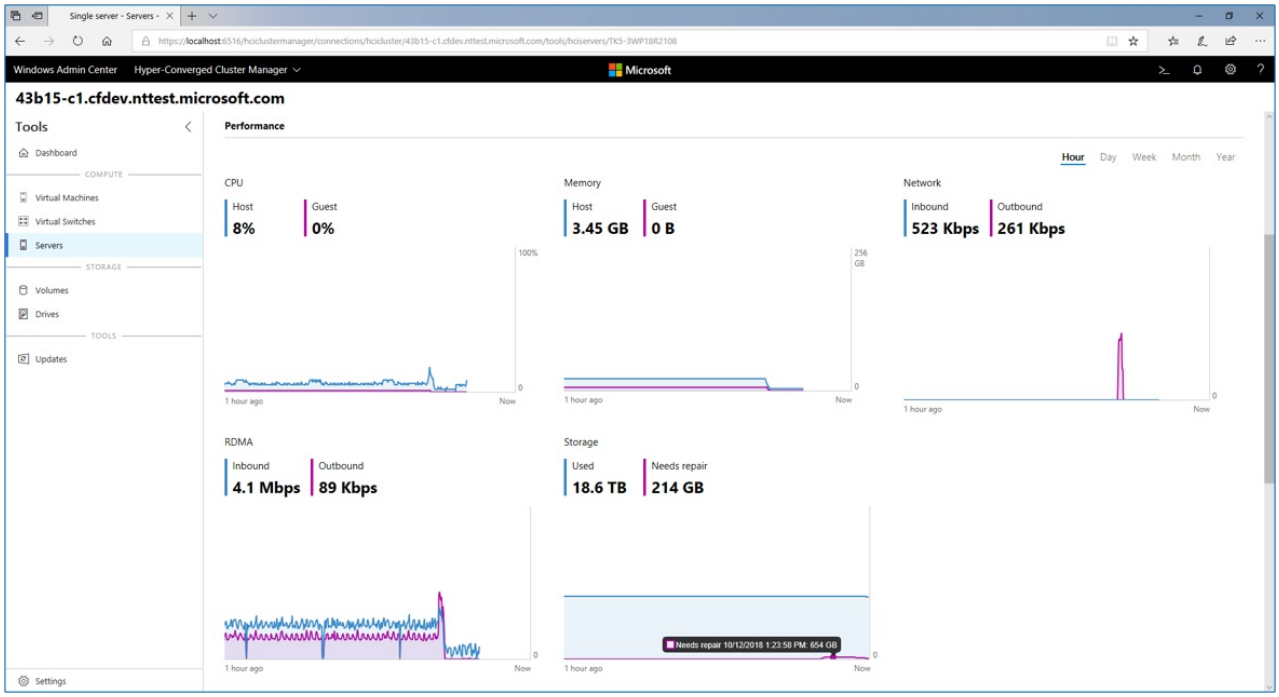



By showing the overall storage resync progress, you can accurately know how much data is out of sync and whether your system is making forward progress. When you open Windows Admin Center and go to the *Dashboard*, you will see the new alert as follows:




The alert is useful in notifying you when resync is happening, so that you don't accidentally take more servers down (which could cause multiple fault domains to be affected, resulting in your cluster going down).

If you navigate to the *Servers* page in Windows Admin Center, click on *Inventory*, and then choose a specific server, you can get a more detailed view of how this storage resync looks on a per-server basis. If you navigate to your server and look at the *Storage* chart, you will see the amount of data that needs to be repaired in a *purple* line with exact number right above. This amount will increase when the server is down (more data needs to be resynced), and gradually decrease when the server comes back online (data is being synced). When the amount of data that needs to be repair is 0, your storage is done resyncing - you are now free to take a server down if you need to. A screenshot of this experience in Windows Admin Center is shown below:




## How to see storage resync in Windows Server 2016

As you can see, this alert is particularly helpful in getting a holistic view of what is happening at the storage layer. It effectively summarizes the information that you can get from the Get-StorageJob cmdlet, which returns information about long-running Storage module jobs, such as a repair operation on a storage space. An example is shown below:

```
Get-StorageJob
```

Here's example output:

```
Name                ElapsedTime          JobState             PercentComplete      IsBackgroundTask
----                -----------          --------             ---------------      ----------------
Regeneration        00:01:19             Running              50                   True
```

This view is a lot more granular since the storage jobs listed are per volume, you can see the list of jobs that are running, and you can track their individual progress. This cmdlet works on both Windows Server 2016 and 2019.

## Additional References

- Taking a server offline for maintenance
- Storage Spaces Direct overview

# Understanding cluster and pool quorum

11/2/2020 • 11 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Windows Server Failover Clustering provides high availability for workloads. These resources are considered highly available if the nodes that host resources are up; however, the cluster generally requires more than half the nodes to be running, which is known as having *quorum*.

Quorum is designed to prevent *split-brain* scenarios which can happen when there is a partition in the network and subsets of nodes cannot communicate with each other. This can cause both subsets of nodes to try to own the workload and write to the same disk which can lead to numerous problems. However, this is prevented with Failover Clustering's concept of quorum which forces only one of these groups of nodes to continue running, so only one of these groups will stay online.

Quorum determines the number of failures that the cluster can sustain while still remaining online. Quorum is designed to handle the scenario when there is a problem with communication between subsets of cluster nodes, so that multiple servers don't try to simultaneously host a resource group and write to the same disk at the same time. By having this concept of quorum, the cluster will force the cluster service to stop in one of the subsets of nodes to ensure that there is only one true owner of a particular resource group. Once nodes which have been stopped can once again communicate with the main group of nodes, they will automatically rejoin the cluster and start their cluster service.

In Windows Server 2019 and Windows Server 2016, there are two components of the system that have their own quorum mechanisms:

- **Cluster Quorum**: This operates at the cluster level (i.e. you can lose nodes and have the cluster stay up)
- **Pool Quorum**: This operates on the pool level when Storage Spaces Direct is enabled (i.e. you can lose nodes and drives and have the pool stay up). Storage pools were designed to be used in both clustered and non-clustered scenarios, which is why they have a different quorum mechanism.

## Cluster quorum overview

The table below gives an overview of the Cluster Quorum outcomes per scenario:

| SERVER NODES | CAN SURVIVE ONE SERVER NODE FAILURE | CAN SURVIVE ONE SERVER NODE FAILURE, THEN ANOTHER | CAN SURVIVE TWO SIMULTANEOUS SERVER NODE FAILURES |
|---|---|---|---|
| 2 | 50/50 | No | No |
| 2 + Witness | Yes | No | No |
| 3 | Yes | 50/50 | No |
| 3 + Witness | Yes | Yes | No |
| 4 | Yes | Yes | 50/50 |
| 4 + Witness | Yes | Yes | Yes |

| SERVER NODES | CAN SURVIVE ONE SERVER NODE FAILURE | CAN SURVIVE ONE SERVER NODE FAILURE, THEN ANOTHER | CAN SURVIVE TWO SIMULTANEOUS SERVER NODE FAILURES |
|---|---|---|---|
| 5 and above | Yes | Yes | Yes |

**Cluster quorum recommendations**

- If you have two nodes, a witness is **required**.
- If you have three or four nodes, witness is **strongly recommended**.
- If you have Internet access, use a **cloud witness**
- If you're in an IT environment with other machines and file shares, use a file share witness

## How cluster quorum works

When nodes fail, or when some subset of nodes loses contact with another subset, surviving nodes need to verify that they constitute the *majority* of the cluster to remain online. If they can't verify that, they'll go offline.

But the concept of *majority* only works cleanly when the total number of nodes in the cluster is odd (for example, three nodes in a five node cluster). So, what about clusters with an even number of nodes (say, a four node cluster)?

There are two ways the cluster can make the *total number of votes* odd:

1. First, it can go *up* one by adding a *witness* with an extra vote. This requires user set-up.
2. Or, it can go *down* one by zeroing one unlucky node's vote (happens automatically as needed).

Whenever surviving nodes successfully verify they are the *majority*, the definition of *majority* is updated to be among just the survivors. This allows the cluster to lose one node, then another, then another, and so forth. This concept of the *total number of votes* adapting after successive failures is known as ***Dynamic quorum***.

**Dynamic witness**

Dynamic witness toggles the vote of the witness to make sure that the *total number of votes* is odd. If there are an odd number of votes, the witness doesn't have a vote. If there is an even number of votes, the witness has a vote. Dynamic witness significantly reduces the risk that the cluster will go down because of witness failure. The cluster decides whether to use the witness vote based on the number of voting nodes that are available in the cluster.

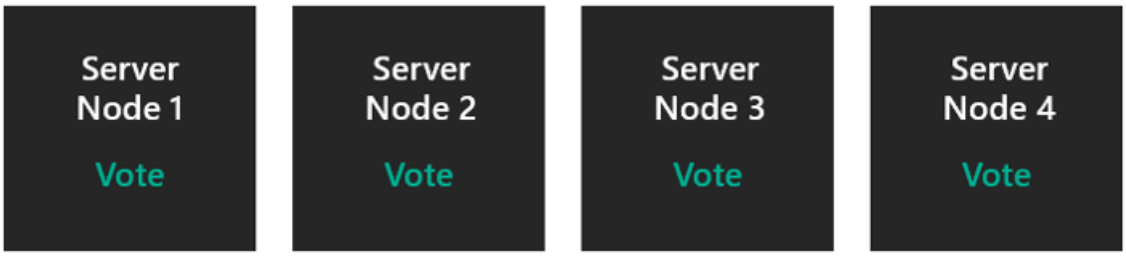
Dynamic quorum works with Dynamic witness in the way described below.

**Dynamic quorum behavior**

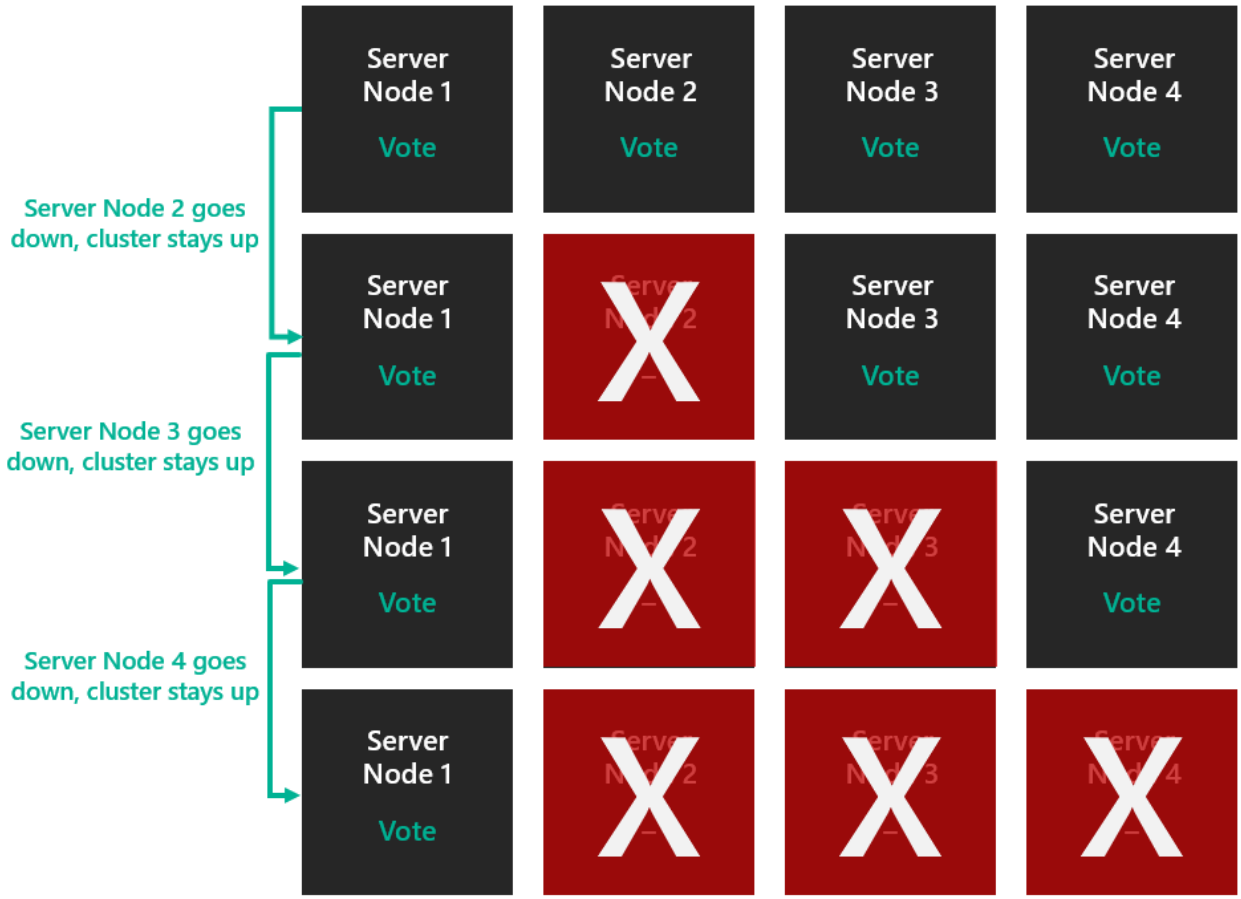
- If you have an **even** number of nodes and no witness, *one node gets its vote zeroed*. For example, only three of the four nodes get votes, so the *total number of votes* is three, and two survivors with votes are considered a majority.
- If you have an **odd** number of nodes and no witness, *they all get votes*.
- If you have an **even** number of nodes plus witness, *the witness votes*, so the total is odd.
- If you have an **odd** number of nodes plus witness, *the witness doesn't vote*.

Dynamic quorum enables the ability to assign a vote to a node dynamically to avoid losing the majority of votes and to allow the cluster to run with one node (known as last-man standing). Let's take a four-node cluster as an example. Assume that quorum requires 3 votes.

In this case, the cluster would have gone down if you lost two nodes.




However, dynamic quorum prevents this from happening. The *total number of votes* required for quorum is now determined based on the number of nodes available. So, with dynamic quorum, the cluster will stay up even if you lose three nodes.

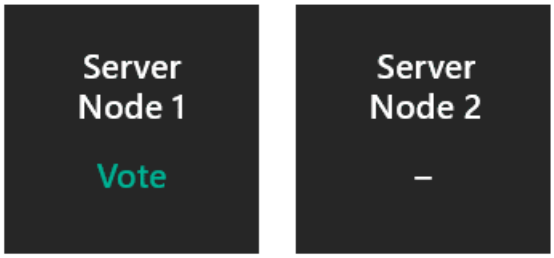



The above scenario applies to a general cluster that doesn't have Storage Spaces Direct enabled. However, when Storage Spaces Direct is enabled, the cluster can only support two node failures. This is explained more in the pool quorum section.

### Examples

#### Two nodes without a witness.

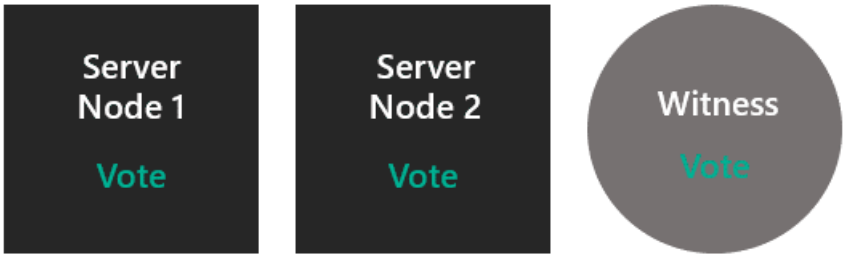
One node's vote is zeroed, so the *majority* vote is determined out of a total of **1 vote**. If the non-voting node goes down unexpectedly, the survivor has 1/1 and the cluster survives. If the voting node goes down unexpectedly, the survivor has 0/1 and the cluster goes down. If the voting node is gracefully powered down, the vote is transferred to the other node, and the cluster survives. ***This is why it's critical to configure a witness.***



- Can survive one server failure: **Fifty percent chance**.
- Can survive one server failure, then another: **No**.
- Can survive two server failures at once: **No**.

**Two nodes with a witness.**

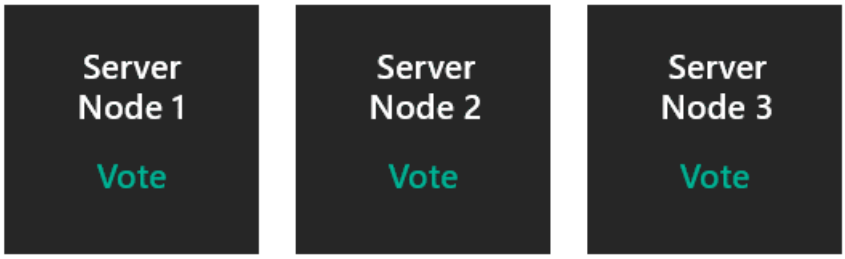
Both nodes vote, plus the witness votes, so the *majority* is determined out of a total of **3 votes**. If either node goes down, the survivor has 2/3 and the cluster survives.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **No**.
- Can survive two server failures at once: **No**.

**Three nodes without a witness.**

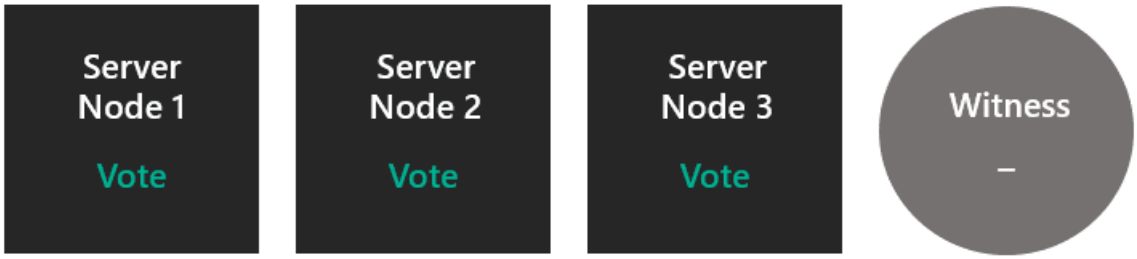
All nodes vote, so the *majority* is determined out of a total of **3 votes**. If any node goes down, the survivors are 2/3 and the cluster survives. The cluster becomes two nodes without a witness – at that point, you're in Scenario 1.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Fifty percent chance**.
- Can survive two server failures at once: **No**.

**Three nodes with a witness.**

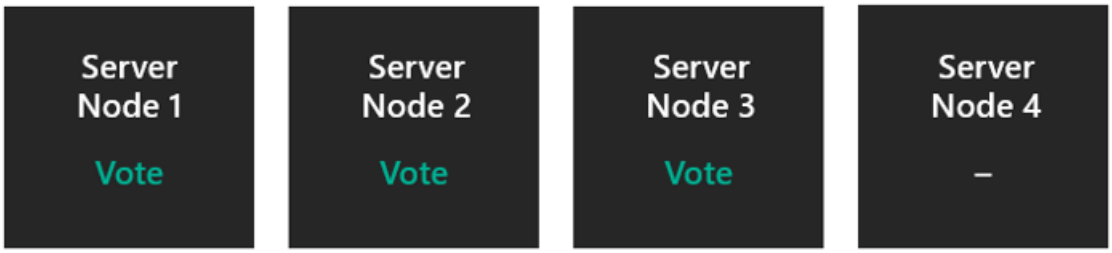
All nodes vote, so the witness doesn't initially vote. The *majority* is determined out of a total of **3 votes**. After one failure, the cluster has two nodes with a witness – which is back to Scenario 2. So, now the two nodes and the witness vote.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Yes**.
- Can survive two server failures at once: **No**.

**Four nodes without a witness**

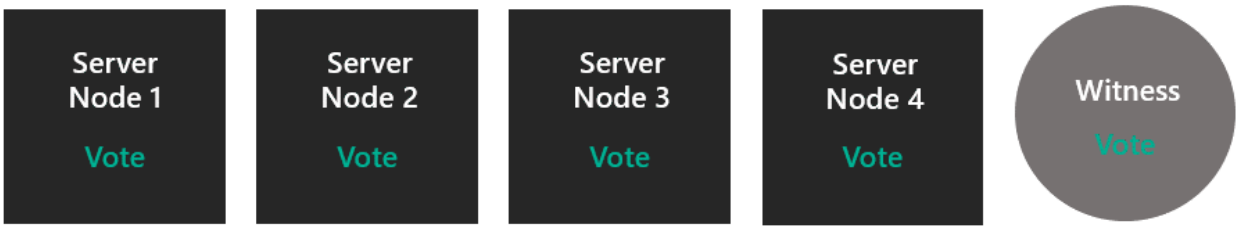
One node's vote is zeroed, so the *majority* is determined out of a total of **3 votes**. After one failure, the cluster becomes three nodes, and you're in Scenario 3.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Yes**.
- Can survive two server failures at once: **Fifty percent chance**.

**Four nodes with a witness.**

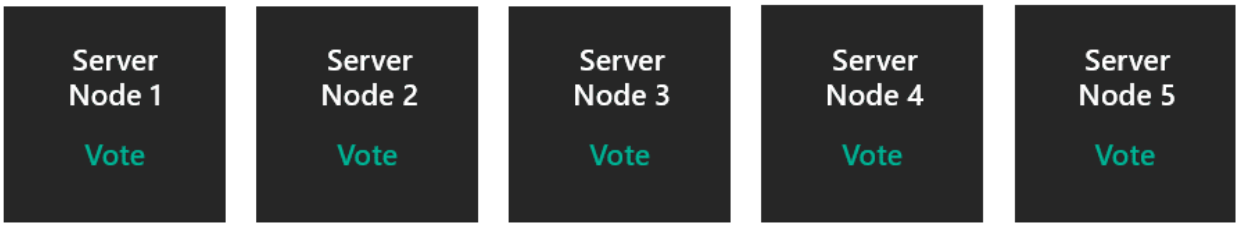
All nodes votes and the witness votes, so the *majority* is determined out of a total of **5 votes**. After one failure, you're in Scenario 4. After two simultaneous failures, you skip down to Scenario 2.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Yes**.
- Can survive two server failures at once: **Yes**.

**Five nodes and beyond.**

All nodes vote, or all but one vote, whatever makes the total odd. Storage Spaces Direct cannot handle more than two nodes down anyway, so at this point, no witness is needed or useful.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Yes**.
- Can survive two server failures at once: **Yes**.

Now that we understand how quorum works, let's look at the types of quorum witnesses.

### Quorum witness types

Failover Clustering supports three types of Quorum Witnesses:

- **Cloud Witness** - Blob storage in Azure accessible by all nodes of the cluster. It maintains clustering information in a witness.log file, but doesn't store a copy of the cluster database.
- **File Share Witness** – A SMB file share that is configured on a file server running Windows Server. It maintains clustering information in a witness.log file, but doesn't store a copy of the cluster database.
- **Disk Witness** - A small clustered disk which is in the Cluster Available Storage group. This disk is highly-available and can failover between nodes. It contains a copy of the cluster database. ***A Disk Witness isn't***

*supported with Storage Spaces Direct*.

## Pool quorum overview

We just talked about Cluster Quorum, which operates at the cluster level. Now, let's dive into Pool Quorum, which operates on the pool level (i.e. you can lose nodes and drives and have the pool stay up). Storage pools were designed to be used in both clustered and non-clustered scenarios, which is why they have a different quorum mechanism.

The table below gives an overview of the Pool Quorum outcomes per scenario:

| SERVER NODES | CAN SURVIVE ONE SERVER NODE FAILURE | CAN SURVIVE ONE SERVER NODE FAILURE, THEN ANOTHER | CAN SURVIVE TWO SIMULTANEOUS SERVER NODE FAILURES |
|---|---|---|---|
| 2 | No | No | No |
| 2 + Witness | Yes | No | No |
| 3 | Yes | No | No |
| 3 + Witness | Yes | No | No |
| 4 | Yes | No | No |
| 4 + Witness | Yes | Yes | Yes |
| 5 and above | Yes | Yes | Yes |

## How pool quorum works

When drives fail, or when some subset of drives loses contact with another subset, surviving drives need to verify that they constitute the *majority* of the pool to remain online. If they can't verify that, they'll go offline. The pool is the entity that goes offline or stays online based on whether it has enough disks for quorum (50% + 1). The pool resource owner (active cluster node) can be the +1.

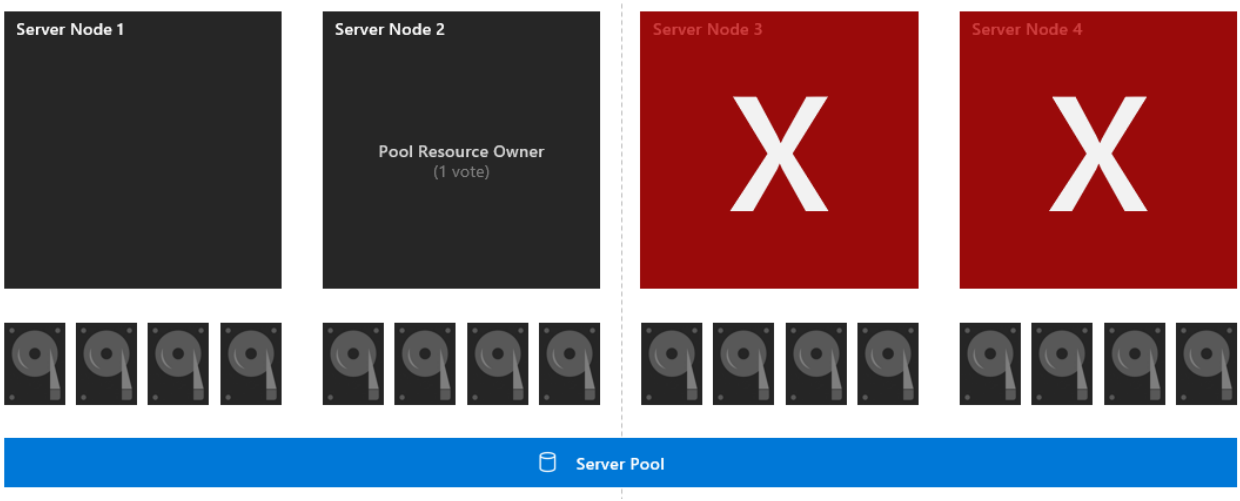
But pool quorum works differently from cluster quorum in the following ways:

- the pool uses one node in the cluster as a witness as a tie-breaker to survive half of drives gone (this node that is the pool resource owner)
- the pool does NOT have dynamic quorum
- the pool does NOT implement its own version of removing a vote

### Examples

#### Four nodes with a symmetrical layout.

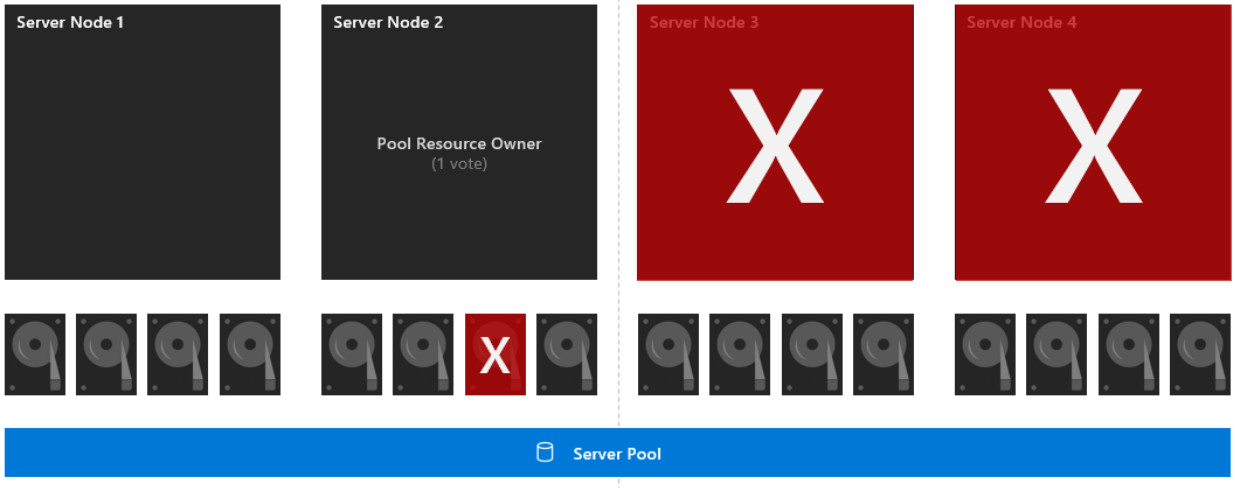
Each of the 16 drives has one vote and node two also has one vote (since it's the pool resource owner). The *majority* is determined out of a total of **16 votes**. If nodes three and four go down, the surviving subset has 8 drives and the pool resource owner, which is 9/16 votes. So, the pool survives.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Yes**.
- Can survive two server failures at once: **Yes**.

**Four nodes with a symmetrical layout and drive failure.**

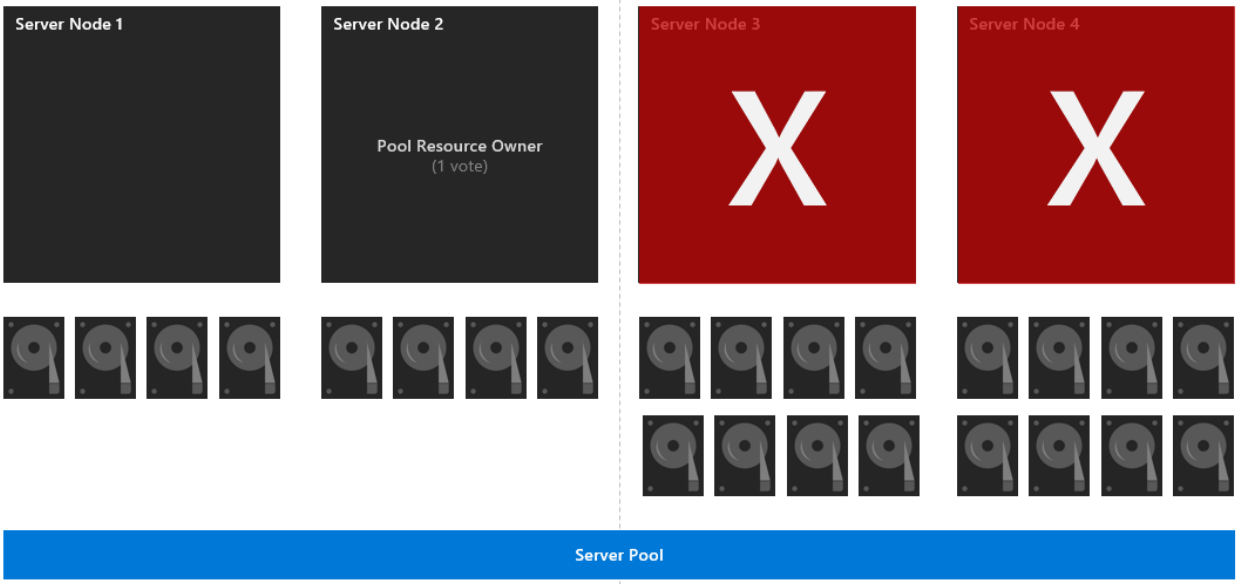
Each of the 16 drives has one vote and node 2 also has one vote (since it's the pool resource owner). The *majority* is determined out of a total of **16 votes**. First, drive 7 goes down. If nodes three and four go down, the surviving subset has 7 drives and the pool resource owner, which is 8/16 votes. So, the pool doesn't have majority and goes down.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **No**.
- Can survive two server failures at once: **No**.

**Four nodes with a non-symmetrical layout.**

Each of the 24 drives has one vote and node two also has one vote (since it's the pool resource owner). The *majority* is determined out of a total of **24 votes**. If nodes three and four go down, the surviving subset has 8 drives and the pool resource owner, which is 9/24 votes. So, the pool doesn't have majority and goes down.




- Can survive one server failure: **Yes**.
- Can survive one server failure, then another: **Depends **(cannot survive if both nodes three and four go down, but can survive all other scenarios.
- Can survive two server failures at once: **Depends **(cannot survive if both nodes three and four go down, but can survive all other scenarios.

**Pool quorum recommendations**

- Ensure that each node in your cluster is symmetrical (each node has the same number of drives)
- Enable three-way mirror or dual parity so that you can tolerate a node failures and keep the virtual disks online. See our volume guidance page for more details.
- If more than two nodes are down, or two nodes and a disk on another node are down, volumes may not have access to all three copies of their data, and therefore be taken offline and be unavailable. It's recommended to bring the servers back or replace the disks quickly to ensure the most resiliency for all the data in the volume.

## More information

- Configure and manage quorum
- Deploy a cloud witness

# Cluster sets

12/16/2020 • 23 minutes to read • Edit Online

Applies to: Windows Server 2019

Cluster sets is the new cloud scale-out technology in the Windows Server 2019 release that increases cluster node count in a single Software Defined Data Center (SDDC) cloud by orders of magnitude. A cluster set is a loosely-coupled grouping of multiple Failover Clusters: compute, storage or hyper-converged. Cluster sets technology enables virtual machine fluidity across member clusters within a cluster set and a unified storage namespace across the set in support of virtual machine fluidity.

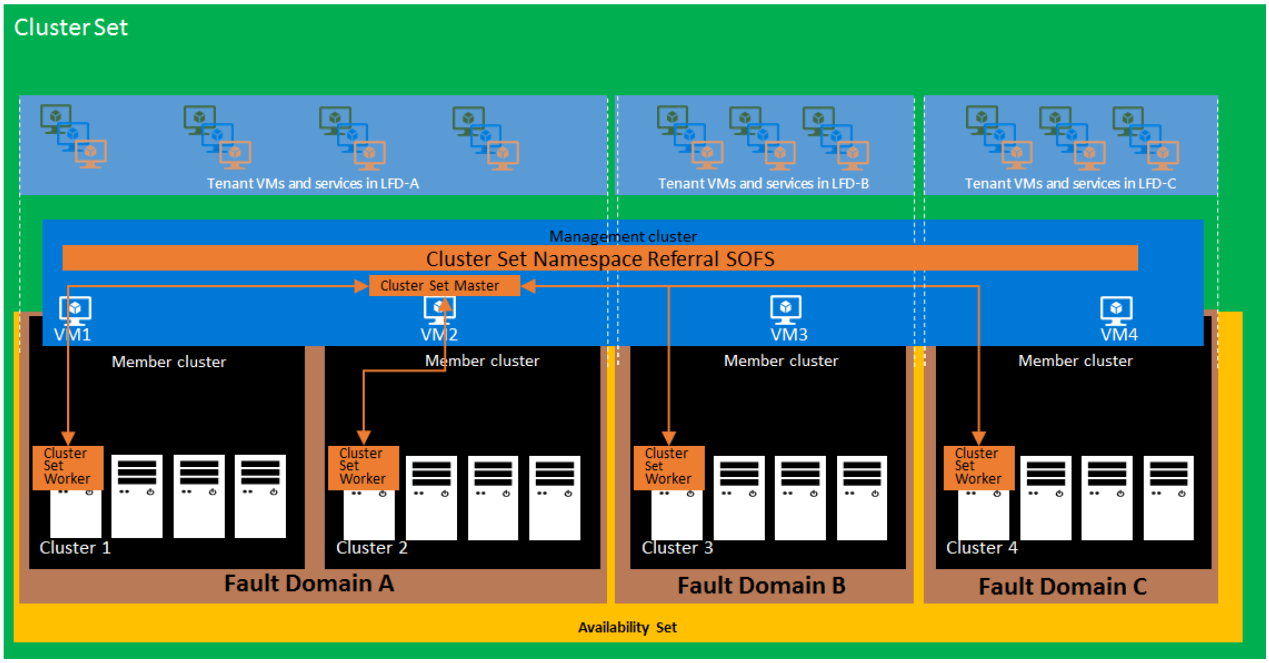
While preserving existing Failover Cluster management experiences on member clusters, a cluster set instance additionally offers key use cases around lifecycle management at the aggregate. This Windows Server 2019 Scenario Evaluation Guide provides you the necessary background information along with step-by-step instructions to evaluate cluster sets technology using PowerShell.

## Technology introduction

Cluster sets technology is developed to meet specific customer requests operating Software Defined Datacenter (SDDC) clouds at scale. Cluster sets value proposition may be summarized as the following:

- Significantly increase the supported SDDC cloud scale for running highly available virtual machines by combining multiple smaller clusters into a single large fabric, even while keeping the software fault boundary to a single cluster
- Manage entire Failover Cluster lifecycle including onboarding and retiring clusters, without impacting tenant virtual machine availability, via fluidly migrating virtual machines across this large fabric
- Easily change the compute-to-storage ratio in your hyper-converged I
- Benefit from Azure-like Fault Domains and Availability sets across clusters in initial virtual machine placement and subsequent virtual machine migration
- Mix-and-match different generations of CPU hardware into the same cluster set fabric, even while keeping individual fault domains homogeneous for maximum efficiency. Please note that the recommendation of same hardware is still present within each individual cluster as well as the entire cluster set.

From a high level view, this is what cluster sets can look like.




The following provides a quick summary of each of the elements in the above image:

### Management cluster

Management cluster in a cluster set is a Failover Cluster that hosts the highly-available management plane of the entire cluster set and the unified storage namespace (Cluster Set Namespace) referral Scale-Out File Server (SOFS). A management cluster is logically decoupled from member clusters that run the virtual machine workloads. This makes the cluster set management plane resilient to any localized cluster-wide failures, e.g. loss of power of a member cluster.

### Member cluster

A member cluster in a cluster set is typically a traditional hyper-converged cluster running virtual machine and Storage Spaces Direct workloads. Multiple member clusters participate in a single cluster set deployment, forming the larger SDDC cloud fabric. Member clusters differ from a management cluster in two key aspects: member clusters participate in fault domain and availability set constructs, and member clusters are also sized to host virtual machine and Storage Spaces Direct workloads. Cluster set virtual machines that move across cluster boundaries in a cluster set must not be hosted on the management cluster for this reason.

### Cluster set namespace referral SOFS

A cluster set namespace referral (Cluster Set Namespace) SOFS is a Scale-Out File Server wherein each SMB Share on the Cluster Set Namespace SOFS is a referral share – of type 'SimpleReferral' newly introduced in Windows Server 2019. This referral allows Server Message Block (SMB) clients access to the target SMB share hosted on the member cluster SOFS. The cluster set namespace referral SOFS is a light-weight referral mechanism and as such, does not participate in the I/O path. The SMB referrals are cached perpetually on the each of the client nodes and the cluster sets namespace dynamically updates automatically these referrals as needed.

### Cluster set master

In a cluster set, the communication between the member clusters is loosely coupled, and is coordinated by a new cluster resource called "Cluster Set Master" (CS-Master). Like any other cluster resource, CS-Master is highly available and resilient to individual member cluster failures and/or the management cluster node failures. Through a new Cluster Set WMI provider, CS-Master provides the management endpoint for all Cluster Set manageability interactions.

### Cluster set worker

In a Cluster Set deployment, the CS-Master interacts with a new cluster resource on the member Clusters called

"Cluster Set Worker" (CS-Worker). CS-Worker acts as the only liaison on the cluster to orchestrate the local cluster interactions as requested by the CS-Master. Examples of such interactions include virtual machine placement and cluster-local resource inventorying. There is only one CS-Worker instance for each of the member clusters in a cluster set.

### Fault domain

A fault domain is the grouping of software and hardware artifacts that the administrator determines could fail together when a failure does occur. While an administrator could designate one or more clusters together as a fault domain, each node could participate in a fault domain in an availability set. Cluster sets by design leaves the decision of fault domain boundary determination to the administrator who is well-versed with data center topology considerations – e.g. PDU, networking – that member clusters share.

### Availability set

An availability set helps the administrator configure desired redundancy of clustered workloads across fault domains, by organizing those into an availability set and deploying workloads into that availability set. Let's say if you are deploying a two-tier application, we recommend that you configure at least two virtual machines in an availability set for each tier which will ensure that when one fault domain in that availability set goes down, your application will at least have one virtual machine in each tier hosted on a different fault domain of that same availability set.

## Why use cluster sets

Cluster sets provides the benefit of scale without sacrificing resiliency.

Cluster sets allows for clustering multiple clusters together to create a large fabric, while each cluster remains independent for resiliency. For example, you have a several 4-node HCI clusters running virtual machines. Each cluster provides the resiliency needed for itself. If the storage or memory starts to fill up, scaling up is your next step. With scaling up, there are some options and considerations.

1. Add more storage to the current cluster. With Storage Spaces Direct, this may be tricky as the exact same model/firmware drives may not be available. The consideration of rebuild times also need to be taken into account.
2. Add more memory. What if you are maxed out on the memory the machines can handle? What if all available memory slots are full?
3. Add additional compute nodes with drives into the current cluster. This takes us back to Option 1 needing to be considered.
4. Purchase a whole new cluster

This is where cluster sets provides the benefit of scaling. If I add my clusters into a cluster set, I can take advantage of storage or memory that may be available on another cluster without any additional purchases. From a resiliency perspective, adding additional nodes to a Storage Spaces Direct is not going to provide additional votes for quorum. As mentioned here, a Storage Spaces Direct Cluster can survive the loss of 2 nodes before going down. If you have a 4-node HCI cluster, 3 nodes go down will take the entire cluster down. If you have an 8-node cluster, 3 nodes go down will take the entire cluster down. With Cluster sets that has two 4-node HCI clusters in the set, 2 nodes in one HCI go down and 1 node in the other HCI go down, both clusters remain up. Is it better to create one large 16-node Storage Spaces Direct cluster or break it down into four 4-node clusters and use cluster sets? Having four 4-node clusters with cluster sets gives the same scale, but better resiliency in that multiple compute nodes can go down (unexpectedly or for maintenance) and production remains.

## Considerations for deploying cluster sets

When considering if cluster sets is something you need to use, consider these questions:

- Do you need to go beyond the current HCI compute and storage scale limits?
- Are all compute and storage not identically the same?
- Do you live migrate virtual machines between clusters?
- Would you like Azure-like computer availability sets and fault domains across multiple clusters?
- Do you need to take the time to look at all your clusters to determine where any new virtual machines need to be placed?

If your answer is yes, then cluster sets is what you need.

There are a few other items to consider where a larger SDDC might change your overall data center strategies. SQL Server is a good example. Does moving SQL Server virtual machines between clusters require licensing SQL to run on additional nodes?

## Scale-out file server and cluster sets

In Windows Server 2019, there is a new scale-out file server role called Infrastructure Scale-Out File Server (SOFS).

The following considerations apply to an Infrastructure SOFS role:

1. There can be at most only one Infrastructure SOFS cluster role on a Failover Cluster. Infrastructure SOFS role is created by specifying the "**-Infrastructure**" switch parameter to the **Add-ClusterScaleOutFileServerRole** cmdlet. For example:

   ```
   Add-ClusterScaleoutFileServerRole -Name "my_infra_sofs_name" -Infrastructure
   ```

2. Each CSV volume created in the failover automatically triggers the creation of an SMB Share with an auto-generated name based on the CSV volume name. An administrator cannot directly create or modify SMB shares under an SOFS role, other than via CSV volume create/modify operations.

3. In hyper-converged configurations, an Infrastructure SOFS allows an SMB client (Hyper-V host) to communicate with guaranteed Continuous Availability (CA) to the Infrastructure SOFS SMB server. This hyper-converged SMB loopback CA is achieved via virtual machines accessing their virtual disk (VHDx) files where the owning virtual machine identity is forwarded between the client and server. This identity forwarding allows ACL-ing VHDx files just as in standard hyper-converged cluster configurations as before.

Once a cluster set is created, the cluster set namespace relies on an Infrastructure SOFS on each of the member clusters, and additionally an Infrastructure SOFS in the management cluster.

At the time a member cluster is added to a cluster set, the administrator specifies the name of an Infrastructure SOFS on that cluster if one already exists. If the Infrastructure SOFS does not exist, a new Infrastructure SOFS role on the new member cluster is created by this operation. If an Infrastructure SOFS role already exists on the member cluster, the Add operation implicitly renames it to the specified name as needed. Any existing singleton SMB servers, or non-Infrastructure SOFS roles on the member clusters are left unutilized by the cluster set.

At the time the cluster set is created, the administrator has the option to use an already-existing AD computer object as the namespace root on the management cluster. Cluster set creation operations create the Infrastructure SOFS cluster role on the management cluster or renames the existing Infrastructure SOFS role just as previously described for member clusters. The Infrastructure SOFS on the management cluster is used as the cluster set namespace referral (Cluster Set Namespace) SOFS. It simply means that each SMB Share on the cluster set namespace SOFS is a referral share – of type 'SimpleReferral' - newly introduced in Windows Server 2019. This referral allows SMB clients access to the target SMB share hosted on the member cluster SOFS. The cluster set namespace referral SOFS is a light-weight referral mechanism and as such, does not participate in the I/O path. The SMB referrals are cached perpetually on the each of the client nodes and the cluster sets namespace dynamically updates automatically these referrals as needed

# Creating a Cluster Set

**Prerequisites**

When creating a cluster set, you following prerequisites are recommended:

1. Configure a management client running Windows Server 2019.
2. Install the Failover Cluster tools on this management server.
3. Create cluster members (at least two clusters with at least two Cluster Shared Volumes on each cluster)
4. Create a management cluster (physical or guest) that straddles the member clusters. This approach ensures that the Cluster sets management plane continues to be available despite possible member cluster failures.

**Steps**

1. Create a new cluster set from three clusters as defined in the prerequisites. The below chart gives an example of clusters to create. The name of the cluster set in this example will be **CSMASTER**.

| CLUSTER NAME | INFRASTRUCTURE SOFS NAME TO BE USED LATER |
|---|---|
| SET-CLUSTER | SOFS-CLUSTERSET |
| CLUSTER1 | SOFS-CLUSTER1 |
| CLUSTER2 | SOFS-CLUSTER2 |

2. Once all the clusters have been created, use the following command to create the cluster set master:

```
New-ClusterSet -Name CSMASTER -NamespaceRoot SOFS-CLUSTERSET -CimSession SET-CLUSTER
```

3. Use the command set below to add a Cluster Server to the cluster set:

```
Add-ClusterSetMember -ClusterName CLUSTER1 -CimSession CSMASTER -InfraSOFSName SOFS-CLUSTER1
Add-ClusterSetMember -ClusterName CLUSTER2 -CimSession CSMASTER -InfraSOFSName SOFS-CLUSTER2
```

> **NOTE**
> If you are using a static IP Address scheme, you must include *-StaticAddress x.x.x.x* on the **New-ClusterSet** command.

4. Once you have created the cluster set out of cluster members, you can list the nodes set and its properties. To enumerate all the member clusters in the cluster set:

```
Get-ClusterSetMember -CimSession CSMASTER
```

5. To enumerate all the member clusters in the cluster set including the management cluster nodes:

```
Get-ClusterSet -CimSession CSMASTER | Get-Cluster | Get-ClusterNode
```

6. To list all the nodes from the member clusters:

```
Get-ClusterSetNode -CimSession CSMASTER
```

7. To list all the resource groups across the cluster set:

```
Get-ClusterSet -CimSession CSMASTER | Get-Cluster | Get-ClusterGroup
```

8. To verify that the cluster set creation process created one SMB share (identified as Volume1, or whatever the CSV folder is labeled with, the ScopeName being the Infrastructure File Server name and the path as both) on the Infrastructure SOFS for each cluster member's CSV volume:

```
Get-SmbShare -CimSession CSMASTER
```

9. Cluster set debug logs can be collected for review. Both the cluster set and cluster debug logs can be gathered for all members and the management cluster:

```
Get-ClusterSetLog -ClusterSetCimSession CSMASTER -IncludeClusterLog -IncludeManagementClusterLog -
DestinationFolderPath <path>
```

10. Configure Kerberos constrained delegation between all cluster set members.

11. Configure the cross-cluster virtual machine live migration authentication type to Kerberos on each node in the Cluster Set.

```
foreach($h in $hosts){ Set-VMHost -VirtualMachineMigrationAuthenticationType Kerberos -ComputerName $h
}
```

12. Add the management cluster to the local administrators group on each node in the cluster set.

```
foreach($h in $hosts){ Invoke-Command -ComputerName $h -ScriptBlock {Net localgroup administrators /add
<management_cluster_name>$} }
```

## Creating new virtual machines and adding to cluster sets

After creating the cluster set, the next step is to create new virtual machines. Normally, when it is time to create virtual machines and add them to a cluster, you need to do some checks on the clusters to see which it may be best to run on. These checks could include:

- How much memory is available on the cluster nodes?
- How much disk space is available on the cluster nodes?
- Does the virtual machine require specific storage requirements (i.e. I want my SQL Server virtual machines to go to a cluster running faster drives; or, my infrastructure virtual machine is not as critical and can run on slower drives).

Once this questions are answered, you create the virtual machine on the cluster you need it to be. One of the benefits of cluster sets is that cluster sets do those checks for you and place the virtual machine on the most optimal node.

The below commands will both identify the optimal cluster and deploy the virtual machine to it. In the below example, a new virtual machine is created specifying that at least 4 gigabytes of memory is available for the virtual machine and that it will need to utilize 1 virtual processor.

- ensure that 4gb is available for the virtual machine
- set the virtual processor used at 1
- check to ensure there is at least 10% CPU available for the virtual machine

```
# Identify the optimal node to create a new virtual machine
$memoryinMB=4096
$vpcount = 1
$targetnode = Get-ClusterSetOptimalNodeForVM -CimSession CSMASTER -VMMemory $memoryinMB -VMVirtualCoreCount
$vpcount -VMCpuReservation 10
$secure_string_pwd = convertto-securestring "<password>" -asplaintext -force
$cred = new-object -typename System.Management.Automation.PSCredential ("<domain\account>",$secure_string_pwd)

# Deploy the virtual machine on the optimal node
Invoke-Command -ComputerName $targetnode.name -scriptblock { param([String]$storagepath); New-VM CSVM1 -
MemoryStartupBytes 3072MB -path $storagepath -NewVHDPath CSVM.vhdx -NewVHDSizeBytes 4194304 } -ArgumentList
@("\\SOFS-CLUSTER1\VOLUME1") -Credential $cred | Out-Null

Start-VM CSVM1 -ComputerName $targetnode.name | Out-Null
Get-VM CSVM1 -ComputerName $targetnode.name | fl State, ComputerName
```

When it completes, you will be given the information about the virtual machine and where it was placed. In the above example, it would show as:

```
State         : Running
ComputerName  : 1-S2D2
```

If you were to have not enough memory, CPU capacity, or disk space to add the virtual machine, you will receive the following error:

```
Get-ClusterSetOptimalNodeForVM : A cluster node is not available for this operation.
```

Once the virtual machine has been created, it will be displayed in Hyper-V manager on the specific node specified. To add it as a cluster set virtual machine, and add it to the cluster, use the command below:

```
Register-ClusterSetVM -CimSession CSMASTER -MemberName $targetnode.Member -VMName CSVM1
```

When it completes, the output will be:

```
Id  VMName  State  MemberName  PSComputerName
--  ------  -----  ----------  --------------
 1  CSVM1     On   CLUSTER1    CSMASTER
```

If you have added a cluster with existing virtual machines, the virtual machines will also need to be registered with Cluster sets. To register all those virtual machines at once, the command to use is:

```
Get-ClusterSetMember -Name CLUSTER3 -CimSession CSMASTER | Register-ClusterSetVM -RegisterAll -CimSession
CSMASTER
```

However, the process is not yet complete, as the path to the virtual machine needs to be added to the cluster set namespace.

For example: An existing cluster is added and it has pre-configured virtual machines which reside on the local Cluster Shared Volume (CSV). The path for the VHDX would be something similar to "C:\ClusterStorage\Volume1\MYVM\Virtual Hard Disks\MYVM.vhdx". A storage migration would need to be accomplished, as CSV paths are by design local to a single member cluster and will therefore not be accessible to the virtual machine once they are live migrated across member clusters.

In this example, CLUSTER3 was added to the cluster set using Add-ClusterSetMember with the Infrastructure

Scale-Out File Server as SOFS-CLUSTER3. To move the virtual machine configuration and storage, the command is:

```
Move-VMStorage -DestinationStoragePath \\SOFS-CLUSTER3\Volume1 -Name MYVM
```

Once it completes, you will receive a warning:

```
WARNING: There were issues updating the virtual machine configuration that may prevent the virtual machine
from running. For more information view the report file below.
WARNING: Report file location: C:\Windows\Cluster\Reports\Update-ClusterVirtualMachineConfiguration '' on date
at time.htm.
```

This warning can be ignored as the warning is "No changes in the virtual machine role storage configuration were detected". The reason for the warning as the actual physical location does not change; only the configuration paths.

For more information on Move-VMStorage, please review this link.

Live migrating a virtual machine between different cluster set clusters is not the same as in the past. In non-cluster set scenarios, the steps would be:

1. remove the virtual machine role from the Cluster.
2. live migrate the virtual machine to a member node of a different cluster.
3. add the virtual machine into the cluster as a new virtual machine role.

With Cluster sets these steps are not necessary and only one command is needed. First, you should set all networks to be available for the migration with the command:

```
Set-VMHost -UseAnyNetworkForMigration $true
```

For example, I want to move a Cluster Set virtual machine from CLUSTER1 to NODE2-CL3 on CLUSTER3. The single command would be:

```
Move-ClusterSetVM -CimSession CSMASTER -VMName CSVM1 -Node NODE2-CL3
```

Please note that this does not move the virtual machine storage or configuration files. This is not necessary as the path to the virtual machine remains as \\SOFS-CLUSTER1\VOLUME1. Once a virtual machine has been registered with cluster sets has the Infrastructure File Server share path, the drives and virtual machine do not require being on the same machine as the virtual machine.

## Creating Availability sets Fault Domains

As described in the introduction, Azure-like fault domains and availability sets can be configured in a cluster set. This is beneficial for initial virtual machine placements and migrations between clusters.

In the example below, there are four clusters participating in the cluster set. Within the set, a logical fault domain will be created with two of the clusters and a fault domain created with the other two clusters. These two fault domains will comprise the Availabiilty Set.

In the example below, CLUSTER1 and CLUSTER2 will be in a fault domain called **FD1** while CLUSTER3 and CLUSTER4 will be in a fault domain called **FD2**. The availability set will be called **CSMASTER-AS** and be comprised of the two fault domains.

To create the fault domains, the commands are:

```
New-ClusterSetFaultDomain -Name FD1 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER1,CLUSTER2 -
Description "This is my first fault domain"

New-ClusterSetFaultDomain -Name FD2 -FdType Logical -CimSession CSMASTER -MemberCluster CLUSTER3,CLUSTER4 -
Description "This is my second fault domain"
```

To ensure they have been created successfully, Get-ClusterSetFaultDomain can be run with its output shown.

```
PS C:\> Get-ClusterSetFaultDomain -CimSession CSMASTER -FdName FD1 | fl *

PSShowComputerName    : True
FaultDomainType       : Logical
ClusterName           : {CLUSTER1, CLUSTER2}
Description           : This is my first fault domain
FDName                : FD1
Id                    : 1
PSComputerName        : CSMASTER
```

Now that the fault domains have been created, the availability set needs to be created.

```
New-ClusterSetAvailabilitySet -Name CSMASTER-AS -FdType Logical -CimSession CSMASTER -ParticipantName FD1,FD2
```

To validate it has been created, then use:

```
Get-ClusterSetAvailabilitySet -AvailabilitySetName CSMASTER-AS -CimSession CSMASTER
```

When creating new virtual machines, you would then need to use the -AvailabilitySet parameter as part of determining the optimal node. So it would then look something like this:

```
# Identify the optimal node to create a new virtual machine
$memoryinMB=4096
$vpcount = 1
$av = Get-ClusterSetAvailabilitySet -Name CSMASTER-AS -CimSession CSMASTER
$targetnode = Get-ClusterSetOptimalNodeForVM -CimSession CSMASTER -VMMemory $memoryinMB -VMVirtualCoreCount
$vpcount -VMCpuReservation 10 -AvailabilitySet $av
$secure_string_pwd = convertto-securestring "<password>" -asplaintext -force
$cred = new-object -typename System.Management.Automation.PSCredential ("<domain\account>",$secure_string_pwd)
```

Removing a cluster from cluster sets due to various life cycles. There are times when a cluster needs to be removed from a cluster set. As a best practice, all cluster set virtual machines should be moved out of the cluster. This can be accomplished using the **Move-ClusterSetVM** and **Move-VMStorage** commands.

However, if the virtual machines will not be moved as well, cluster sets runs a series of actions to provide an intuitive outcome to the administrator. When the cluster is removed from the set, all remaining cluster set virtual machines hosted on the cluster being removed will simply become highly available virtual machines bound to that cluster, assuming they have access to their storage. Cluster sets will also automatically update its inventory by:

- No longer tracking the health of the now-removed cluster and the virtual machines running on it
- Removes from cluster set namespace and all references to shares hosted on the now-removed cluster

For example, the command to remove the CLUSTER1 cluster from cluster sets would be:

```
Remove-ClusterSetMember -ClusterName CLUSTER1 -CimSession CSMASTER
```

# Frequently asked questions (FAQ)

**Question:** In my cluster set, am I limited to only using hyper-converged clusters?
**Answer:** No. You can mix Storage Spaces Direct with traditional clusters.

**Question:** Can I manage my Cluster Set via System Center Virtual Machine Manager?
**Answer:** System Center Virtual Machine Manager does not currently support Cluster sets

**Question:** Can Windows Server 2012 R2 or 2016 clusters co-exist in the same cluster set?
**Question:** Can I migrate workloads off Windows Server 2012 R2 or 2016 clusters by simply having those clusters join the same Cluster Set?
**Answer:** Cluster sets is a new technology being introduced in Windows Server 2019, so as such, does not exist in previous releases. Down-level OS-based clusters cannot join a cluster set. However, Cluster Operating System rolling upgrades technology should provide the migration functionality that you are looking for by upgrading these clusters to Windows Server 2019.

**Question:** Can Cluster sets allow me to scale storage or compute (alone)?
**Answer:** Yes, by simply adding a Storage Space Direct or traditional Hyper-V cluster. With cluster sets, it is a straightforward change of Compute-to-Storage ratio even in a hyper-converged cluster set.

**Question:** What is the management tooling for cluster sets
**Answer:** PowerShell or WMI in this release.

**Question:** How will the cross-cluster live migration work with processors of different generations?
**Answer:** Cluster sets does not work around processor differences and supersede what Hyper-V currently supports. Therefore, processor compatibility mode must be used with quick migrations. The recommendation for Cluster sets is to use the same processor hardware within each individual Cluster as well as the entire Cluster Set for live migrations between clusters to occur.

**Question:** Can my cluster set virtual machines automatically failover on a cluster failure?
**Answer:** In this release, cluster set virtual machines can only be manually live-migrated across clusters; but cannot automatically failover.

**Question:** How do we ensure storage is resilient to cluster failures?
**Answer:** Use cross-cluster Storage Replica (SR) solution across member clusters to realize the storage resiliency to cluster failures.

**Question:** I use Storage Replica (SR) to replicate across member clusters. Do cluster set namespace storage UNC paths change on SR failover to the replica target Storage Spaces Direct cluster?
**Answer:** In this release, such a cluster set namespace referral change does not occur with SR failover. Please let Microsoft know if this scenario is critical to you and how you plan to use it.

**Question:** Is it possible to failover virtual machines across fault domains in a disaster recovery situation (say the entire fault domain went down)?
**Answer:** No, note that cross-cluster failover within a logical fault domain is not yet supported.

**Question:** Can my cluster set span clusters in multiple sites (or DNS domains)?
**Answer:** This is an untested scenario and not immediately planned for production support. Please let Microsoft know if this scenario is critical to you and how you plan to use it.

**Question:** Does cluster set work with IPv6?
**Answer:** Both IPv4 and IPv6 are supported with cluster sets as with Failover Clusters.

**Question:** What are the Active Directory Forest requirements for cluster sets
**Answer:** All member clusters must be in the same AD forest.

**Question:** How many clusters or nodes can be part of a single cluster Set?

**Answer:** In Windows Server 2019, cluster sets been tested and supported up to 64 total cluster nodes. However, cluster sets architecture scales to much larger limits and is not something that is hardcoded for a limit. Please let Microsoft know if larger scale is critical to you and how you plan to use it.

**Question:** Will all Storage Spaces Direct clusters in a cluster set form a single storage pool?
**Answer:** No. Storage Spaces Direct technology still operates within a single cluster and not across member clusters in a cluster set.

**Question:** Is the cluster set namespace highly available?
**Answer:** Yes, the cluster set namespace is provided via a Continuously Available (CA) referral SOFS namespace server running on the management cluster. Microsoft recommends having enough number of virtual machines from member clusters to make it resilient to localized cluster-wide failures. However, to account for unforeseen catastrophic failures – e.g. all virtual machines in the management cluster going down at the same time – the referral information is additionally persistently cached in each cluster set node, even across reboots.

**Question:** Does the cluster set namespace-based storage access slow down storage performance in a cluster set?
**Answer:** No. Cluster set namespace offers an overlay referral namespace within a cluster set – conceptually like Distributed File System Namespaces (DFSN). And unlike DFSN, all cluster set namespace referral metadata is auto-populated and auto-updated on all nodes without any administrator intervention, so there is almost no performance overhead in the storage access path.

**Question:** How can I backup cluster set metadata?
**Answer:** This guidance is the same as that of Failover Cluster. The System State Backup will backup the cluster state as well. Through Windows Server Backup, you can do restores of just a node's cluster database (which should never be needed because of a bunch of self-healing logic we have) or do an authoritative restore to roll back the entire cluster database across all nodes. In the case of cluster sets, Microsoft recommends doing such an authoritative restore first on the member cluster and then the management cluster if needed.

# Storage Spaces Direct hardware requirements

11/2/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic describes minimum hardware requirements for Storage Spaces Direct on Windows Server. For hardware requirements on Azure Stack HCI, our operating system designed for hyperconverged deployments with a connection to the cloud, see Before you deploy Azure Stack HCI: Determine hardware requirements.

For production, Microsoft recommends purchasing a validated hardware/software solution from our partners, which include deployment tools and procedures. These solutions are designed, assembled, and validated against our reference architecture to ensure compatibility and reliability, so you get up and running quickly. For Windows Server 2019 solutions, visit the Azure Stack HCI solutions website. For Windows Server 2016 solutions, learn more at Windows Server Software-Defined.

> **TIP**
> Want to evaluate Storage Spaces Direct but don't have hardware? Use Hyper-V or Azure virtual machines as described in Using Storage Spaces Direct in guest virtual machine clusters.

## Base requirements

Systems, components, devices, and drivers must be certified for the operating system you're using in the Windows Server Catalog. In addition, we recommend that servers, drives, host bus adapters, and network adapters have the **Software-Defined Data Center (SDDC) Standard** and/or **Software-Defined Data Center (SDDC) Premium** additional qualifications (AQs), as pictured below. There are over 1,000 components with the SDDC AQs.


The fully configured cluster (servers, networking, and storage) must pass all cluster validation tests per the wizard in Failover Cluster Manager or with the `Test-Cluster` cmdlet in PowerShell.

In addition, the following requirements apply:

## Servers

- Minimum of 2 servers, maximum of 16 servers
- Recommended that all servers be the same manufacturer and model

## CPU

- Intel Nehalem or later compatible processor; or
- AMD EPYC or later compatible processor

## Memory

- Memory for Windows Server, VMs, and other apps or workloads; plus
- 4 GB of RAM per terabyte (TB) of cache drive capacity on each server, for Storage Spaces Direct metadata

## Boot

- Any boot device supported by Windows Server, which now includes SATADOM
- RAID 1 mirror is **not** required, but is supported for boot
- Recommended: 200 GB minimum size

## Networking

Storage Spaces Direct requires a reliable high bandwidth, low latency network connection between each node.

Minimum interconnect for small scale 2-3 node

- 10 Gbps network interface card (NIC), or faster
- Two or more network connections from each node recommended for redundancy and performance

Recommended interconnect for high performance, at scale, or deployments of 4+

- NICs that are remote-direct memory access (RDMA) capable, iWARP (recommended) or RoCE
- Two or more network connections from each node recommended for redundancy and performance
- 25 Gbps NIC or faster

Switched or switchless node interconnects

- Switched: Network switches must be properly configured to handle the bandwidth and networking type. If using RDMA that implements the RoCE protocol, network device and switch configuration is even more important.
- Switchless: Nodes can be interconnected using direct connections, avoiding using a switch. It is required that every node have a direct connection with every other node of the cluster.

## Drives

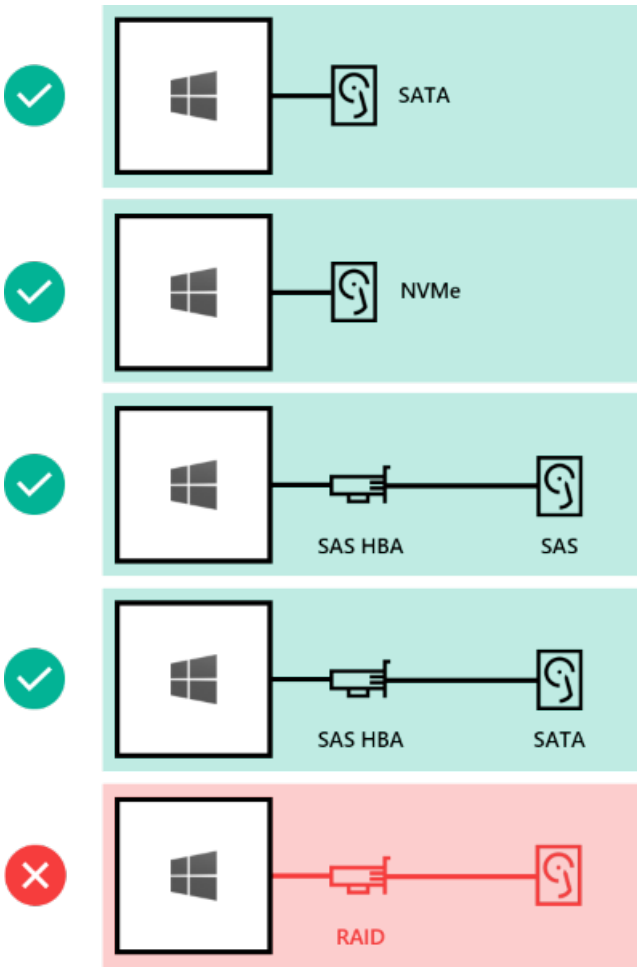
Storage Spaces Direct works with direct-attached SATA, SAS, NVMe, or persistent memory (PMem) drives that are physically attached to just one server each. For more help choosing drives, see the Choosing drives and Understand and deploy persistent memory topics.

- SATA, SAS, persistent memory, and NVMe (M.2, U.2, and Add-In-Card) drives are all supported
- 512n, 512e, and 4K native drives are all supported
- Solid-state drives must provide power-loss protection
- Same number and types of drives in every server – see Drive symmetry considerations
- Cache devices must be 32 GB or larger
- Persistent memory devices are used in block storage mode
- When using persistent memory devices as cache devices, you must use NVMe or SSD capacity devices (you can't use HDDs)
- NVMe driver is the Microsoft-provided one included in Windows (stornvme.sys)

- Recommended: Number of capacity drives is a whole multiple of the number of cache drives
- Recommended: Cache drives should have high write endurance: at least 3 drive-writes-per-day (DWPD) or at least 4 terabytes written (TBW) per day – see Understanding drive writes per day (DWPD), terabytes written (TBW), and the minimum recommended for Storage Spaces Direct

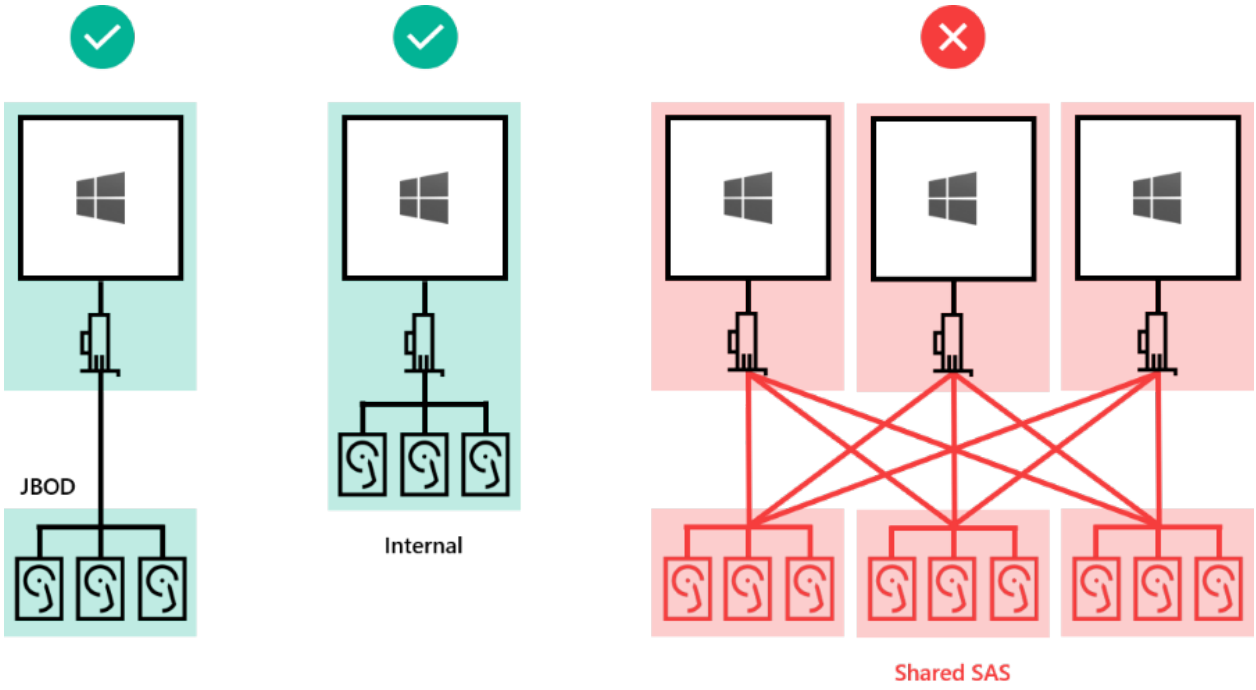
Here's how drives can be connected for Storage Spaces Direct:

- Direct-attached SATA drives
- Direct-attached NVMe drives
- SAS host-bus adapter (HBA) with SAS drives
- SAS host-bus adapter (HBA) with SATA drives
- **NOT SUPPORTED:** RAID controller cards or SAN (Fibre Channel, iSCSI, FCoE) storage. Host-bus adapter (HBA) cards must implement simple pass-through mode.




Drives can be internal to the server, or in an external enclosure that is connected to just one server. SCSI Enclosure Services (SES) is required for slot mapping and identification. Each external enclosure must present a unique identifier (Unique ID).

- Drives internal to the server
- Drives in an external enclosure ("JBOD") connected to one server
- **NOT SUPPORTED:** Shared SAS enclosures connected to multiple servers or any form of multi-path IO (MPIO) where drives are accessible by multiple paths.




### Minimum number of drives (excludes boot drive)

- If there are drives used as cache, there must be at least 2 per server
- There must be at least 4 capacity (non-cache) drives per server

| DRIVE TYPES PRESENT | MINIMUM NUMBER REQUIRED |
|---|---|
| All persistent memory (same model) | 4 persistent memory |
| All NVMe (same model) | 4 NVMe |
| All SSD (same model) | 4 SSD |
| Persistent memory + NVMe or SSD | 2 persistent memory + 4 NVMe or SSD |
| NVMe + SSD | 2 NVMe + 4 SSD |
| NVMe + HDD | 2 NVMe + 4 HDD |
| SSD + HDD | 2 SSD + 4 HDD |
| NVMe + SSD + HDD | 2 NVMe + 4 Others |

> **NOTE**
> This table provides the minimum for hardware deployments. If you're deploying with virtual machines and virtualized storage, such as in Microsoft Azure, see Using Storage Spaces Direct in guest virtual machine clusters.

### Maximum capacity

| MAXIMUMS | WINDOWS SERVER 2019 | WINDOWS SERVER 2016 |
|---|---|---|
| Raw capacity per server | 400 TB | 100 TB |

| MAXIMUMS | WINDOWS SERVER 2019 | WINDOWS SERVER 2016 |
| --- | --- | --- |
| Pool capacity | 4 PB (4,000 TB) | 1 PB |

# Using Storage Spaces Direct with the CSV in-memory read cache

12/16/2020 • 2 minutes to read • Edit Online

Applies To: Windows Server 2019, Windows Server 2016

This topic describes how to use system memory to boost the performance of Storage Spaces Direct.

Storage Spaces Direct is compatible with the Cluster Shared Volume (CSV) in-memory read cache. Using system memory to cache reads can improve performance for applications like Hyper-V, which uses unbuffered I/O to access VHD or VHDX files. (Unbuffered IOs are any operations that are not cached by the Windows Cache Manager.)

Because the in-memory cache is server-local, it improves data locality for hyper-converged Storage Spaces Direct deployments: recent reads are cached in memory on the same host where the virtual machine is running, reducing how often reads go over the network. This results in lower latency and better storage performance.

## Planning considerations

The in-memory read cache is most effective for read-intensive workloads, such as Virtual Desktop Infrastructure (VDI). Conversely, if the workload is extremely write-intensive, the cache may introduce more overhead than value and should be disabled.

You can use up to 80% of total physical memory for the CSV in-memory read cache.

> **TIP**
> For hyper-converged deployments, where compute and storage run on the same servers, be careful to leave enough memory for your virtual machines. For converged Scale-Out File Server (SoFS) deployments, with less contention for memory, this doesn't apply.

> **NOTE**
> Certain microbenchmarking tools like DISKSPD and VM Fleet may produce worse results with the CSV in-memory read cache enabled than without it. By default VM Fleet creates one 10 gibibyte (GiB) VHDX per virtual machine – approximately 1 TiB total for 100 VMs – and then performs *uniformly random* reads and writes to them. Unlike real workloads, the reads don't follow any predictable or repetitive pattern, so the in-memory cache is not effective and just incurs overhead.

## Configuring the in-memory read cache

The CSV in-memory read cache is available in Windows Server 2019 and Windows Server 2016 with the same functionality. In Windows Server 2019, it's on by default with 1 GiB allocated. In Windows Server 2016, it's off by default.

| OS VERSION | DEFAULT CSV CACHE SIZE |
|---|---|
| Windows Server 2019 | 1 GiB |

| OS VERSION | DEFAULT CSV CACHE SIZE |
| --- | --- |
| Windows Server 2016 | 0 (disabled) |
| Windows Server 2012 R2 | enabled - user must specify size |
| Windows Server 2012 | 0 (disabled) |

To see how much memory is allocated using PowerShell, run:

```
(Get-Cluster).BlockCacheSize
```

The value returned is in mebibytes (MiB) per server. For example, `1024` represents 1 gibibyte (GiB).

To change how much memory is allocated, modify this value using PowerShell. For example, to allocate 2 GiB per server, run:

```
(Get-Cluster).BlockCacheSize = 2048
```

For changes to take effect immediately, pause then resume your CSV volumes, or move them between servers. For example, use this PowerShell fragment to move each CSV to another server node and back again:

```
Get-ClusterSharedVolume | ForEach {
    $Owner = $_.OwnerNode
    $_ | Move-ClusterSharedVolume
    $_ | Move-ClusterSharedVolume -Node $Owner
}
```

## Additional References

- Storage Spaces Direct overview

# Choosing drives for Storage Spaces Direct

12/16/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic provides guidance on how to choose drives for Storage Spaces Direct to meet your performance and capacity requirements.

## Drive types

Storage Spaces Direct currently works with four types of drives:

| | |
|---|---|
|  | **PMem** refers to persistent memory, a new type of low latency, high performance storage. |
|  | **NVMe** (Non-Volatile Memory Express) refers to solid-state drives that sit directly on the PCIe bus. Common form factors are 2.5" U.2, PCIe Add-In-Card (AIC), and M.2. NVMe offers higher IOPS and IO throughput with lower latency than any other type of drive we support today except persistent memory. |
|  | **SSD** refers to solid-state drives which connect via conventional SATA or SAS. |
|  | **HDD** refers to rotational, magnetic hard disk drives which offer vast storage capacity. |

## Built-in cache

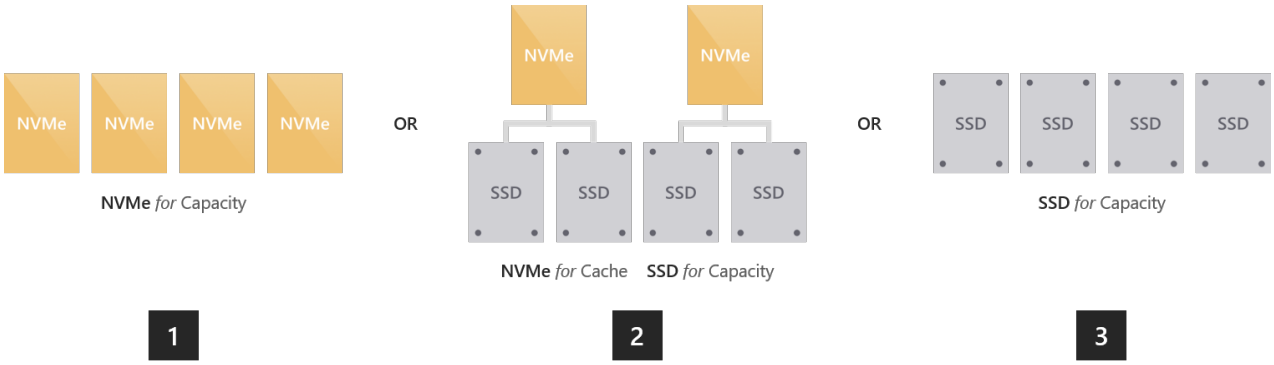
Storage Spaces Direct features a built-in server-side cache. It is a large, persistent, real-time read and write cache. In deployments with multiple types of drives, it is configured automatically to use all drives of the "fastest" type. The remaining drives are used for capacity.

For more information, check out Understanding the cache in Storage Spaces Direct.

## Option 1 – Maximizing performance

To achieve predictable and uniform sub-millisecond latency across random reads and writes to any data, or to achieve extremely high IOPS (we've done over six million!) or IO throughput (we've done over 1 Tb/s!), you should go "all-flash".

There are currently three ways to do so:




1. **All NVMe.** Using all NVMe provides unmatched performance, including the most predictable low latency. If all your drives are the same model, there is no cache. You can also mix higher-endurance and lower-endurance NVMe models, and configure the former to cache writes for the latter (requires set-up).

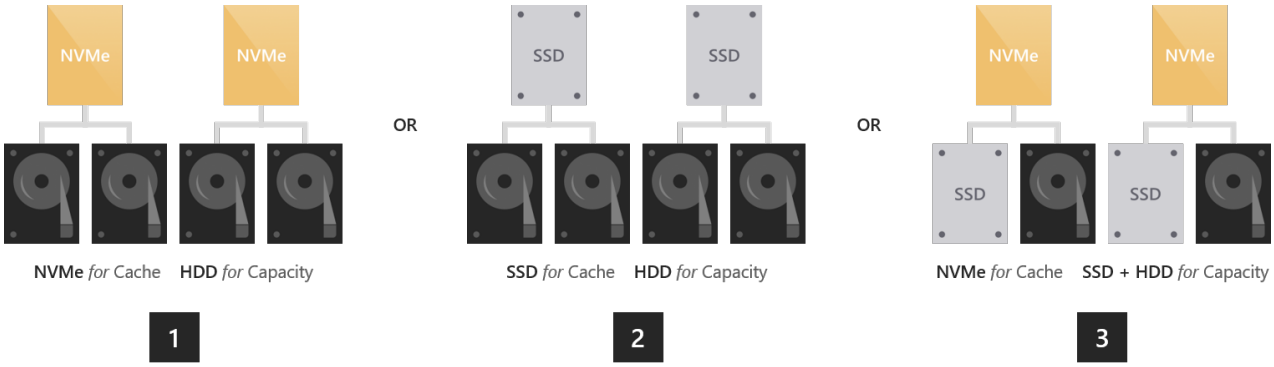
2. **NVMe + SSD.** Using NVMe together with SSDs, the NVMe will automatically cache writes to the SSDs. This allows writes to coalesce in cache and be de-staged only as needed, to reduce wear on the SSDs. This provides NVMe-like write characteristics, while reads are served directly from the also-fast SSDs.

3. **All SSD.** As with All-NVMe, there is no cache if all your drives are the same model. If you mix higher-endurance and lower-endurance models, you can configure the former to cache writes for the latter (requires set-up).

> **NOTE**
> An advantage to using all-NVMe or all-SSD with no cache is that you get usable storage capacity from every drive. There is no capacity "spent" on caching, which may be appealing at smaller scale.

## Option 2 – Balancing performance and capacity

For environments with a variety of applications and workloads, some with stringent performance requirements and others requiring considerable storage capacity, you should go "hybrid" with either NVMe or SSDs caching for larger HDDs.




1. **NVMe + HDD**. The NVMe drives will accelerate reads and writes by caching both. Caching reads allows the HDDs to focus on writes. Caching writes absorbs bursts and allows writes to coalesce and be de-staged only as needed, in an artificially serialized manner that maximizes HDD IOPS and IO throughput. This provides NVMe-like write characteristics, and for frequently or recently read data, NVMe-like read characteristics too.

2. **SSD + HDD**. Similar to the above, the SSDs will accelerate reads and writes by caching both. This provides SSD-like write characteristics, and SSD-like read characteristics for frequently or recently read data.

   There is one additional, rather exotic option: to use drives of *all three* types.

3. **NVMe + SSD + HDD.** With drives of all three types, the NVMe drives cache for both the SSDs and HDDs. The appeal is that you can create volumes on the SSDs, and volumes on the HDDs, side-by-side in the same

cluster, all accelerated by NVMe. The former are exactly as in an "all-flash" deployment, and the latter are exactly as in the "hybrid" deployments described above. This is conceptually like having two pools, with largely independent capacity management, failure and repair cycles, and so on.

> **IMPORTANT**
> We recommend using the SSD tier to place your most performance-sensitive workloads on all-flash.

## Option 3 – Maximizing capacity

For workloads which require vast capacity and write infrequently, such as archival, backup targets, data warehouses or "cold" storage, you should combine a few SSDs for caching with many larger HDDs for capacity.


1. **SSD + HDD**. The SSDs will cache reads and writes, to absorb bursts and provide SSD-like write performance, with optimized de-staging later to the HDDs.

> **IMPORTANT**
> Configuration with HDDs only is not supported. High endurance SSDs caching to low endurance SSDs is not advised.

## Sizing considerations

**Cache**

Every server must have at least two cache drives (the minimum required for redundancy). We recommend making the number of capacity drives a multiple of the number of cache drives. For example, if you have 4 cache drives, you will experience more consistent performance with 8 capacity drives (1:2 ratio) than with 7 or 9.

The cache should be sized to accommodate the working set of your applications and workloads, i.e. all the data they are actively reading and writing at any given time. There is no cache size requirement beyond that. For deployments with HDDs, a fair starting place is 10% of capacity – for example, if each server has 4 x 4 TB HDD = 16 TB of capacity, then 2 x 800 GB SSD = 1.6 TB of cache per server. For all-flash deployments, especially with very high endurance SSDs, it may be fair to start closer to 5% of capacity – for example, if each server has 24 x 1.2 TB SSD = 28.8 TB of capacity, then 2 x 750 GB NVMe = 1.5 TB of cache per server. You can always add or remove cache drives later to adjust.

**General**

We recommend limiting the total storage capacity per server to approximately 400 terabytes (TB). The more storage capacity per server, the longer the time required to resync data after downtime or rebooting, such when applying software updates. The current maximum size per storage pool is 4 petabyte (PB) (4,000 TB) for Windows Server 2019, or 1 petabyte for Windows Server 2016.

## Additional References

- Storage Spaces Direct overview
- Understand the cache in Storage Spaces Direct
- Storage Spaces Direct hardware requirements
- Planning volumes in Storage Spaces Direct
- Fault tolerance and storage efficiency

# Planning volumes in Storage Spaces Direct

12/16/2020 • 10 minutes to read • Edit Online

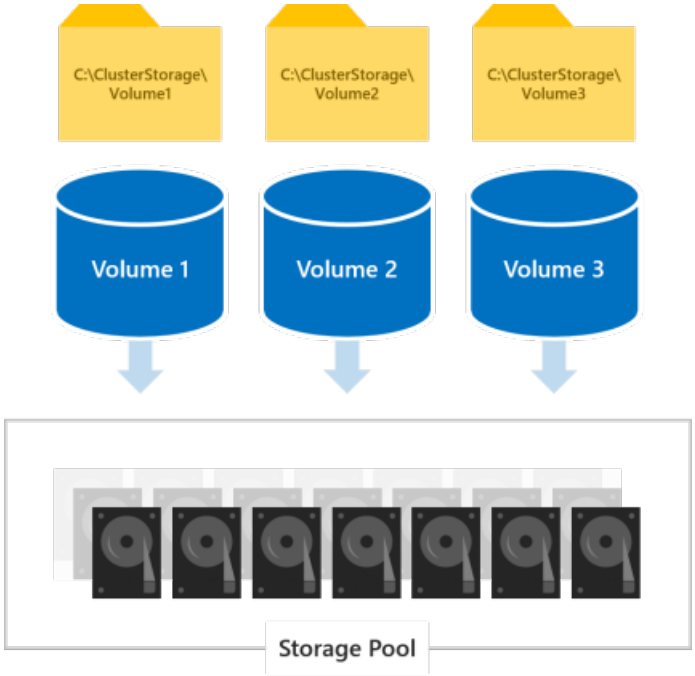
Applies to: Windows Server 2019, Windows Server 2016

This topic provides guidance for how to plan volumes in Storage Spaces Direct to meet the performance and capacity needs of your workloads, including choosing their filesystem, resiliency type, and size.

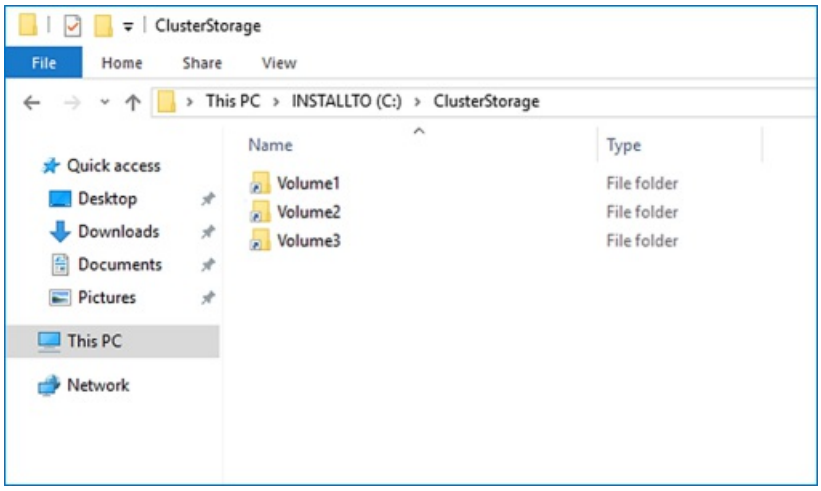
## Review: What are volumes

Volumes are where you put the files your workloads need, such as VHD or VHDX files for Hyper-V virtual machines. Volumes combine the drives in the storage pool to introduce the fault tolerance, scalability, and performance benefits of Storage Spaces Direct.

> **NOTE**
>
> Throughout documentation for Storage Spaces Direct, we use term "volume" to refer jointly to the volume and the virtual disk under it, including functionality provided by other built-in Windows features such as Cluster Shared Volumes (CSV) and ReFS. Understanding these implementation-level distinctions is not necessary to plan and deploy Storage Spaces Direct successfully.




All volumes are accessible by all servers in the cluster at the same time. Once created, they show up at **C:\ClusterStorage** on all servers.




## Choosing how many volumes to create

We recommend making the number of volumes a multiple of the number of servers in your cluster. For example, if you have 4 servers, you will experience more consistent performance with 4 total volumes than with 3 or 5. This allows the cluster to distribute volume "ownership" (one server handles metadata orchestration for each volume) evenly among servers.

We recommend limiting the total number of volumes to:

| WINDOWS SERVER 2016 | WINDOWS SERVER 2019 |
| --- | --- |
| Up to 32 volumes per cluster | Up to 64 volumes per cluster |

## Choosing the filesystem

We recommend using the new Resilient File System (ReFS) for Storage Spaces Direct. ReFS is the premier filesystem purpose-built for virtualization and offers many advantages, including dramatic performance accelerations and built-in protection against data corruption. It supports nearly all key NTFS features, including Data Deduplication in Windows Server, version 1709 and later. See the ReFS feature comparison table for details.

If your workload requires a feature that ReFS doesn't support yet, you can use NTFS instead.

> **TIP**
> Volumes with different file systems can coexist in the same cluster.

## Choosing the resiliency type

Volumes in Storage Spaces Direct provide resiliency to protect against hardware problems, such as drive or server failures, and to enable continuous availability throughout server maintenance, such as software updates.

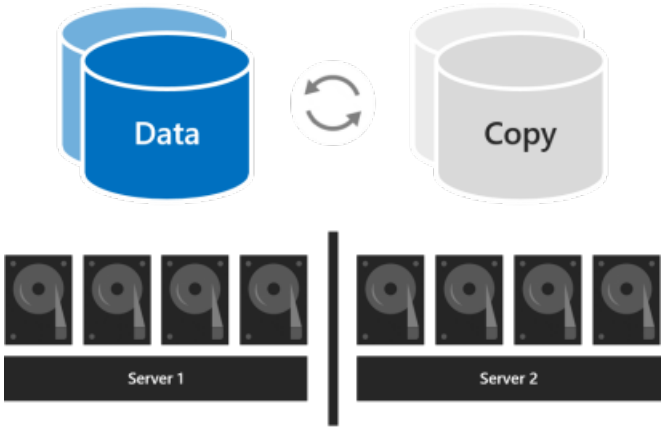
> **NOTE**
> Which resiliency types you can choose is independent of which types of drives you have.

**With two servers**

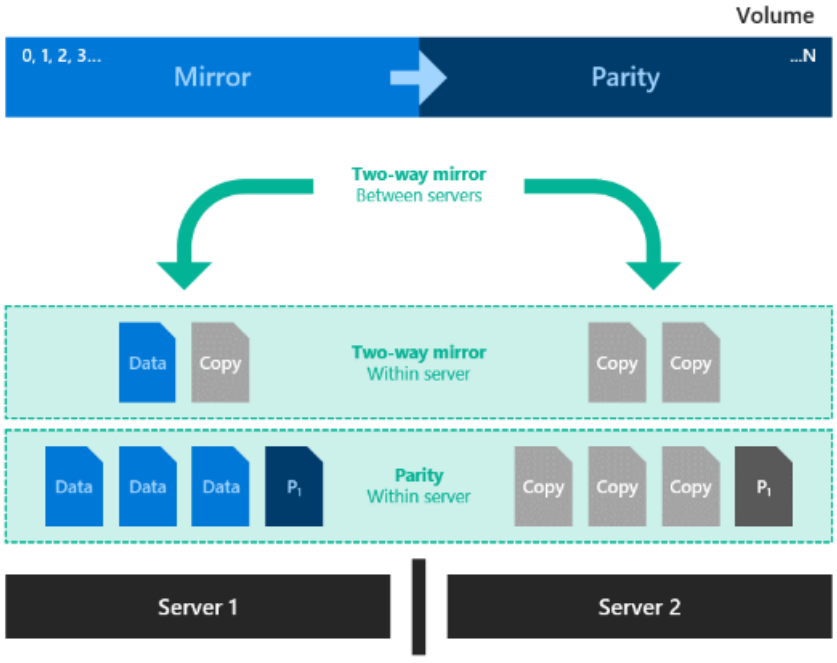
With two servers in the cluster, you can use two-way mirroring. If you're running Windows Server 2019, you can also use nested resiliency.

Two-way mirroring keeps two copies of all data, one copy on the drives in each server. Its storage efficiency is

50%—to write 1 TB of data, you need at least 2 TB of physical storage capacity in the storage pool. Two-way mirroring can safely tolerate one hardware failure at a time (one server or drive).

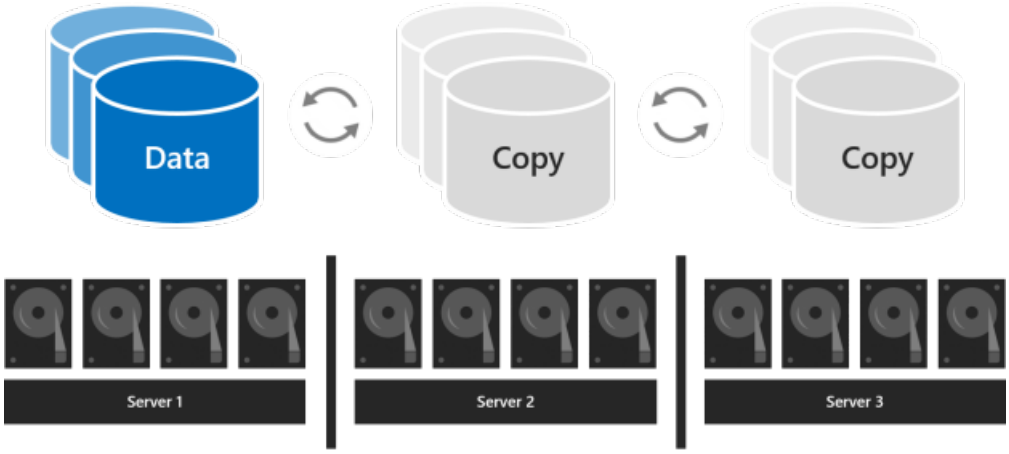



Nested resiliency (available only on Windows Server 2019) provides data resiliency between servers with two-way mirroring, then adds resiliency within a server with two-way mirroring or mirror-accelerated parity. Nesting provides data resilience even when one server is restarting or unavailable. Its storage efficiency is 25% with nested two-way mirroring and around 35-40% for nested mirror-accelerated parity. Nested resiliency can safely tolerate two hardware failures at a time (two drives, or a server and a drive on the remaining server). Because of this added data resilience, we recommend using nested resiliency on production deployments of two-server clusters, if you're running Windows Server 2019. For more info, see Nested resiliency.




**With three servers**

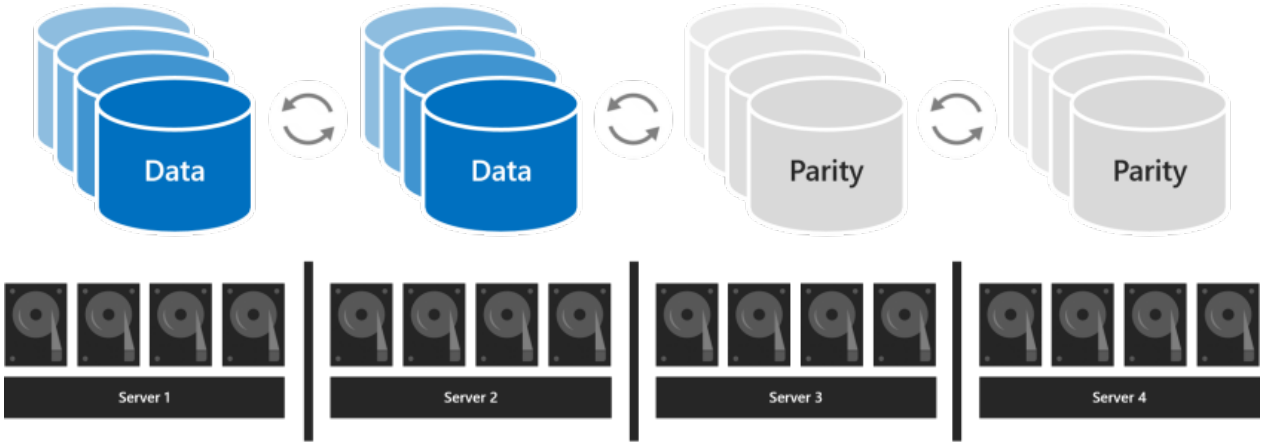
With three servers, you should use three-way mirroring for better fault tolerance and performance. Three-way mirroring keeps three copies of all data, one copy on the drives in each server. Its storage efficiency is 33.3% – to write 1 TB of data, you need at least 3 TB of physical storage capacity in the storage pool. Three-way mirroring can safely tolerate at least two hardware problems (drive or server) at a time. If 2 nodes become unavailable the storage pool will lose quorum, since 2/3 of the disks are not available, and the virtual disks will be unaccessible. However, a node can be down and one or more disks on another node can fail and the virtual disks will remain online. For example, if you're rebooting one server when suddenly another drive or server fails, all data remains safe and continuously accessible.




**With four or more servers**

With four or more servers, you can choose for each volume whether to use three-way mirroring, dual parity (often called "erasure coding"), or mix the two with mirror-accelerated parity.

Dual parity provides the same fault tolerance as three-way mirroring but with better storage efficiency. With four servers, its storage efficiency is 50.0%—to store 2 TB of data, you need 4 TB of physical storage capacity in the storage pool. This increases to 66.7% storage efficiency with seven servers, and continues up to 80.0% storage efficiency. The tradeoff is that parity encoding is more compute-intensive, which can limit its performance.




Which resiliency type to use depends on the needs of your workload. Here's a table that summarizes which workloads are a good fit for each resiliency type, as well as the performance and storage efficiency of each resiliency type.

| RESILIENCY TYPE | CAPACITY EFFICIENCY | SPEED | WORKLOADS |
|---|---|---|---|
| **Mirror** | Three-way mirror: 33%<br>Two-way-mirror: 50% | Highest performance | Virtualized workloads<br>Databases<br>Other high performance workloads |
| **Mirror-accelerated parity** | Depends on proportion of mirror and parity | Much slower than mirror, but up to twice as fast as dual-parity<br>Best for large sequential writes and reads | Archival and backup<br>Virtualized desktop infrastructure |

| RESILIENCY TYPE | CAPACITY EFFICIENCY | SPEED | WORKLOADS |
| --- | --- | --- | --- |
| Dual-parity | 4 servers: 50%<br>16 servers: up to 80% | Highest I/O latency & CPU usage on writes<br>Best for large sequential writes and reads | Archival and backup<br>Virtualized desktop infrastructure |

#### When performance matters most

Workloads that have strict latency requirements or that need lots of mixed random IOPS, such as SQL Server databases or performance-sensitive Hyper-V virtual machines, should run on volumes that use mirroring to maximize performance.

> **TIP**
> Mirroring is faster than any other resiliency type. We use mirroring for nearly all our performance examples.

#### When capacity matters most

Workloads that write infrequently, such as data warehouses or "cold" storage, should run on volumes that use dual parity to maximize storage efficiency. Certain other workloads, such as traditional file servers, virtual desktop infrastructure (VDI), or others that don't create lots of fast-drifting random IO traffic and/or don't require the best performance may also use dual parity, at your discretion. Parity inevitably increases CPU utilization and IO latency, particularly on writes, compared to mirroring.

#### When data is written in bulk

Workloads that write in large, sequential passes, such as archival or backup targets, have another option that is new in Windows Server 2016: one volume can mix mirroring and dual parity. Writes land first in the mirrored portion and are gradually moved into the parity portion later. This accelerates ingestion and reduces resource utilization when large writes arrive by allowing the compute-intensive parity encoding to happen over a longer time. When sizing the portions, consider that the quantity of writes that happen at once (such as one daily backup) should comfortably fit in the mirror portion. For example, if you ingest 100 GB once daily, consider using mirroring for 150 GB to 200 GB, and dual parity for the rest.

The resulting storage efficiency depends on the proportions you choose. See this demo for some examples.

> **TIP**
> If you observe an abrupt decrease in write performance partway through data ingestion, it may indicate that the mirror portion is not large enough or that mirror-accelerated parity isn't well suited for your use case. As an example, if write performance decreases from 400 MB/s to 40 MB/s, consider expanding the mirror portion or switching to three-way mirror.

### About deployments with NVMe, SSD, and HDD

In deployments with two types of drives, the faster drives provide caching while the slower drives provide capacity. This happens automatically – for more information, see Understanding the cache in Storage Spaces Direct. In such deployments, all volumes ultimately reside on the same type of drives – the capacity drives.

In deployments with all three types of drives, only the fastest drives (NVMe) provide caching, leaving two types of drives (SSD and HDD) to provide capacity. For each volume, you can choose whether it resides entirely on the SSD tier, entirely on the HDD tier, or whether it spans the two.

**IMPORTANT**

We recommend using the SSD tier to place your most performance-sensitive workloads on all-flash.

## Choosing the size of volumes

We recommend limiting the size of each volume to:

| WINDOWS SERVER 2016 | WINDOWS SERVER 2019 |
| --- | --- |
| Up to 32 TB | Up to 64 TB |

**TIP**

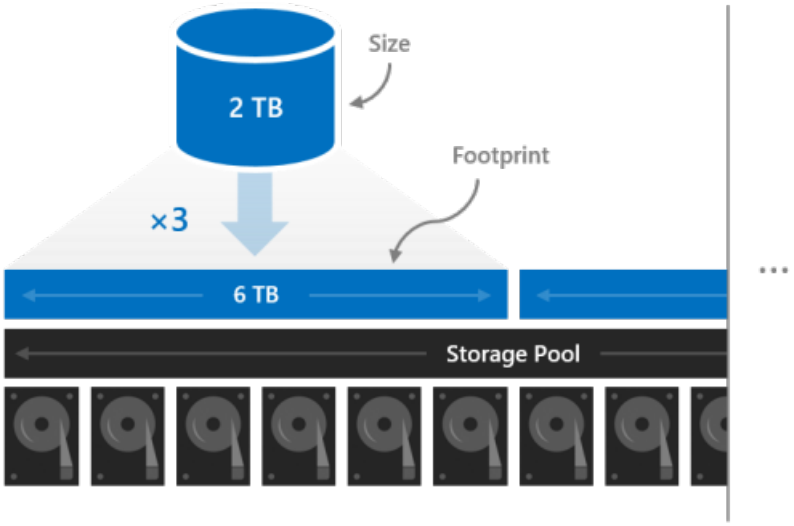
If you use a backup solution that relies on the Volume Shadow Copy service (VSS) and the Volsnap software provider—as is common with file server workloads—limiting the volume size to 10 TB will improve performance and reliability. Backup solutions that use the newer Hyper-V RCT API and/or ReFS block cloning and/or the native SQL backup APIs perform well up to 32 TB and beyond.

### Footprint

The size of a volume refers to its usable capacity, the amount of data it can store. This is provided by the **-Size** parameter of the **New-Volume** cmdlet and then appears in the **Size** property when you run the **Get-Volume** cmdlet.

Size is distinct from volume's *footprint*, the total physical storage capacity it occupies on the storage pool. The footprint depends on its resiliency type. For example, volumes that use three-way mirroring have a footprint three times their size.

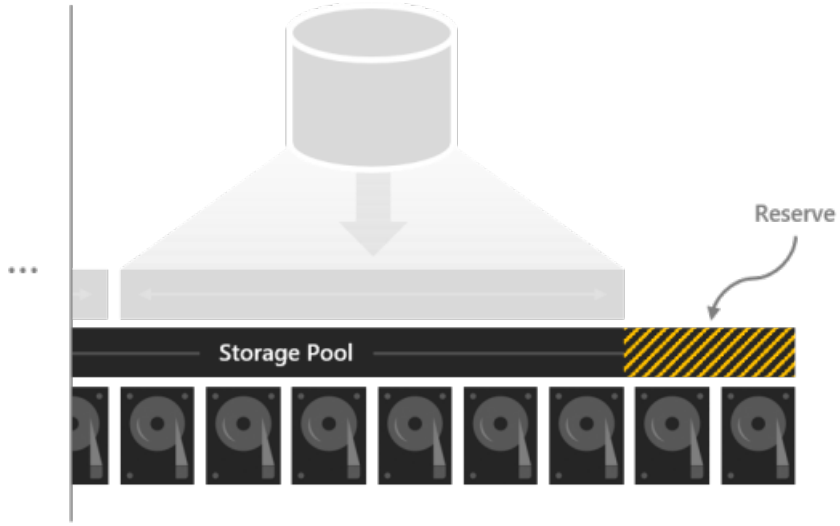
The footprints of your volumes need to fit in the storage pool.




### Reserve capacity

Leaving some capacity in the storage pool unallocated gives volumes space to repair "in-place" after drives fail, improving data safety and performance. If there is sufficient capacity, an immediate, in-place, parallel repair can restore volumes to full resiliency even before the failed drives are replaced. This happens automatically.

We recommend reserving the equivalent of one capacity drive per server, up to 4 drives. You may reserve more at your discretion, but this minimum recommendation guarantees an immediate, in-place, parallel repair can succeed after the failure of any drive.




For example, if you have 2 servers and you are using 1 TB capacity drives, set aside 2 x 1 = 2 TB of the pool as reserve. If you have 3 servers and 1 TB capacity drives, set aside 3 x 1 = 3 TB as reserve. If you have 4 or more servers and 1 TB capacity drives, set aside 4 x 1 = 4 TB as reserve.

> **NOTE**
> In clusters with drives of all three types (NVMe + SSD + HDD), we recommend reserving the equivalent of one SSD plus one HDD per server, up to 4 drives of each.

## Example: Capacity planning

Consider one four-server cluster. Each server has some cache drives plus sixteen 2 TB drives for capacity.

```
4 servers x 16 drives each x 2 TB each = 128 TB
```

From this 128 TB in the storage pool, we set aside four drives, or 8 TB, so that in-place repairs can happen without any rush to replace drives after they fail. This leaves 120 TB of physical storage capacity in the pool with which we can create volumes.

```
128 TB – (4 x 2 TB) = 120 TB
```

Suppose we need our deployment to host some highly active Hyper-V virtual machines, but we also have lots of cold storage – old files and backups we need to retain. Because we have four servers, let's create four volumes.

Let's put the virtual machines on the first two volumes, *Volume1* and *Volume2*. We choose ReFS as the filesystem (for the faster creation and checkpoints) and three-way mirroring for resiliency to maximize performance. Let's put the cold storage on the other two volumes, *Volume 3* and *Volume 4*. We choose NTFS as the filesystem (for Data Deduplication) and dual parity for resiliency to maximize capacity.

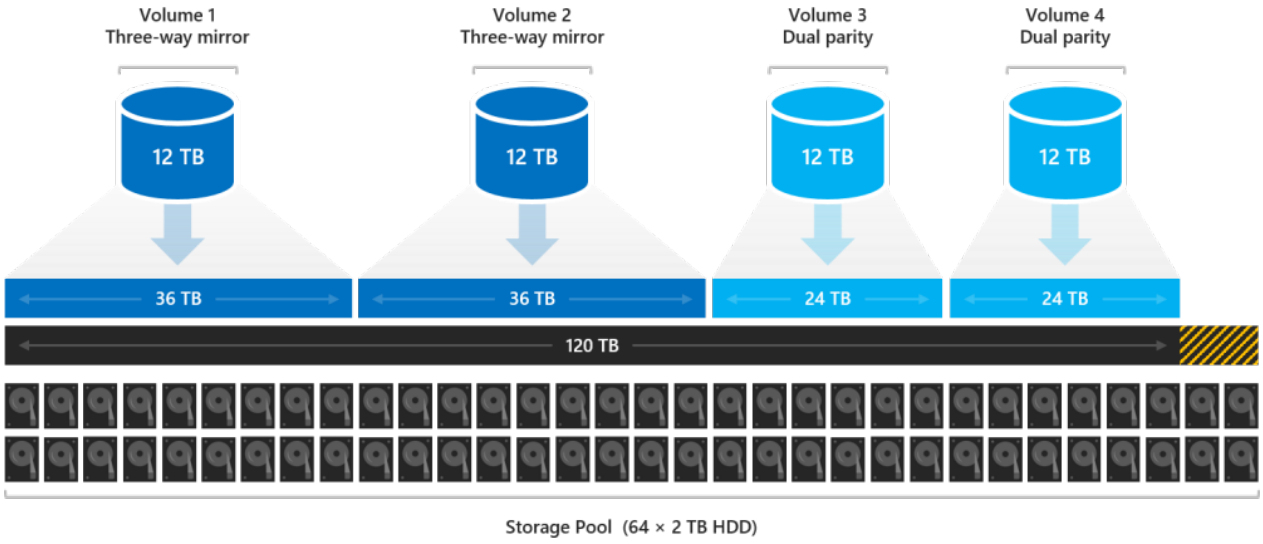
We aren't required to make all volumes the same size, but for simplicity, let's – for example, we can make them all 12 TB.

*Volume1* and *Volume2* will each occupy 12 TB x 33.3% efficiency = 36 TB of physical storage capacity.

*Volume3* and *Volume4* will each occupy 12 TB x 50.0% efficiency = 24 TB of physical storage capacity.

```
36 TB + 36 TB + 24 TB + 24 TB = 120 TB
```

The four volumes fit exactly on the physical storage capacity available in our pool. Perfect!




> **TIP**
> You don't need to create all the volumes right away. You can always extend volumes or create new volumes later.

For simplicity, this example uses decimal (base-10) units throughout, meaning 1 TB = 1,000,000,000,000 bytes. However, storage quantities in Windows appear in binary (base-2) units. For example, each 2 TB drive would appear as 1.82 TiB in Windows. Likewise, the 128 TB storage pool would appear as 116.41 TiB. This is expected.

## Usage

See Creating volumes in Storage Spaces Direct.

**Additional References**

- Storage Spaces Direct overview
- Choosing drives for Storage Spaces Direct
- Fault tolerance and storage efficiency

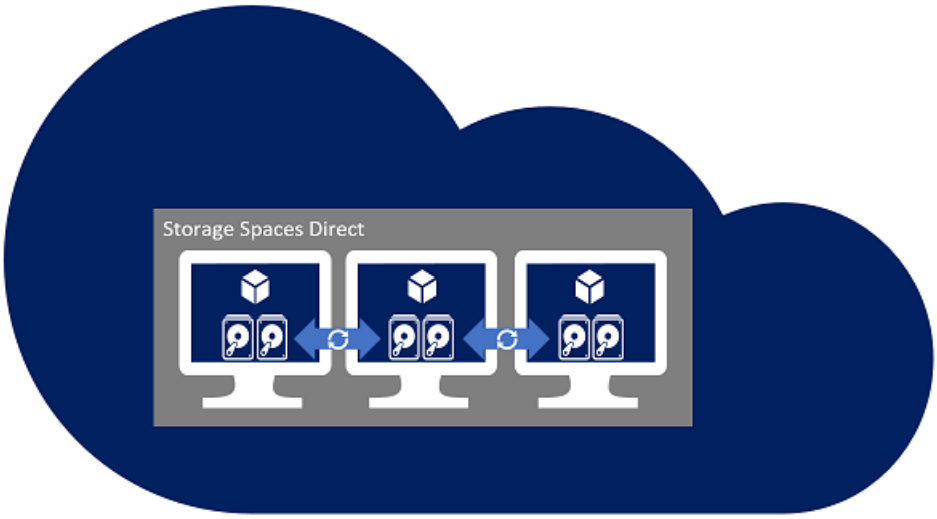
# Using Storage Spaces Direct in guest virtual machine clusters

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

You can deploy Storage Spaces Direct (sometimes called S2D) on a cluster of physical servers or on virtual machine guest clusters as discussed in this topic. This type of deployment delivers virtual shared storage across a set of VMs on top of a private or public cloud so that application high availability solutions can be used to increase the availability of applications.

To instead use Azure Shared Disks for guest virtual machines, see Azure Shared Disks.




## Deploying in Azure Iaas VM guest clusters

Azure templates have been published decrease the complexity, configure best practices, and speed of your Storage Spaces Direct deployments in an Azure Iaas VM. This is the recommended solution for deploying in Azure.

https://channel9.msdn.com/Series/Microsoft-Hybrid-Cloud-Best-Practices-for-IT-Pros/Step-by-Step-Deploy-Windows-Server-2016-Storage-Spaces-Direct-S2D-Cluster-in-Microsoft-Azure/player

## Requirements for guest clusters

The following considerations apply when deploying Storage Spaces Direct in a virtualized environment.

> **TIP**
> Azure templates will automatically configure the below considerations for you and are the recommended solution when deploying in Azure IaaS VMs.

- Minimum of 2 nodes and maximum of 3 nodes
- 2-node deployments must configure a witness (Cloud Witness or File Share Witness)
- 3-node deployments can tolerate 1 node down and the loss of 1 or more disks on another node. If 2 nodes are shutdown then the virtual disks we be offline until one of the nodes returns.

- Configure the virtual machines to be deployed across fault domains
  - Azure – Configure Availability Set
  - Hyper-V – Configure AntiAffinityClassNames on the VMs to separate the VMs across nodes
  - VMware – Configure VM-VM Anti-Affinity rule by Creating a DRS Rule of type 'Separate Virtual Machines" to separate the VMs across ESX hosts. Disks presented for use with Storage Spaces Direct should use the Paravirtual SCSI (PVSCSI) adapter. For PVSCSI support with Windows Server, consult https://kb.vmware.com/s/article/1010398.
- Leverage low latency / high performance storage - Azure Premium Storage managed disks are required
- Deploy a flat storage design with no caching devices configured
- Minimum of 2 virtual data disks presented to each VM (VHD / VHDX / VMDK)

  This number is different than bare-metal deployments because the virtual disks can be implemented as files that aren't susceptible to physical failures.
- Disable the automatic drive replacement capabilities in the Health Service by running the following PowerShell cmdlet:

  ```
  Get-storagesubsystem clus* | set-storagehealthsetting -name
  "System.Storage.PhysicalDisk.AutoReplace.Enabled" -value "False"
  ```
- To give greater resiliency to possible VHD / VHDX / VMDK storage latency in guest clusters, increase the Storage Spaces I/O timeout value:

  `HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\spaceport\\Parameters\\HwTimeout`

  `dword: 00007530`

  The decimal equivalent of Hexadecimal 7530 is 30000, which is 30 seconds. Note that the default value is 1770 Hexadecimal, or 6000 Decimal, which is 6 seconds.

## Not supported

- Host level virtual disk snapshot/restore

  Instead use traditional guest level backup solutions to backup and restore the data on the Storage Spaces Direct volumes.
- Host level virtual disk size change

  The virtual disks exposed through the virtual machine must retain the same size and characteristics. Adding more capacity to the storage pool can be accomplished by adding more virtual disks to each of the virtual machines and adding them to the pool. It's highly recommended to use virtual disks of the same size and characteristics as the current virtual disks.

## Additional References

- Additional Azure Iaas VM templates for deploying Storage Spaces Direct, videos, and step-by-step guides.
- Additional Storage Spaces Direct Overview

# Disaster recovery with Storage Spaces Direct

11/2/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic provides scenarios on how hyper-converged infrastructure (HCI) can be configured for disaster recovery.

Numerous companies are running hyper-converged solutions and planning for a disaster gives the ability to remain in or get back to production quickly if a disaster were to occur. There are several ways to configure HCI for disaster recovery and this document explains the options that are available to you today.

When discussions of restoring availability if disaster occurs revolve around what's known as Recovery Time Objective (RTO). This is the duration of time targeted where services must be restored to avoid unacceptable consequences to the business. In some cases, this process can occur automatically with production restored nearly immediately. In other cases, manual administrator intervention must occur to restore services.

The disaster recovery options with a hyper-converged today are:

1. Multiple clusters utilizing Storage Replica
2. Hyper-V Replica between clusters
3. Backup and Restore

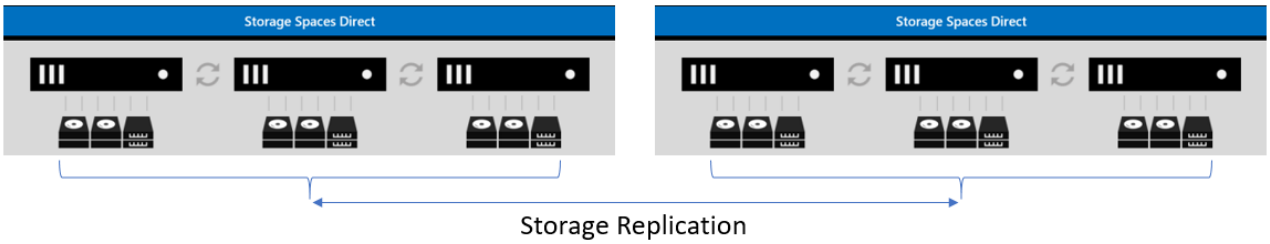
## Multiple clusters utilizing Storage Replica

Storage Replica enables the replication of volumes and supports both synchronous and asynchronous replication. When choosing between using either synchronous or asynchronous replication, you should consider your Recovery Point Objective (RPO). Recovery Point Objective is the amount of possible data loss you are willing to incur before it is considered major loss. If you go with synchronous replication, it will sequentially write to both ends at the same time. If you go with asynchronous, writes will replicate very fast but could still be lost. You should consider the application or file usage to see which best works for you.

Storage Replica is a block level copy mechanism versus file level; meaning, it does not matter what types of data being replicated. This makes it a popular option for hyper-converged infrastructure. Storage Replica also can utilize different types of drives between the replication partners, so having all of one type storage on one HCI and another type storage on the other is perfectly fine.

One important capability of Storage Replica is that it can be run in Azure as well as on-premises. You can set up on-premises to on-premises, Azure to Azure, or even on-premises to Azure (or vice versa).

In this scenario, there are two separate independent clusters. For configuring Storage Replica between HCI, you can follow the steps in Cluster-to-cluster storage replication.




The following considerations apply when deploying Storage Replica.

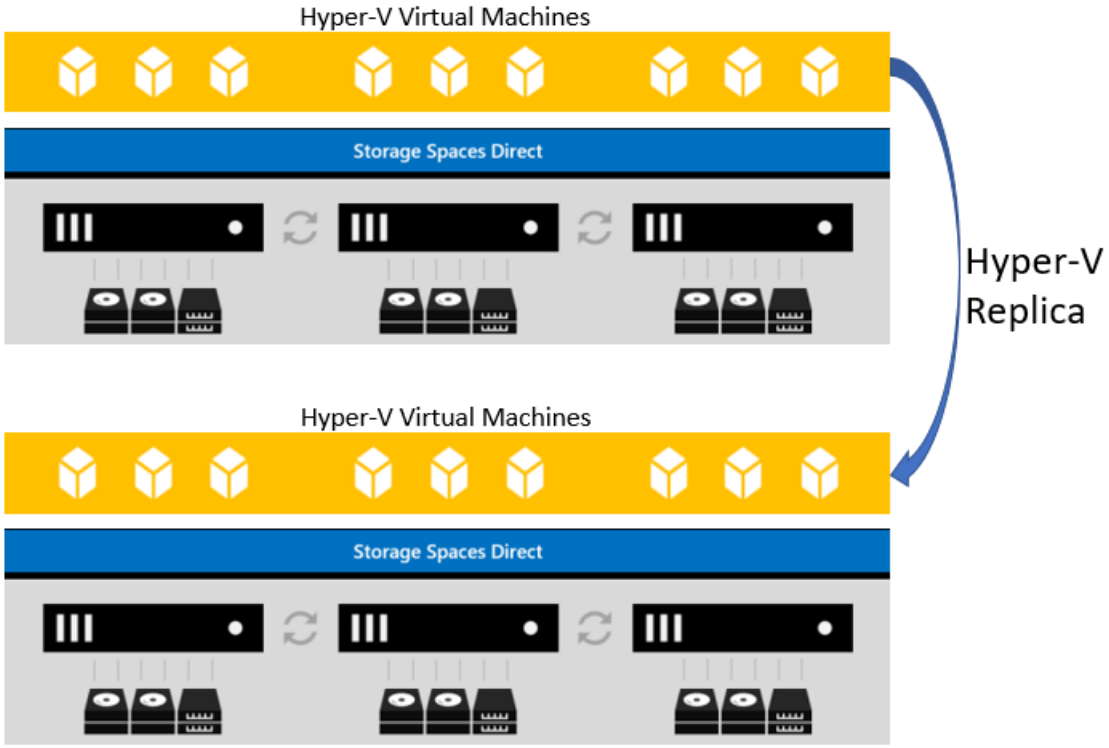
1. Configuring replication is done outside of Failover Clustering.

2. Choosing the method of replication will be dependent upon your network latency and RPO requirements. Synchronous replicates the data on low-latency networks with crash consistency to ensure no data loss at a time of failure. Asynchronous replicates the data over networks with higher latencies, but each site may not have identical copies at a time of failure.
3. In the case of a disaster, failovers between the clusters are not automatic and need to be orchestrated manually through the Storage Replica PowerShell cmdlets. In the diagram above, ClusterA is the primary and ClusterB is the secondary. If ClusterA goes down, you would need to manually set ClusterB as Primary before you can bring the resources up. Once ClusterA is back up, you would need to make it Secondary. Once all data has been synced up, make the change and swap the roles back to the way they were originally set.
4. Since Storage Replica is only replicating the data, a new virtual machine or Scale Out File Server (SOFS) utilizing this data would need to be created inside Failover Cluster Manager on the replica partner.

Storage Replica can be used if you have virtual machines or an SOFS running on your cluster. Bringing resources online in the replica HCI can be manual or automated through the use of PowerShell scripting.

## Hyper-V Replica

Hyper-V Replica provides virtual machine level replication for disaster recovery on hyper-converged infrastructures. What Hyper-V Replica can do is to take a virtual machine and replicate it to a secondary site or Azure (replica). Then from the secondary site, Hyper-V Replica can replicate the virtual machine to a third (extended replica).




With Hyper-V Replica, the replication is taken care of by Hyper-V. When you first enable a virtual machine for replication, there are three choices for how you wish the initial copy to be sent to the corresponding replica cluster(s).

1. Send the initial copy over the network
2. Send the initial copy to external media so that it can be copied onto your server manually
3. Use an existing virtual machine already created on the replica hosts

The other option is for when you wish this initial replication should take place.

1. Start the replication immediately
2. Schedule a time for when the initial replication takes place.

Other considerations you will need are:

- What VHD/VHDX's you wish to replicate. You can choose to replicate all of them or only one of them.
- Number of recovery points you wish to save. If you wish to have several options about what point in time you wish to restore, then you would want to specify how many you want. If you only want one restore point, you can choose that as well.
- How often you wish to have the Volume Shadow Copy Service (VSS) replicate an incremental shadow copy.
- How often changes get replicated (30 seconds, 5 minutes, 15 minutes).

When HCI participate in Hyper-V Replica, you must have the Hyper-V Replica Broker resource created in each cluster. This resource does several things:

1. Gives you a single namespace for each cluster for Hyper-V Replica to connect to.
2. Determines which node within that cluster the replica (or extended replica) will reside on when it first receives the copy.
3. Keeps track of which node owns the replica (or extended replica) in case the virtual machine moves to another node. It needs to track this so that when replication takes place, it can send the information to the proper node.

## Backup and restore

One traditional disaster recovery option that isn't talked about very much but is just as important is the failure of the entire cluster or a node in the cluster. Either option with this scenario makes use of Windows NT Backup.

It is always a recommendation to have periodic backups of the hyper-converged infrastructure. While the Cluster Service is running, if you take a System State Backup, the cluster registry database would be a part of that backup. Restoring the cluster or the database has two different methods (Non-Authoritative and Authoritative).

**Non-authoritative**

A Non-Authoritative restore can be accomplished using Windows NT Backup and equates to a full restore of just the cluster node itself. If you only need to restore a cluster node (and the cluster registry database) and all current cluster information good, you would restore using non-authoritative. Non-Authoritative restores can be done through the Windows NT Backup interface or the command line WBADMIN.EXE.

Once you restore the node, let it join the cluster. What will happen is that it will go out to the existing running cluster and update all of its information with what is currently there.

**Authoritative**

An Authoritative restore of the cluster configuration, on the other hand, takes the cluster configuration back in time. This type of restore should only be accomplished when the cluster information itself has been lost and needs restored. For example, someone accidentally deleted a File Server that contained over 1000 shares and you need them back. Completing an Authoritative restore of the cluster requires that Backup be run from the command line.

When an Authoritative restore is initiated on a cluster node, the cluster service is stopped on all other nodes in the cluster view and the cluster configuration is frozen. This is why it is critical that the cluster service on the node on which the restore was executed be started first so the cluster is formed using the new copy of the cluster configuration.

To run through an authoritative restore, the following steps can be accomplished.

1. Run WBADMIN.EXE from an administrative command prompt to get the latest version of backups that you want to install and ensure that System State is one of the components you can restore.

   ```
   wbadmin get versions
   ```

2. Determine if the version backup you have has the cluster registry information in it as a component. There

are a couple items you will need from this command, the version and the application/component for use in Step 3. For the version, for example, say the backup was done January 3, 2018 at 2:04am and this is the one you need restored.

```
wbadmin get items -backuptarget:\\backupserver\location
```

3. Start the authoritative restore to recover only the cluster registry version you need.

```
wbadmin start recovery -version:01/03/2018-02:04 -itemtype:app -items:cluster
```

Once the restore has taken place, this node must be the one to start the Cluster Service first and form the cluster. All other nodes would then need to be started and join the cluster.

## Summary

To sum this all up, hyper-converged disaster recovery is something that should be planned out carefully. There are several scenarios that can best suits your needs and should be thoroughly tested. One item to note is that if you are familiar with Failover Clusters in the past, stretch clusters have been a very popular option over the years. There was a bit of a design change with the hyper-converged solution and it is based on resiliency. If you lose two nodes in a hyper-converged cluster, the entire cluster will go down. With this being the case, in a hyper-converged environment, the stretch scenario is not supported.

# Deploy Storage Spaces Direct

12/16/2020 • 17 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic provides step-by-step instructions to deploy Storage Spaces Direct on Windows Server. To deploy Storage Spaces Direct as part of Azure Stack HCI, see What is the deployment process for Azure Stack HCI?

> **TIP**
> Looking to acquire hyperconverged infrastructure? Microsoft recommends purchasing a validated hardware/software Azure Stack HCI solution from our partners. These solutions are designed, assembled, and validated against our reference architecture to ensure compatibility and reliability, so you get up and running quickly. To peruse a catalog of hardware/software solutions that work with Azure Stack HCI, see the Azure Stack HCI Catalog.

> **TIP**
> You can use Hyper-V virtual machines, including in Microsoft Azure, to evaluate Storage Spaces Direct without hardware. You may also want to review the handy Windows Server rapid lab deployment scripts, which we use for training purposes.

## Before you start

Review the Storage Spaces Direct hardware requirements and skim this document to familiarize yourself with the overall approach and important notes associated with some steps.

Gather the following information:

- **Deployment option.** Storage Spaces Direct supports two deployment options: hyper-converged and converged, also known as disaggregated. Familiarize yourself with the advantages of each to decide which is right for you. Steps 1-3 below apply to both deployment options. Step 4 is only needed for converged deployment.
- **Server names.** Get familiar with your organization's naming policies for computers, files, paths, and other resources. You'll need to provision several servers, each with unique names.
- **Domain name.** Get familiar with your organization's policies for domain naming and domain joining. You'll be joining the servers to your domain, and you'll need to specify the domain name.
- **RDMA networking.** There are two types of RDMA protocols: iWarp and RoCE. Note which one your network adapters use, and if RoCE, also note the version (v1 or v2). For RoCE, also note the model of your top-of-rack switch.
- **VLAN ID.** Note the VLAN ID to be used for management OS network adapters on the servers, if any. You should be able to obtain this from your network administrator.

## Step 1: Deploy Windows Server

### Step 1.1: Install the operating system

The first step is to install Windows Server on every server that will be in the cluster. Storage Spaces Direct requires Windows Server Datacenter Edition. You can use the Server Core installation option, or Server with Desktop

Experience.

When you install Windows Server using the Setup wizard, you can choose between *Windows Server* (referring to Server Core) and *Windows Server (Server with Desktop Experience)*, which is the equivalent of the *Full* installation option available in Windows Server 2012 R2. If you don't choose, you'll get the Server Core installation option. For more information, see Install Server Core.

**Step 1.2: Connect to the servers**

This guide focuses the Server Core installation option and deploying/managing remotely from a separate management system, which must have:

- A version of Windows Server or Windows 10 at least as new as the servers it's managing, and with the latest updates
- Network connectivity to the servers it's managing
- Joined to the same domain or a fully trusted domain
- Remote Server Administration Tools (RSAT) and PowerShell modules for Hyper-V and Failover Clustering. RSAT tools and PowerShell modules are available on Windows Server and can be installed without installing other features. You can also install the Remote Server Administration Tools on a Windows 10 management PC.

On the Management system install the Failover Cluster and Hyper-V management tools. This can be done through Server Manager using the **Add Roles and Features** wizard. On the **Features** page, select **Remote Server Administration Tools**, and then select the tools to install.

Enter the PS session and use either the server name or the IP address of the node you want to connect to. You'll be prompted for a password after you execute this command, enter the administrator password you specified when setting up Windows.

```
Enter-PSSession -ComputerName <myComputerName> -Credential LocalHost\Administrator
```

Here's an example of doing the same thing in a way that is more useful in scripts, in case you need to do this more than once:

```
$myServer1 = "myServer-1"
$user = "$myServer1\Administrator"

Enter-PSSession -ComputerName $myServer1 -Credential $user
```

> **TIP**
> If you're deploying remotely from a management system, you might get an error like *WinRM cannot process the request.* To fix this, use Windows PowerShell to add each server to the Trusted Hosts list on your management computer:
>
> `Set-Item WSMAN:\Localhost\Client\TrustedHosts -Value Server01 -Force`
>
> Note: the trusted hosts list supports wildcards, like `Server*`.
>
> To view your Trusted Hosts list, type `Get-Item WSMAN:\Localhost\Client\TrustedHosts`.
>
> To empty the list, type `Clear-Item WSMAN:\Localhost\Client\TrustedHost`.

**Step 1.3: Join the domain and add domain accounts**

So far you've configured the individual servers with the local administrator account, `<ComputerName>\Administrator`.

To manage Storage Spaces Direct, you'll need to join the servers to a domain and use an Active Directory Domain

Services domain account that is in the Administrators group on every server.

From the management system, open a PowerShell console with Administrator privileges. Use `Enter-PSSession` to connect to each server and run the following cmdlet, substituting your own computer name, domain name, and domain credentials:

```
Add-Computer -NewName "Server01" -DomainName "contoso.com" -Credential "CONTOSO\User" -Restart -Force
```

If your storage administrator account isn't a member of the Domain Admins group, add your storage administrator account to the local Administrators group on each node - or better yet, add the group you use for storage administrators. You can use the following command (or write a Windows PowerShell function to do so - see Use PowerShell to Add Domain Users to a Local Group for more info):

```
Net localgroup Administrators <Domain\Account> /add
```

**Step 1.4: Install roles and features**

The next step is to install server roles on every server. You can do this by using Windows Admin Center, Server Manager), or PowerShell. Here are the roles to install:

- Failover Clustering
- Hyper-V
- File Server (if you want to host any file shares, such as for a converged deployment)
- Data-Center-Bridging (if you're using RoCEv2 instead of iWARP network adapters)
- RSAT-Clustering-PowerShell
- Hyper-V-PowerShell

To install via PowerShell, use the Install-WindowsFeature cmdlet. You can use it on a single server like this:

```
Install-WindowsFeature -Name "Hyper-V", "Failover-Clustering", "Data-Center-Bridging", "RSAT-Clustering-
PowerShell", "Hyper-V-PowerShell", "FS-FileServer"
```

To run the command on all servers in the cluster as the same time, use this little bit of script, modifying the list of variables at the beginning of the script to fit your environment.

```
# Fill in these variables with your values
$ServerList = "Server01", "Server02", "Server03", "Server04"
$FeatureList = "Hyper-V", "Failover-Clustering", "Data-Center-Bridging", "RSAT-Clustering-PowerShell",
"Hyper-V-PowerShell", "FS-FileServer"

# This part runs the Install-WindowsFeature cmdlet on all servers in $ServerList, passing the list of
features into the scriptblock with the "Using" scope modifier so you don't have to hard-code them here.
Invoke-Command ($ServerList) {
    Install-WindowsFeature -Name $Using:Featurelist
}
```

## Step 2: Configure the network

If you're deploying Storage Spaces Direct inside virtual machines, skip this section.

Storage Spaces Direct requires high-bandwidth, low-latency networking between servers in the cluster. At least 10 GbE networking is required and remote direct memory access (RDMA) is recommended. You can use either iWARP or RoCE as long as it has the Windows Server logo that matches your operating system version, but iWARP is usually easier to set up.

> **IMPORTANT**
>
> Depending on your networking equipment, and especially with RoCE v2, some configuration of the top-of-rack switch may be required. Correct switch configuration is important to ensure reliability and performance of Storage Spaces Direct.

Windows Server 2016 introduced switch-embedded teaming (SET) within the Hyper-V virtual switch. This allows the same physical NIC ports to be used for all network traffic while using RDMA, reducing the number of physical NIC ports required. Switch-embedded teaming is recommended for Storage Spaces Direct.

Switched or switchless node interconnects

- Switched: Network switches must be properly configured to handle the bandwidth and networking type. If using RDMA that implements the RoCE protocol, network device and switch configuration is even more important.
- Switchless: Nodes can be interconnected using direct connections, avoiding using a switch. It is required that every node have a direct connection with every other node of the cluster.

For instructions to set up networking for Storage Spaces Direct, see the Windows Server 2016 and 2019 RDMA Deployment Guide.

## Step 3: Configure Storage Spaces Direct

The following steps are done on a management system that is the same version as the servers being configured. The following steps should NOT be run remotely using a PowerShell session, but instead run in a local PowerShell session on the management system, with administrative permissions.

### Step 3.1: Clean drives

Before you enable Storage Spaces Direct, ensure your drives are empty: no old partitions or other data. Run the following script, substituting your computer names, to remove all any old partitions or other data.

> **WARNING**
>
> This script will permanently remove any data on any drives other than the operating system boot drive!

```
# Fill in these variables with your values
$ServerList = "Server01", "Server02", "Server03", "Server04"

Invoke-Command ($ServerList) {
    Update-StorageProviderCache
    Get-StoragePool | ? IsPrimordial -eq $false | Set-StoragePool -IsReadOnly:$false -ErrorAction
SilentlyContinue
    Get-StoragePool | ? IsPrimordial -eq $false | Get-VirtualDisk | Remove-VirtualDisk -Confirm:$false -
ErrorAction SilentlyContinue
    Get-StoragePool | ? IsPrimordial -eq $false | Remove-StoragePool -Confirm:$false -ErrorAction
SilentlyContinue
    Get-PhysicalDisk | Reset-PhysicalDisk -ErrorAction SilentlyContinue
    Get-Disk | ? Number -ne $null | ? IsBoot -ne $true | ? IsSystem -ne $true | ? PartitionStyle -ne RAW | %
{
        $_ | Set-Disk -isoffline:$false
        $_ | Set-Disk -isreadonly:$false
        $_ | Clear-Disk -RemoveData -RemoveOEM -Confirm:$false
        $_ | Set-Disk -isreadonly:$true
        $_ | Set-Disk -isoffline:$true
    }
    Get-Disk | Where Number -Ne $Null | Where IsBoot -Ne $True | Where IsSystem -Ne $True | Where
PartitionStyle -Eq RAW | Group -NoElement -Property FriendlyName
} | Sort -Property PsComputerName, Count
```

The output will look like this, where **Count** is the number of drives of each model in each server:

```
Count Name                         PSComputerName
----- ----                         --------------
4     ATA SSDSC2BA800G4n           Server01
10    ATA ST4000NM0033             Server01
4     ATA SSDSC2BA800G4n           Server02
10    ATA ST4000NM0033             Server02
4     ATA SSDSC2BA800G4n           Server03
10    ATA ST4000NM0033             Server03
4     ATA SSDSC2BA800G4n           Server04
10    ATA ST4000NM0033             Server04
```

### Step 3.2: Validate the cluster

In this step, you'll run the cluster validation tool to ensure that the server nodes are configured correctly to create a cluster using Storage Spaces Direct. When cluster validation (`Test-Cluster`) is run before the cluster is created, it runs the tests that verify that the configuration appears suitable to successfully function as a failover cluster. The example directly below uses the `-Include` parameter, and then the specific categories of tests are specified. This ensures that the Storage Spaces Direct specific tests are included in the validation.

Use the following PowerShell command to validate a set of servers for use as a Storage Spaces Direct cluster.

```
Test-Cluster –Node <MachineName1, MachineName2, MachineName3, MachineName4> –Include "Storage Spaces Direct",
"Inventory", "Network", "System Configuration"
```

### Step 3.3: Create the cluster

In this step, you'll create a cluster with the nodes that you have validated for cluster creation in the preceding step using the following PowerShell cmdlet.

When creating the cluster, you'll get a warning that states - "There were issues while creating the clustered role that may prevent it from starting. For more information, view the report file below." You can safely ignore this warning. It's due to no disks being available for the cluster quorum. Its recommended that a file share witness or cloud witness is configured after creating the cluster.

> **NOTE**
>
> If the servers are using static IP addresses, modify the following command to reflect the static IP address by adding the following parameter and specifying the IP address:–StaticAddress <X.X.X.X>. In the following command the ClusterName placeholder should be replaced with a netbios name that is unique and 15 characters or less.
>
> ```
> New-Cluster –Name <ClusterName> –Node <MachineName1,MachineName2,MachineName3,MachineName4> –NoStorage
> ```

After the cluster is created, it can take time for DNS entry for the cluster name to be replicated. The time is dependent on the environment and DNS replication configuration. If resolving the cluster isn't successful, in most cases you can be successful with using the machine name of a node that is an active member of the cluster may be used instead of the cluster name.

### Step 3.4: Configure a cluster witness

We recommend that you configure a witness for the cluster, so clusters with three or more servers can withstand two servers failing or being offline. A two-server deployment requires a cluster witness, otherwise either server going offline causes the other to become unavailable as well. With these systems, you can use a file share as a witness, or use cloud witness.

For more info, see the following topics:

- Configure and manage quorum
- Deploy a Cloud Witness for a Failover Cluster

**Step 3.5: Enable Storage Spaces Direct**

After creating the cluster, use the `Enable-ClusterStorageSpacesDirect` PowerShell cmdlet, which will put the storage system into the Storage Spaces Direct mode and do the following automatically:

- **Create a pool:** Creates a single large pool that has a name like "S2D on Cluster1".
- **Configures the Storage Spaces Direct caches:** If there is more than one media (drive) type available for Storage Spaces Direct use, it enables the fastest as cache devices (read and write in most cases)
- **Tiers:** Creates two tiers as default tiers. One is called "Capacity" and the other called "Performance". The cmdlet analyzes the devices and configures each tier with the mix of device types and resiliency.

From the management system, in a PowerShell command windows opened with Administrator privileges, initiate the following command. The cluster name is the name of the cluster that you created in the previous steps. If this command is run locally on one of the nodes, the -CimSession parameter is not necessary.

```
Enable-ClusterStorageSpacesDirect –CimSession <ClusterName>
```

To enable Storage Spaces Direct using the above command, you can also use the node name instead of the cluster name. Using the node name may be more reliable due to DNS replication delays that may occur with the newly created cluster name.

When this command is finished, which may take several minutes, the system will be ready for volumes to be created.

**Step 3.6: Create volumes**

We recommend using the `New-Volume` cmdlet as it provides the fastest and most straightforward experience. This single cmdlet automatically creates the virtual disk, partitions and formats it, creates the volume with matching name, and adds it to cluster shared volumes – all in one easy step.

For more information, check out Creating volumes in Storage Spaces Direct.

**Step 3.7: Optionally enable the CSV cache**

You can optionally enable the cluster shared volume (CSV) cache to use system memory (RAM) as a write-through block-level cache of read operations that aren't already cached by the Windows cache manager. This can improve performance for applications such as Hyper-V. The CSV cache can boost the performance of read requests and is also useful for Scale-Out File Server scenarios.

Enabling the CSV cache reduces the amount of memory available to run VMs on a hyper-converged cluster, so you'll have to balance storage performance with memory available to VHDs.

To set the size of the CSV cache, open a PowerShell session on the management system with an account that has administrator permissions on the storage cluster, and then use this script, changing the `$ClusterName` and `$CSVCacheSize` variables as appropriate (this example sets a 2 GB CSV cache per server):

```
$ClusterName = "StorageSpacesDirect1"
$CSVCacheSize = 2048 #Size in MB

Write-Output "Setting the CSV cache..."
(Get-Cluster $ClusterName).BlockCacheSize = $CSVCacheSize

$CSVCurrentCacheSize = (Get-Cluster $ClusterName).BlockCacheSize
Write-Output "$ClusterName CSV cache size: $CSVCurrentCacheSize MB"
```

For more info, see Using the CSV in-memory read cache.

### Step 3.8: Deploy virtual machines for hyper-converged deployments

If you're deploying a hyper-converged cluster, the last step is to provision virtual machines on the Storage Spaces Direct cluster.

The virtual machine's files should be stored on the systems CSV namespace (example: c:\ClusterStorage\Volume1) just like clustered VMs on failover clusters.

You can use in-box tools or other tools to manage the storage and virtual machines, such as System Center Virtual Machine Manager.

## Step 4: Deploy Scale-Out File Server for converged solutions

If you're deploying a converged solution, the next step is to create a Scale-Out File Server instance and setup some file shares. If you're deploying a hyper-converged cluster - you're finished and don't need this section.

### Step 4.1: Create the Scale-Out File Server role

The next step in setting up the cluster services for your file server is creating the clustered file server role, which is when you create the Scale-Out File Server instance on which your continuously available file shares are hosted.

**To create a Scale-Out File Server role by using Server Manager**

1. In Failover Cluster Manager, select the cluster, go to **Roles**, and then click **Configure Role...**.
   The High Availability Wizard appears.
2. On the **Select Role** page, click **File Server**.
3. On the **File Server Type** page, click **Scale-Out File Server for application data**.
4. On the **Client Access Point** page, type a name for the Scale-Out File Server.
5. Verify that the role was successfully set up by going to **Roles** and confirming that the **Status** column shows **Running** next to the clustered file server role you created, as shown in Figure 1.

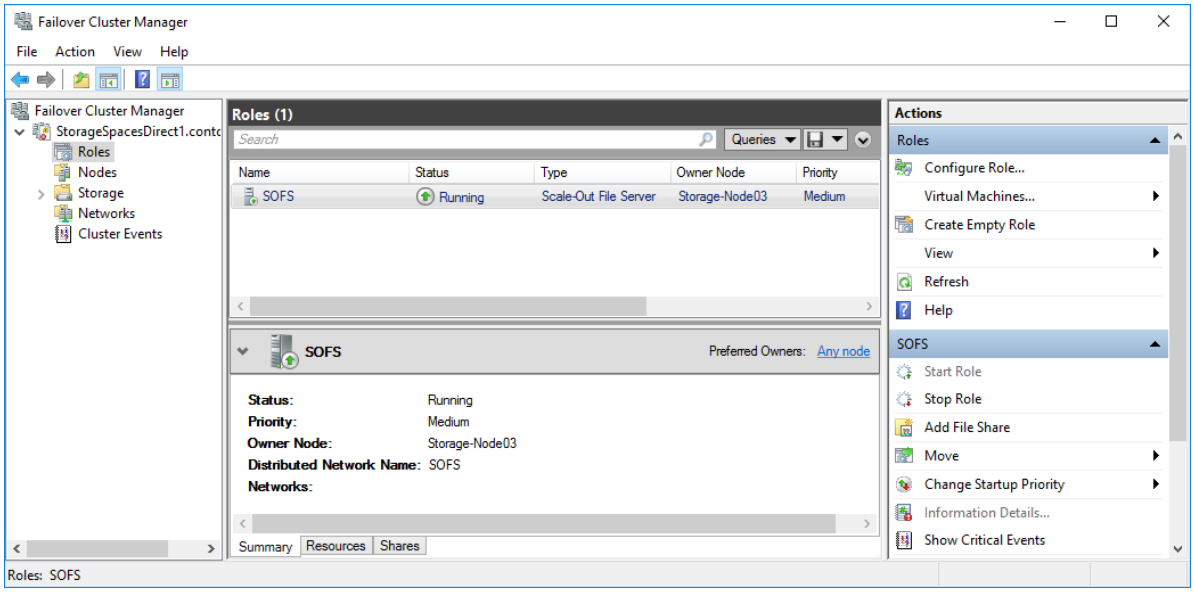



**Figure 1** Failover Cluster Manager showing the Scale-Out File Server with the Running status

> **NOTE**
>
> After creating the clustered role, there might be some network propagation delays that could prevent you from creating file shares on it for a few minutes, or potentially longer.

#### To create a Scale-Out File Server role by using Windows PowerShell

In a Windows PowerShell session that's connected to the file server cluster, enter the following commands to create the Scale-Out File Server role, changing *FSCLUSTER* to match the name of your cluster, and *SOFS* to match the name you want to give the Scale-Out File Server role:

```
Add-ClusterScaleOutFileServerRole -Name SOFS -Cluster FSCLUSTER
```

> **NOTE**
>
> After creating the clustered role, there might be some network propagation delays that could prevent you from creating file shares on it for a few minutes, or potentially longer. If the SOFS role fails immediately and won't start, it might be because the cluster's computer object doesn't have permission to create a computer account for the SOFS role. For help with that, see this blog post: Scale-Out File Server Role Fails To Start With Event IDs 1205, 1069, and 1194.

### Step 4.2: Create file shares

After you've created your virtual disks and added them to CSVs, it's time to create file shares on them - one file share per CSV per virtual disk. System Center Virtual Machine Manager (VMM) is probably the handiest way to do this because it handles permissions for you, but if you don't have it in your environment, you can use Windows PowerShell to partially automate the deployment.

Use the scripts included in the SMB Share Configuration for Hyper-V Workloads script, which partially automates the process of creating groups and shares. It's written for Hyper-V workloads, so if you're deploying other workloads, you might have to modify the settings or perform additional steps after you create the shares. For example, if you're using Microsoft SQL Server, the SQL Server service account must be granted full control on the share and the file system.

> **NOTE**
>
> You'll have to update the group membership when you add cluster nodes unless you use System Center Virtual Machine Manager to create your shares.

To create file shares by using PowerShell scripts, do the following:

1. Download the scripts included in SMB Share Configuration for Hyper-V Workloads to one of the nodes of the file server cluster.
2. Open a Windows PowerShell session with Domain Administrator credentials on the management system, and then use the following script to create an Active Directory group for the Hyper-V computer objects, changing the values for the variables as appropriate for your environment:

   ```
   # Replace the values of these variables
   $HyperVClusterName = "Compute01"
   $HyperVObjectADGroupSamName = "Hyper-VServerComputerAccounts" <#No spaces#>
   $ScriptFolder = "C:\Scripts\SetupSMBSharesWithHyperV"

   # Start of script itself
   CD $ScriptFolder
   .\ADGroupSetup.ps1 -HyperVObjectADGroupSamName $HyperVObjectADGroupSamName -HyperVClusterName
   $HyperVClusterName
   ```

3. Open a Windows PowerShell session with Administrator credentials on one of the storage nodes, and then use the following script to create shares for each CSV and grant administrative permissions for the shares to the Domain Admins group and the compute cluster.

```
# Replace the values of these variables
$StorageClusterName = "StorageSpacesDirect1"
$HyperVObjectADGroupSamName = "Hyper-VServerComputerAccounts" <#No spaces#>
$SOFSName = "SOFS"
$SharePrefix = "Share"
$ScriptFolder = "C:\Scripts\SetupSMBSharesWithHyperV"

# Start of the script itself
CD $ScriptFolder
Get-ClusterSharedVolume -Cluster $StorageClusterName | ForEach-Object
{
    $ShareName = $SharePrefix +
$_.SharedVolumeInfo.friendlyvolumename.trimstart("C:\ClusterStorage\Volume")
    Write-host "Creating share $ShareName on "$_.name "on Volume: "
$_.SharedVolumeInfo.friendlyvolumename
    .\FileShareSetup.ps1 -HyperVClusterName $StorageClusterName -CSVVolumeNumber
$_.SharedVolumeInfo.friendlyvolumename.trimstart("C:\ClusterStorage\Volume") -ScaleOutFSName $SOFSName
-ShareName $ShareName -HyperVObjectADGroupSamName $HyperVObjectADGroupSamName
}
```

**Step 4.3 Enable Kerberos constrained delegation**

To setup Kerberos constrained delegation for remote scenario management and increased Live Migration security, from one of the storage cluster nodes, use the KCDSetup.ps1 script included in SMB Share Configuration for Hyper-V Workloads. Here's a little wrapper for the script:

```
$HyperVClusterName = "Compute01"
$ScaleOutFSName = "SOFS"
$ScriptFolder = "C:\Scripts\SetupSMBSharesWithHyperV"

CD $ScriptFolder
.\KCDSetup.ps1 -HyperVClusterName $HyperVClusterName -ScaleOutFSName $ScaleOutFSName -EnableLM
```

## Next steps

After deploying your clustered file server, we recommend testing the performance of your solution using synthetic workloads prior to bringing up any real workloads. This lets you confirm that the solution is performing properly and work out any lingering issues before adding the complexity of workloads. For more info, see Test Storage Spaces Performance Using Synthetic Workloads.

## Additional References

- Storage Spaces Direct overview
- Understand the cache in Storage Spaces Direct
- Planning volumes in Storage Spaces Direct
- Storage Spaces Fault Tolerance
- Storage Spaces Direct Hardware Requirements
- To RDMA, or not to RDMA – that is the question (TechNet blog)

# Creating volumes in Storage Spaces Direct

11/2/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic describes how to create volumes on a Storage Spaces Direct cluster by using Windows Admin Center and PowerShell.

> **TIP**
> If you haven't already, check out Planning volumes in Storage Spaces Direct first.

## Create a three-way mirror volume

To create a three-way mirror volume in Windows Admin Center:

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab, and then select **Create volume**.
3. In the **Create volume** pane, enter a name for the volume, and leave **Resiliency** as **Three-way mirror**.
4. In **Size on HDD**, specify the size of the volume. For example, 5 TB (terabytes).
5. Select **Create**.

Depending on the size, creating the volume can take a few minutes. Notifications in the upper-right will let you know when the volume is created. The new volume appears in the Inventory list.

Watch a quick video on how to create a three-way mirror volume.

## Create a mirror-accelerated parity volume

Mirror-accelerated parity reduces the footprint of the volume on the HDD. For example, a three-way mirror volume would mean that for every 10 terabytes of size, you will need 30 terabytes as footprint. To reduce the overhead in footprint, create a volume with mirror-accelerated parity. This reduces the footprint from 30 terabytes to just 22 terabytes, even with only 4 servers, by mirroring the most active 20 percent of data, and using parity, which is more space efficient, to store the rest. You can adjust this ratio of parity and mirror to make the performance versus capacity tradeoff that's right for your workload. For example, 90 percent parity and 10 percent mirror yields less performance but streamlines the footprint even further.

To create a volume with mirror-accelerated parity in Windows Admin Center:

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab, and then select **Create volume**.
3. In the **Create volume** pane, enter a name for the volume.
4. In **Resiliency**, select **Mirror-accelerated parity**.
5. In **Parity percentage**, select the percentage of parity.
6. Select **Create**.

Watch a quick video on how to create a mirror-accelerated parity volume.

## Open volume and add files

To open a volume and add files to the volume in Windows Admin Center:

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab.
3. In the list of volumes, select the name of the volume that you want to open.

   On the volume details page, you can see the path to the volume.
4. At the top of the page, select **Open**. This launches the Files tool in Windows Admin Center.
5. Navigate to the path of the volume. Here you can browse the files in the volume.
6. Select **Upload**, and then select a file to upload.
7. Use the browser **Back** button to go back to the Tools pane in Windows Admin Center.

Watch a quick video on how to open a volume and add files.

## Turn on deduplication and compression

Deduplication and compression is managed per volume. Deduplication and compression uses a post-processing model, which means that you won't see savings until it runs. When it does, it'll work over all files, even those that were there from before.

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab.
3. In the list of volumes, select the name of the volume that want to manage.
4. On the volume details page, click the switch labeled **Deduplication and compression**.
5. In the Enable deduplication pane, select the deduplication mode.

   Instead of complicated settings, Windows Admin Center lets you choose between ready-made profiles for different workloads. If you're not sure, use the default setting.
6. Select **Enable**.

Watch a quick video on how to turn on deduplication and compression.

## Create volumes using PowerShell

We recommend using the **New-Volume** cmdlet to create volumes for Storage Spaces Direct. It provides the fastest and most straightforward experience. This single cmdlet automatically creates the virtual disk, partitions and formats it, creates the volume with matching name, and adds it to cluster shared volumes – all in one easy step.

The **New-Volume** cmdlet has four parameters you'll always need to provide:

- **FriendlyName:** Any string you want, for example *"Volume1"*
- **FileSystem:** Either **CSVFS_ReFS** (recommended) or **CSVFS_NTFS**
- **StoragePoolFriendlyName:** The name of your storage pool, for example *"S2D on ClusterName"*
- **Size:** The size of the volume, for example *"10TB"*

> **NOTE**
> Windows, including PowerShell, counts using binary (base-2) numbers, whereas drives are often labeled using decimal (base-10) numbers. This explains why a "one terabyte" drive, defined as 1,000,000,000,000 bytes, appears in Windows as about "909 GB". This is expected. When creating volumes using **New-Volume**, you should specify the **Size** parameter in binary (base-2) numbers. For example, specifying "909GB" or "0.909495TB" will create a volume of approximately 1,000,000,000,000 bytes.

**Example: With 2 or 3 servers**

To make things easier, if your deployment has only two servers, Storage Spaces Direct will automatically use two-way mirroring for resiliency. If your deployment has only three servers, it will automatically use three-way mirroring.

```
New-Volume -FriendlyName "Volume1" -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size 1TB
```

**Example: With 4+ servers**

If you have four or more servers, you can use the optional **ResiliencySettingName** parameter to choose your resiliency type.

- **ResiliencySettingName:** Either **Mirror** or **Parity**.

In the following example, *"Volume2"* uses three-way mirroring and *"Volume3"* uses dual parity (often called "erasure coding").

```
New-Volume -FriendlyName "Volume2" -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size 1TB -
ResiliencySettingName Mirror
New-Volume -FriendlyName "Volume3" -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size 1TB -
ResiliencySettingName Parity
```

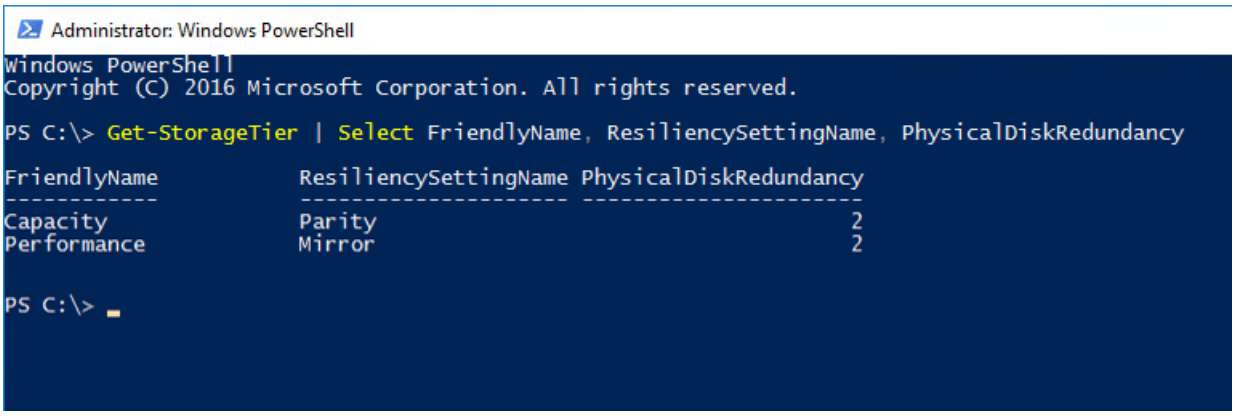
**Example: Using storage tiers**

In deployments with three types of drives, one volume can span the SSD and HDD tiers to reside partially on each. Likewise, in deployments with four or more servers, one volume can mix mirroring and dual parity to reside partially on each.

To help you create such volumes, Storage Spaces Direct provides default tier templates called *Performance* and *Capacity*. They encapsulate definitions for three-way mirroring on the faster capacity drives (if applicable), and dual parity on the slower capacity drives (if applicable).

You can see them by running the **Get-StorageTier** cmdlet.

```
Get-StorageTier | Select FriendlyName, ResiliencySettingName, PhysicalDiskRedundancy
```




To create tiered volumes, reference these tier templates using the **StorageTierFriendlyNames** and **StorageTierSizes** parameters of the **New-Volume** cmdlet. For example, the following cmdlet creates one volume which mixes three-way mirroring and dual parity in 30:70 proportions.

```
New-Volume -FriendlyName "Volume4" -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -
StorageTierFriendlyNames Performance, Capacity -StorageTierSizes 300GB, 700GB
```

You're done! Repeat as needed to create more than one volume.

## Additional References

- Storage Spaces Direct overview
- Planning volumes in Storage Spaces Direct
- Extending volumes in Storage Spaces Direct
- Deleting volumes in Storage Spaces Direct

# Nested resiliency for Storage Spaces Direct

12/16/2020 • 8 minutes to read • Edit Online

Applies to: Windows Server 2019

Nested resiliency is a new capability of Storage Spaces Direct in Windows Server 2019 that enables a two-server cluster to withstand multiple hardware failures at the same time without loss of storage availability, so users, apps, and virtual machines continue to run without disruption. This topic explains how it works, provides step-by-step instructions to get started, and answers the most frequently asked questions.

## Prerequisites

**Consider nested resiliency if:**

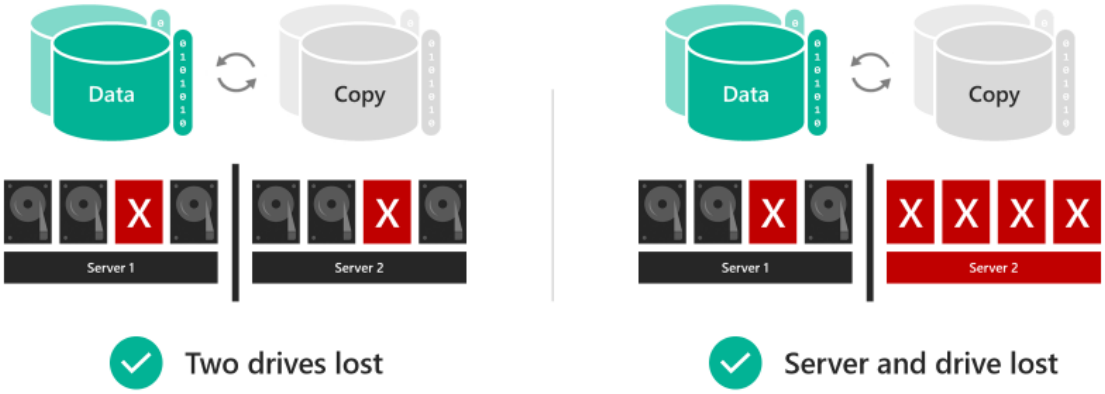
- Your cluster runs Windows Server 2019; and
- Your cluster has exactly 2 server nodes

**You can't use nested resiliency if:**

- Your cluster runs Windows Server 2016; or
- Your cluster has 3 or more server nodes

## Why nested resiliency

Volumes that use nested resiliency can **stay online and accessible even if multiple hardware failures happen at the same time**, unlike classic two-way mirroring resiliency. For example, if two drives fail at the same time, or if a server goes down and a drive fails, volumes that use nested resiliency stay online and accessible. For hyper-converged infrastructure, this increases uptime for apps and virtual machines; for file server workloads, this means users enjoy uninterrupted access to their files.



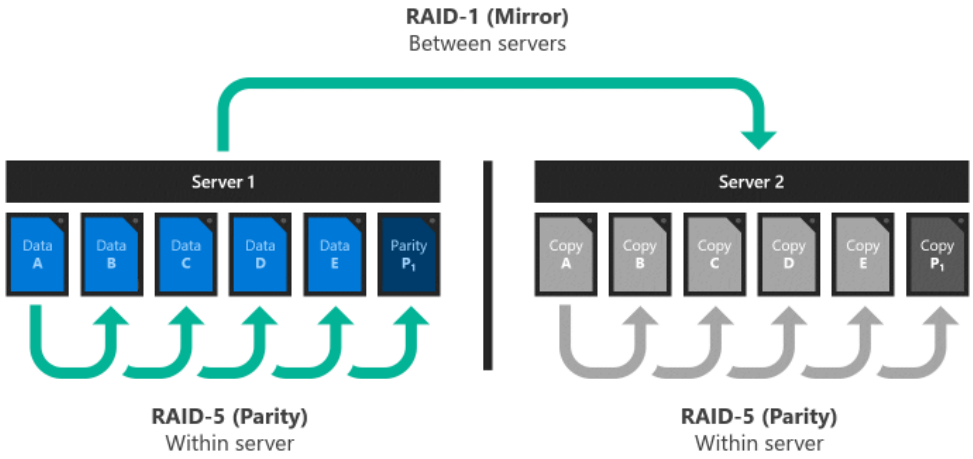

The trade-off is that nested resiliency has **lower capacity efficiency than classic two-way mirroring**, meaning you get slightly less usable space. For details, see the Capacity efficiency section below.

## How it works

**Inspiration: RAID 5+1**

RAID 5+1 is an established form of distributed storage resiliency that provides helpful background for understanding nested resiliency. In RAID 5+1, within each server, local resiliency is provided by RAID-5, or *single parity*, to protect against the loss of any single drive. Then, further resiliency is provided by RAID-1, or *two-way*

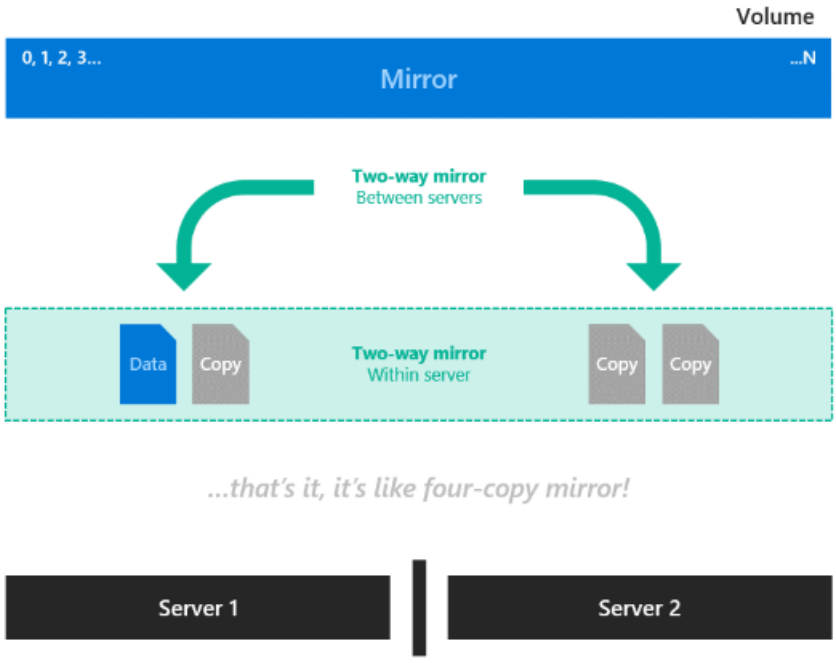
*mirroring*, between the two servers to protect against the loss of either server.



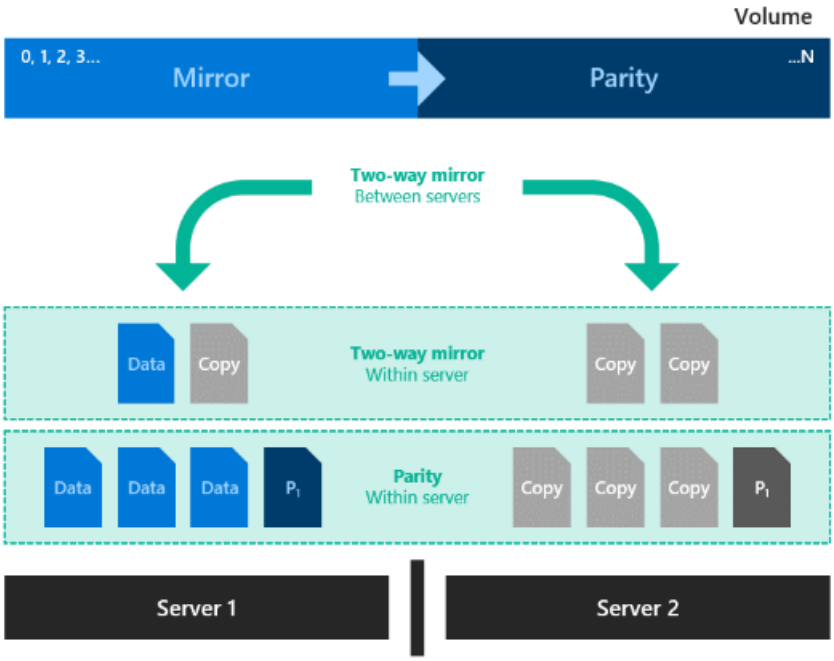

### Two new resiliency options

Storage Spaces Direct in Windows Server 2019 offers two new resiliency options implemented in software, without the need for specialized RAID hardware:

- **Nested two-way mirror.** Within each server, local resiliency is provided by two-way mirroring, and then further resiliency is provided by two-way mirroring between the two servers. It's essentially a four-way mirror, with two copies in each server. Nested two-way mirroring provides uncompromising performance: writes go to all copies, and reads come from any copy.




- **Nested mirror-accelerated parity.** Combine nested two-way mirroring, from above, with nested parity. Within each server, local resiliency for most data is provided by single bitwise parity arithmetic, except new recent writes which use two-way mirroring. Then, further resiliency for all data is provided by two-way mirroring between the servers. For more information about how mirror-accelerated parity works, see Mirror-accelerated parity.




### Capacity efficiency

Capacity efficiency is the ratio of usable space to volume footprint. It describes the capacity overhead attributable to resiliency, and depends on the resiliency option you choose. As a simple example, storing data without resiliency is 100% capacity efficient (1 TB of data takes up 1 TB of physical storage capacity), while two-way mirroring is 50% efficient (1 TB of data takes up 2 TB of physical storage capacity).

- **Nested two-way mirror** writes four copies of everything, meaning to store 1 TB of data, you need 4 TB of physical storage capacity. Although its simplicity is appealing, nested two-way mirror's capacity efficiency of 25% is the lowest of any resiliency option in Storage Spaces Direct.
- **Nested mirror-accelerated parity** achieves higher capacity efficiency, around 35%-40%, that depends on two factors: the number of capacity drives in each server, and the mix of mirror and parity you specify for the volume. This table provides a lookup for common configurations:

| CAPACITY DRIVES PER SERVER | 10% MIRROR | 20% MIRROR | 30% MIRROR |
|---|---|---|---|
| 4 | 35.7% | 34.1% | 32.6% |
| 5 | 37.7% | 35.7% | 33.9% |
| 6 | 39.1% | 36.8% | 34.7% |
| 7+ | 40.0% | 37.5% | 35.3% |

> **NOTE**
>
> **If you're curious, here's an example of the full math.** Suppose we have six capacity drives in each of two servers, and we want to create one 100 GB volume comprised of 10 GB of mirror and 90 GB of parity. Server-local two-way mirror is 50.0% efficient, meaning the 10 GB of mirror data takes 20 GB to store on each server. Mirrored to both servers, its total footprint is 40 GB. Server-local single parity, in this case, is 5/6 = 83.3% efficient, meaning the 90 GB of parity data takes 108 GB to store on each server. Mirrored to both servers, its total footprint is 216 GB. The total footprint is thus [(10 GB / 50.0%) + (90 GB / 83.3%)] × 2 = 256 GB, for 39.1% overall capacity efficiency.

Notice that the capacity efficiency of classic two-way mirroring (about 50%) and nested mirror-accelerated parity

(up to 40%) are not very different. Depending on your requirements, the slightly lower capacity efficiency may be well worth the significant increase in storage availability. You choose resiliency per-volume, so you can mix nested resiliency volumes and classic two-way mirror volumes within the same cluster.


## Usage in PowerShell

You can use familiar storage cmdlets in PowerShell to create volumes with nested resiliency.

### Step 1: Create storage tier templates

First, create new storage tier templates using the `New-StorageTier` cmdlet. You only need to do this once, and then every new volume you create can reference these template. Specify the `-MediaType` of your capacity drives and, optionally, the `-FriendlyName` of your choice. Do not modify the other parameters.

If your capacity drives are hard disk drives (HDD), launch PowerShell as Administrator and run:

```
# For mirror
New-StorageTier -StoragePoolFriendlyName S2D* -FriendlyName NestedMirror -ResiliencySettingName Mirror -
MediaType HDD -NumberOfDataCopies 4

# For parity
New-StorageTier -StoragePoolFriendlyName S2D* -FriendlyName NestedParity -ResiliencySettingName Parity -
MediaType HDD -NumberOfDataCopies 2 -PhysicalDiskRedundancy 1 -NumberOfGroups 1 -FaultDomainAwareness
StorageScaleUnit -ColumnIsolation PhysicalDisk
```

If your capacity drives are solid-state drives (SSD), set the `-MediaType` to `SSD` instead. Do not modify the other parameters.

> **TIP**
> Verify the tiers created successfully with `Get-StorageTier`.

### Step 2: Create volumes

Then, create new volumes using the `New-Volume` cmdlet.

#### Nested two-way mirror

To use nested two-way mirror, reference the `NestedMirror` tier template and specify the size. For example:

```
New-Volume -StoragePoolFriendlyName S2D* -FriendlyName Volume01 -StorageTierFriendlyNames NestedMirror -
StorageTierSizes 500GB
```

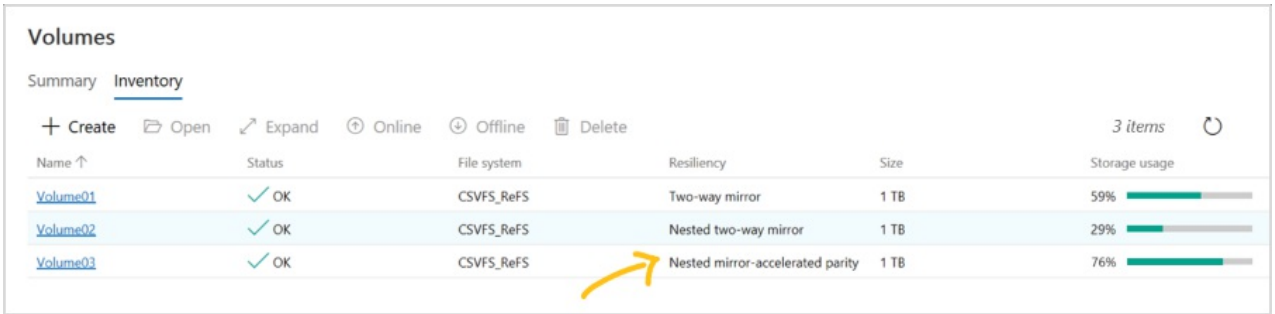
#### Nested mirror-accelerated parity

To use nested mirror-accelerated parity, reference both the `NestedMirror` and `NestedParity` tier templates and specify two sizes, one for each part of the volume (mirror first, parity second). For example, to create one 500 GB volume that's 20% nested two-way mirror and 80% nested parity, run:

```
New-Volume -StoragePoolFriendlyName S2D* -FriendlyName Volume02 -StorageTierFriendlyNames NestedMirror,
NestedParity -StorageTierSizes 100GB, 400GB
```

### Step 3: Continue in Windows Admin Center

Volumes that use nested resiliency appear in Windows Admin Center with clear labeling, as in the screenshot below. Once they're created, you can manage and monitor them using Windows Admin Center just like any other volume in Storage Spaces Direct.




### Optional: Extend to cache drives

With its default settings, nested resiliency protects against the loss of multiple capacity drives at the same time, or one server and one capacity drive at the same time. To extend this protection to cache drives has an additional consideration: because cache drives often provide read *and write* caching for *multiple* capacity drives, the only way to ensure you can tolerate the loss of a cache drive when the other server is down is to simply not cache writes, but that impacts performance.

To address this scenario, Storage Spaces Direct offers the option to automatically disable write caching when one server in a two-server cluster is down, and then re-enable write caching once the server is back up. To allow routine restarts without performance impact, write caching isn't disabled until the server has been down for 30 minutes. Once write caching is disabled, the contents of the write cache is written to capacity devices. After this, the server can tolerate a failed cache device in the online server, though reads from the cache might be delayed or fail if a cache device fails.

To set this behavior (optional), launch PowerShell as Administrator and run:

```
Get-StorageSubSystem Cluster* | Set-StorageHealthSetting -Name
"System.Storage.NestedResiliency.DisableWriteCacheOnNodeDown.Enabled" -Value "True"
```

Once set to **True**, the cache behavior is:

| SITUATION | CACHE BEHAVIOR | CAN TOLERATE CACHE DRIVE LOSS? |
|---|---|---|
| Both servers up | Cache reads and writes, full performance | Yes |
| Server down, first 30 minutes | Cache reads and writes, full performance | No (temporarily) |
| After first 30 minutes | Cache reads only, performance impacted | Yes (after the cache has been written to capacity drives) |

## Frequently asked questions

### Can I convert an existing volume between two-way mirror and nested resiliency?

No, volumes cannot be converted between resiliency types. For new deployments on Windows Server 2019,

decide ahead of time which resiliency type best fits your needs. If you're upgrading from Windows Server 2016, you can create new volumes with nested resiliency, migrate your data, and then delete the older volumes.

**Can I use nested resiliency with multiple types of capacity drives?**

Yes, just specify the `-MediaType` of each tier accordingly during step 1 above. For example, with NVMe, SSD, and HDD in the same cluster, the NVMe provides cache while the latter two provide capacity: set the `NestedMirror` tier to `-MediaType SSD` and the `NestedParity` tier to `-MediaType HDD`. In this case, note that parity capacity efficiency depends on the number of HDD drives only, and you need at least 4 of them per server.

**Can I use nested resiliency with 3 or more servers?**

No, only use nested resiliency if your cluster has exactly 2 servers.

**How many drives do I need to use nested resiliency?**

The minimum number of drives required for Storage Spaces Direct is 4 capacity drives per server node, plus 2 cache drives per server node (if any). This is unchanged from Windows Server 2016. There is no additional requirement for nested resiliency, and the recommendation for reserve capacity is unchanged too.

**Does nested resiliency change how drive replacement works?**

No.

**Does nested resiliency change how server node replacement works?**

No. To replace a server node and its drives, follow this order:

1. Retire the drives in the outgoing server
2. Add the new server, with its drives, to the cluster
3. The storage pool will rebalance
4. Remove the outgoing server and its drives

For details see the Remove servers topic.

## Additional References

- Storage Spaces Direct overview
- Understand fault tolerance in Storage Spaces Direct
- Plan volumes in Storage Spaces Direct
- Create volumes in Storage Spaces Direct

# Configure and manage quorum

12/16/2020 • 20 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic provides background and steps to configure and manage the quorum in a Windows Server failover cluster.

## Understanding quorum

The quorum for a cluster is determined by the number of voting elements that must be part of active cluster membership for that cluster to start properly or continue running. For a more detailed explanation, see the understanding cluster and pool quorum doc.

## Quorum configuration options

The quorum model in Windows Server is flexible. If you need to modify the quorum configuration for your cluster, you can use the Configure Cluster Quorum Wizard or the FailoverClusters Windows PowerShell cmdlets. For steps and considerations to configure the quorum, see Configure the cluster quorum later in this topic.

The following table lists the three quorum configuration options that are available in the Configure Cluster Quorum Wizard.

| OPTION | DESCRIPTION |
| --- | --- |
| Use typical settings | The cluster automatically assigns a vote to each node and dynamically manages the node votes. If it is suitable for your cluster, and there is cluster shared storage available, the cluster selects a disk witness. This option is recommended in most cases, because the cluster software automatically chooses a quorum and witness configuration that provides the highest availability for your cluster. |
| Add or change the quorum witness | You can add, change, or remove a witness resource. You can configure a file share or disk witness. The cluster automatically assigns a vote to each node and dynamically manages the node votes. |
| Advanced quorum configuration and witness selection | You should select this option only when you have application-specific or site-specific requirements for configuring the quorum. You can modify the quorum witness, add or remove node votes, and choose whether the cluster dynamically manages node votes. By default, votes are assigned to all nodes, and the node votes are dynamically managed. |

Depending on the quorum configuration option that you choose and your specific settings, the cluster will be configured in one of the following quorum modes:

| MODE | DESCRIPTION |
| --- | --- |

| MODE | DESCRIPTION |
| --- | --- |
| Node majority (no witness) | Only nodes have votes. No quorum witness is configured. The cluster quorum is the majority of voting nodes in the active cluster membership. |
| Node majority with witness (disk or file share) | Nodes have votes. In addition, a quorum witness has a vote. The cluster quorum is the majority of voting nodes in the active cluster membership plus a witness vote. A quorum witness can be a designated disk witness or a designated file share witness. |
| No majority (disk witness only) | No nodes have votes. Only a disk witness has a vote. The cluster quorum is determined by the state of the disk witness. Generally, this mode is not recommended, and it should not be selected because it creates a single point of failure for the cluster. |

The following subsections will give you more information about advanced quorum configuration settings.

**Witness configuration**

As a general rule when you configure a quorum, the voting elements in the cluster should be an odd number. Therefore, if the cluster contains an even number of voting nodes, you should configure a disk witness or a file share witness. The cluster will be able to sustain one additional node down. In addition, adding a witness vote enables the cluster to continue running if half the cluster nodes simultaneously go down or are disconnected.

A disk witness is usually recommended if all nodes can see the disk. A file share witness is recommended when you need to consider multisite disaster recovery with replicated storage. Configuring a disk witness with replicated storage is possible only if the storage vendor supports read-write access from all sites to the replicated storage. ***A Disk Witness isn't supported with Storage Spaces Direct***.

The following table provides additional information and considerations about the quorum witness types.

| WITNESS TYPE | DESCRIPTION | REQUIREMENTS AND RECOMMENDATIONS |
| --- | --- | --- |
| Disk witness | • Dedicated LUN that stores a copy of the cluster database<br>• Most useful for clusters with shared (not replicated) storage | • Size of LUN must be at least 512 MB<br>• Must be dedicated to cluster use and not assigned to a clustered role<br>• Must be included in clustered storage and pass storage validation tests<br>• Cannot be a disk that is a Cluster Shared Volume (CSV)<br>• Basic disk with a single volume<br>• Does not need to have a drive letter<br>• Can be formatted with NTFS or ReFS<br>• Can be optionally configured with hardware RAID for fault tolerance<br>• Should be excluded from backups and antivirus scanning<br>• A Disk witness isn't supported with Storage Spaces Direct |

| WITNESS TYPE | DESCRIPTION | REQUIREMENTS AND RECOMMENDATIONS |
| --- | --- | --- |
| File share witness | • SMB file share that is configured on a file server running Windows Server<br>• Does not store a copy of the cluster database<br>• Maintains cluster information only in a witness.log file<br>• Most useful for multisite clusters with replicated storage | • Must have a minimum of 5 MB of free space<br>• Must be dedicated to the single cluster and not used to store user or application data<br>• Must have write permissions enabled for the computer object for the cluster name<br><br>The following are additional considerations for a file server that hosts the file share witness:<br>• A single file server can be configured with file share witnesses for multiple clusters.<br>• The file server must be on a site that is separate from the cluster workload. This allows equal opportunity for any cluster site to survive if site-to-site network communication is lost. If the file server is on the same site, that site becomes the primary site, and it is the only site that can reach the file share.<br>• The file server can run on a virtual machine if the virtual machine is not hosted on the same cluster that uses the file share witness.<br>• For high availability, the file server can be configured on a separate failover cluster. |
| Cloud witness | • A witness file stored in Azure blob storage<br>• Recommended when all servers in the cluster have a reliable Internet connection. | See Deploy a cloud witness. |

**Node vote assignment**

As an advanced quorum configuration option, you can choose to assign or remove quorum votes on a per-node basis. By default, all nodes are assigned votes. Regardless of vote assignment, all nodes continue to function in the cluster, receive cluster database updates, and can host applications.

You might want to remove votes from nodes in certain disaster recovery configurations. For example, in a multisite cluster, you could remove votes from the nodes in a backup site so that those nodes do not affect quorum calculations. This configuration is recommended only for manual failover across sites. For more information, see Quorum considerations for disaster recovery configurations later in this topic.

The configured vote of a node can be verified by looking up the **NodeWeight** common property of the cluster node by using the Get-ClusterNode Windows PowerShell cmdlet. A value of 0 indicates that the node does not have a quorum vote configured. A value of 1 indicates that the quorum vote of the node is assigned, and it is managed by the cluster. For more information about management of node votes, see Dynamic quorum

management later in this topic.

The vote assignment for all cluster nodes can be verified by using the **Validate Cluster Quorum** validation test.

**Additional considerations for node vote assignment**

- Node vote assignment is not recommended to enforce an odd number of voting nodes. Instead, you should configure a disk witness or file share witness. For more information, see Witness configuration later in this topic.
- If dynamic quorum management is enabled, only the nodes that are configured to have node votes assigned can have their votes assigned or removed dynamically. For more information, see Dynamic quorum management later in this topic.

### Dynamic quorum management

In Windows Server 2012, as an advanced quorum configuration option, you can choose to enable dynamic quorum management by cluster. For more details on how dynamic quorum works, see this explanation.

With dynamic quorum management, it is also possible for a cluster to run on the last surviving cluster node. By dynamically adjusting the quorum majority requirement, the cluster can sustain sequential node shutdowns to a single node.

The cluster-assigned dynamic vote of a node can be verified with the **DynamicWeight** common property of the cluster node by using the Get-ClusterNode Windows PowerShell cmdlet. A value of 0 indicates that the node does not have a quorum vote. A value of 1 indicates that the node has a quorum vote.

The vote assignment for all cluster nodes can be verified by using the **Validate Cluster Quorum** validation test.

**Additional considerations for dynamic quorum management**

- Dynamic quorum management does not allow the cluster to sustain a simultaneous failure of a majority of voting members. To continue running, the cluster must always have a quorum majority at the time of a node shutdown or failure.
- If you have explicitly removed the vote of a node, the cluster cannot dynamically add or remove that vote.
- When Storage Spaces Direct is enabled, the cluster can only support two node failures. This is explained more in the pool quorum section

## General recommendations for quorum configuration

The cluster software automatically configures the quorum for a new cluster, based on the number of nodes configured and the availability of shared storage. This is usually the most appropriate quorum configuration for that cluster. However, it is a good idea to review the quorum configuration after the cluster is created, before placing the cluster into production. To view the detailed cluster quorum configuration, you can you use the Validate a Configuration Wizard, or the Test-Cluster Windows PowerShell cmdlet, to run the **Validate Quorum Configuration** test. In Failover Cluster Manager, the basic quorum configuration is displayed in the summary information for the selected cluster, or you can review the information about quorum resources that returns when you run the Get-ClusterQuorum Windows PowerShell cmdlet.

At any time, you can run the **Validate Quorum Configuration** test to validate that the quorum configuration is optimal for your cluster. The test output indicates if a change to the quorum configuration is recommended and the settings that are optimal. If a change is recommended, you can use the Configure Cluster Quorum Wizard to apply the recommended settings.

After the cluster is in production, do not change the quorum configuration unless you have determined that the change is appropriate for your cluster. You might want to consider changing the quorum configuration in the following situations:

- Adding or evicting nodes

- Adding or removing storage
- A long-term node or witness failure
- Recovering a cluster in a multisite disaster recovery scenario

For more information about validating a failover cluster, see Validate Hardware for a Failover Cluster.

## Configure the cluster quorum

You can configure the cluster quorum settings by using Failover Cluster Manager or the FailoverClusters Windows PowerShell cmdlets.

> **IMPORTANT**
> It is usually best to use the quorum configuration that is recommended by the Configure Cluster Quorum Wizard. We recommend customizing the quorum configuration only if you have determined that the change is appropriate for your cluster. For more information, see General recommendations for quorum configuration in this topic.

**Configure the cluster quorum settings**

Membership in the local **Administrators** group on each clustered server, or equivalent, is the minimum permissions required to complete this procedure. Also, the account you use must be a domain user account.

> **NOTE**
> You can change the cluster quorum configuration without stopping the cluster or taking cluster resources offline.

**Change the quorum configuration in a failover cluster by using Failover Cluster Manager**

1. In Failover Cluster Manager, select or specify the cluster that you want to change.
2. With the cluster selected, under **Actions**, select **More Actions**, and then select **Configure Cluster Quorum Settings**. The Configure Cluster Quorum Wizard appears. Select **Next**.
3. On the **Select Quorum Configuration Option** page, select one of the three configuration options and complete the steps for that option. Before you configure the quorum settings, you can review your choices. For more information about the options, see Understanding quorum, earlier in this topic.
   - To allow the cluster to automatically reset the quorum settings that are optimal for your current cluster configuration, select **Use default quorum configuration** and then complete the wizard.
   - To add or change the quorum witness, select **Select the quorum witness**, and then complete the following steps. For information and considerations about configuring a quorum witness, see Witness configuration earlier in this topic.
     a. On the **Select Quorum Witness** page, select an option to configure a disk witness or a file share witness. The wizard indicates the witness selection options that are recommended for your cluster.

        > **NOTE**
        > You can also select **Do not configure a quorum witness** and then complete the wizard. If you have an even number of voting nodes in your cluster, this may not be a recommended configuration.

     b. If you select the option to configure a disk witness, on the **Configure Storage Witness** page, select the storage volume that you want to assign as the disk witness, and then complete the wizard.

c. If you select the option to configure a file share witness, on the **Configure File Share Witness** page, type or browse to a file share that will be used as the witness resource, and then complete the wizard.

d. If you select the option to configure a cloud witness, on the **Configure Cloud Witness** page, enter your Azure storage account name, Azure storage account key and the Azure service endpoint, and then complete the wizard.

> **NOTE**
> This option is available in Windows Server 2016 and above.

- To configure quorum management settings and to add or change the quorum witness, select **Advanced quorum configuration**, and then complete the following steps. For information and considerations about the advanced quorum configuration settings, see Node vote assignment and Dynamic quorum management earlier in this topic.

  a. On the **Select Voting Configuration** page, select an option to assign votes to nodes. By default, all nodes are assigned a vote. However, for certain scenarios, you can assign votes only to a subset of the nodes.

  > **NOTE**
  > You can also select **No Nodes**. This is generally not recommended, because it does not allow nodes to participate in quorum voting, and it requires configuring a disk witness. This disk witness becomes the single point of failure for the cluster.

  b. On the **Configure Quorum Management** page, you can enable or disable the **Allow cluster to dynamically manage the assignment of node votes** option. Selecting this option generally increases the availability of the cluster. By default the option is enabled, and it is strongly recommended to not disable this option. This option allows the cluster to continue running in failure scenarios that are not possible when this option is disabled.

  > **NOTE**
  > This option is not present in Windows Server 2016 and above.

  c. On the **Select Quorum Witness** page, select an option to configure a disk witness, file share witness or a cloud witness. The wizard indicates the witness selection options that are recommended for your cluster.

  > **NOTE**
  > You can also select **Do not configure a quorum witness**, and then complete the wizard. If you have an even number of voting nodes in your cluster, this may not be a recommended configuration.

  d. If you select the option to configure a disk witness, on the **Configure Storage Witness** page, select the storage volume that you want to assign as the disk witness, and then complete the wizard.

  e. If you select the option to configure a file share witness, on the **Configure File Share Witness** page, type or browse to a file share that will be used as the witness resource, and then complete the wizard.

f. If you select the option to configure a cloud witness, on the **Configure Cloud Witness** page, enter your Azure storage account name, Azure storage account key and the Azure service endpoint, and then complete the wizard.

> **NOTE**
> This option is available in Windows Server 2016 and above.

4. Select **Next**. Confirm your selections on the confirmation page that appears, and then select **Next**.

After the wizard runs and the **Summary** page appears, if you want to view a report of the tasks that the wizard performed, select **View Report**. The most recent report will remain in the *systemroot***Cluster\Reports** folder with the name **QuorumConfiguration.mht**.

> **NOTE**
> After you configure the cluster quorum, we recommend that you run the **Validate Quorum Configuration** test to verify the updated quorum settings.

**Windows PowerShell equivalent commands**

The following examples show how to use the Set-ClusterQuorum cmdlet and other Windows PowerShell cmdlets to configure the cluster quorum.

The following example changes the quorum configuration on cluster *CONTOSO-FC1* to a simple node majority configuration with no quorum witness.

```
Set-ClusterQuorum –Cluster CONTOSO-FC1 -NodeMajority
```

The following example changes the quorum configuration on the local cluster to a node majority with witness configuration. The disk resource named *Cluster Disk 2* is configured as a disk witness.

```
Set-ClusterQuorum -NodeAndDiskMajority "Cluster Disk 2"
```

The following example changes the quorum configuration on the local cluster to a node majority with witness configuration. The file share resource named *\\CONTOSO-FS\fsw* is configured as a file share witness.

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\fileserver\fsw"
```

The following example removes the quorum vote from node *ContosoFCNode1* on the local cluster.

```
(Get-ClusterNode ContosoFCNode1).NodeWeight=0
```

The following example adds the quorum vote to node *ContosoFCNode1* on the local cluster.

```
(Get-ClusterNode ContosoFCNode1).NodeWeight=1
```

The following example enables the **DynamicQuorum** property of the cluster *CONTOSO-FC1* (if it was previously disabled):

```
(Get-Cluster CONTOSO-FC1).DynamicQuorum=1
```

## Recover a cluster by starting without quorum

A cluster that does not have enough quorum votes will not start. As a first step, you should always confirm the cluster quorum configuration and investigate why the cluster no longer has quorum. This might happen if you have nodes that stopped responding, or if the primary site is not reachable in a multisite cluster. After you identify the root cause for the cluster failure, you can use the recovery steps described in this section.

> **NOTE**
>
> - If the Cluster service stops because quorum is lost, Event ID 1177 appears in the system log.
> - It is always necessary to investigate why the cluster quorum was lost.
> - It is always preferable to bring a node or quorum witness to a healthy state (join the cluster) rather than starting the cluster without quorum.

### Force start cluster nodes

After you determine that you cannot recover your cluster by bringing the nodes or quorum witness to a healthy state, forcing your cluster to start becomes necessary. Forcing the cluster to start overrides your cluster quorum configuration settings and starts the cluster in **ForceQuorum** mode.

Forcing a cluster to start when it does not have quorum may be especially useful in a multisite cluster. Consider a disaster recovery scenario with a cluster that contains separately located primary and backup sites, *SiteA* and *SiteB*. If there is a genuine disaster at *SiteA*, it could take a significant amount of time for the site to come back online. You would likely want to force *SiteB* to come online, even though it does not have quorum.

When a cluster is started in **ForceQuorum** mode, and after it regains sufficient quorum votes, the cluster automatically leaves the forced state, and it behaves normally. Hence, it is not necessary to start the cluster again normally. If the cluster loses a node and it loses quorum, it goes offline again because it is no longer in the forced state. To bring it back online when it does not have quorum requires forcing the cluster to start without quorum.

> **IMPORTANT**
>
> - After a cluster is force started, the administrator is in full control of the cluster.
> - The cluster uses the cluster configuration on the node where the cluster is force started, and replicates it to all other nodes that are available.
> - If you force the cluster to start without quorum, all quorum configuration settings are ignored while the cluster remains in **ForceQuorum** mode. This includes specific node vote assignments and dynamic quorum management settings.

### Prevent quorum on remaining cluster nodes

After you have force started the cluster on a node, it is necessary to start any remaining nodes in your cluster with a setting to prevent quorum. A node started with a setting that prevents quorum indicates to the Cluster service to join an existing running cluster instead of forming a new cluster instance. This prevents the remaining nodes from forming a split cluster that contains two competing instances.

This becomes necessary when you need to recover your cluster in some multisite disaster recovery scenarios after you have force started the cluster on your backup site, *SiteB*. To join the force started cluster in *SiteB*, the nodes in your primary site, *SiteA*, need to be started with the quorum prevented.

> **IMPORTANT**
> After a cluster is force started on a node, we recommend that you always start the remaining nodes with the quorum prevented.

Here's how to recover the cluster with Failover Cluster Manager:

1. In Failover Cluster Manager, select or specify the cluster you want to recover.
2. With the cluster selected, under **Actions**, select **Force Cluster Start**.

   Failover Cluster Manager force starts the cluster on all nodes that are reachable. The cluster uses the current cluster configuration when starting.

> **NOTE**
> - To force the cluster to start on a specific node that contains a cluster configuration that you want to use, you must use the Windows PowerShell cmdlets or equivalent command-line tools as presented after this procedure.
> - If you use Failover Cluster Manager to connect to a cluster that is force started, and you use the **Start Cluster Service** action to start a node, the node is automatically started with the setting that prevents quorum.

**Windows PowerShell equivalent commands (Start-Clusternode)**

The following example shows how to use the **Start-ClusterNode** cmdlet to force start the cluster on node *ContosoFCNode1*.

```
Start-ClusterNode –Node ContosoFCNode1 –FQ
```

Alternatively, you can type the following command locally on the node:

```
Net Start ClusSvc /FQ
```

The following example shows how to use the **Start-ClusterNode** cmdlet to start the Cluster service with the quorum prevented on node *ContosoFCNode1*.

```
Start-ClusterNode –Node ContosoFCNode1 –PQ
```

Alternatively, you can type the following command locally on the node:

```
Net Start ClusSvc /PQ
```

## Quorum considerations for disaster recovery configurations

This section summarizes characteristics and quorum configurations for two multisite cluster configurations in disaster recovery deployments. The quorum configuration guidelines differ depending on if you need automatic failover or manual failover for workloads between the sites. Your configuration usually depends on the service level agreements (SLAs) that are in place in your organization to provide and support clustered workloads in the event of a failure or disaster at a site.

### Automatic failover

In this configuration, the cluster consists of two or more sites that can host clustered roles. If a failure occurs at any site, the clustered roles are expected to automatically fail over to the remaining sites. Therefore, the cluster

quorum must be configured so that any site can sustain a complete site failure.

The following table summarizes considerations and recommendations for this configuration.

| ITEM | DESCRIPTION |
|---|---|
| Number of node votes per site | Should be equal |
| Node vote assignment | Node votes should not be removed because all nodes are equally important |
| Dynamic quorum management | Should be enabled |
| Witness configuration | File share witness is recommended, configured in a site that is separate from the cluster sites |
| Workloads | Workloads can be configured on any of the sites |

**Additional considerations for automatic failover**

- Configuring the file share witness in a separate site is necessary to give each site an equal opportunity to survive. For more information, see Witness configuration earlier in this topic.

### Manual failover

In this configuration, the cluster consists of a primary site, *SiteA*, and a backup (recovery) site, *SiteB*. Clustered roles are hosted on *SiteA*. Because of the cluster quorum configuration, if a failure occurs at all nodes in *SiteA*, the cluster stops functioning. In this scenario the administrator must manually fail over the cluster services to *SiteB* and perform additional steps to recover the cluster.

The following table summarizes considerations and recommendations for this configuration.

| ITEM | DESCRIPTION |
|---|---|
| Number of node votes per site | • Node votes should not be removed from nodes at the primary site, **SiteA**<br>• Node votes should be removed from nodes at the backup site, **SiteB**<br>• If a long-term outage occurs at **SiteA**, votes must be assigned to nodes at **SiteB** to enable a quorum majority at that site as part of recovery |
| Dynamic quorum management | Should be enabled |
| Witness configuration | • Configure a witness if there is an even number of nodes at **SiteA**<br>• If a witness is needed, configure either a file share witness or a disk witness that is accessible only to nodes in **SiteA** (sometimes called an asymmetric disk witness) |
| Workloads | Use preferred owners to keep workloads running on nodes at **SiteA** |

**Additional considerations for manual failover**

- Only the nodes at *SiteA* are initially configured with quorum votes. This is necessary to ensure that the state of nodes at *SiteB* does not affect the cluster quorum.

- Recovery steps can vary depending on if *SiteA* sustains a temporary failure or a long-term failure.

## More information

- Failover Clustering
- Failover Clusters Windows PowerShell cmdlets
- Understanding Cluster and Pool Quorum

# Upgrade a Storage Spaces Direct cluster to Windows Server 2019

11/2/2020 • 14 minutes to read • Edit Online

This topic describes how to upgrade a Storage Spaces Direct cluster to Windows Server 2019. There are four approaches to upgrading a Storage Spaces Direct cluster from Windows Server 2016 to Windows Server 2019, using the cluster OS rolling upgrade process —two that involve keeping the VMs running, and two that involve stopping all VMs. Each approach has different strengths and weaknesses, so select that one that best suits the needs of your organization:

- **In-place upgrade while VMs are running** on each server in the cluster—this option incurs no VM downtime, but you'll need to wait for storage jobs (mirror repair) to complete after each server is upgraded.
- **Clean-OS installation while VMs are running** on each server in the cluster—this option incurs no VM downtime, but you'll need to wait for storage jobs (mirror repair) to complete after each server is upgraded, and you'll have to set up each server and all its apps and roles again.
- **In-place upgrade while VMs are stopped** on each server in the cluster—this option incurs VM downtime, but you don't need to wait for storage jobs (mirror repair), so it's faster.
- **Clean-OS install while VMs are stopped** on each server in the cluster—This option incurs VM downtime, but you don't need to wait for storage jobs (mirror repair) so it's faster.

## Prerequisites and limitations

Before proceeding with an upgrade:

- Check that you have usable backups in case there are any issues during the upgrade process.
- Check that your hardware vendor has a BIOS, firmware, and drivers for your servers that they will support on Windows Server 2019.

There are some limitations with the upgrade process to be aware of:

- To enable Storage Spaces Direct with Windows Server 2019 builds earlier than 176693.292, customers may need to contact Microsoft support for registry keys that enable Storage Spaces Direct and Software Defined Networking functionality. For more info, see Microsoft Knowledge Base article 4464776.
- When upgrading a cluster with ReFS volumes, there are a few limitations:
- Upgrading is fully supported on ReFS volumes, however, upgraded volumes won't benefit from ReFS enhancements in Windows Server 2019. These benefits, such as increased performance for mirror-accelerated parity, require a newly-created Windows Server 2019 ReFS volume. In other words, you'd have to create new volumes using the `New-Volume` cmdlet or Server Manager. Here are the some of the ReFS enhancements new volumes would get:
  - **MAP log-bypass**: a performance improvement in ReFS that only applies to clustered (Storage Spaces Direct) systems and doesn't apply to stand-alone storage pools.
  - **Compaction** efficiency improvements in Windows Server 2019 that are specific to multi-resilient volumes.
- Before upgrading a Windows Server 2016 Storage Spaces Direct cluster server, we recommend putting the

server into storage maintenance mode. For more info, see the Event 5120 section of Troubleshoot Storage Spaces Direct. Although this issue has been fixed in Windows Server 2016, we recommend putting each Storage Spaces Direct server into storage maintenance mode during the upgrade as a best practice.

- There is a known issue with Software Defined Networking environments that use SET switches. This issue involves Hyper-V VM live migrations from Windows Server 2019 to Windows Server 2016 (live migration to an earlier operating system). To ensure successful live migrations, we recommend changing a VM network setting on VMs that are being live-migrated from Windows Server 2019 to Windows Server 2016. This issue is fixed for Windows Server 2019 in the 2019-01D hotfix rollup package, AKA build 17763.292. For more info, see Microsoft Knowledge Base article 4476976.

Because of the known issues above, some customers may consider building a new Windows Server 2019 cluster and copying data from the old cluster, instead of upgrading their Windows Server 2016 clusters using one of the four processes described below.

## Performing an in-place upgrade while VMs are running

This option incurs no VM downtime, but you'll need to wait for storage jobs (mirror repair) to complete after each server is upgraded. Although individual servers will be restarted sequentially during the upgrade process, the remaining servers in the cluster, as well as all VMs, will remain running.

1. Check that all the servers in the cluster have installed the latest Windows updates. For more info, see Windows 10 and Windows Server 2016 update history. At a minimum, install Microsoft Knowledge Base article 4487006 (Feb 19th, 2019). The build number (see `ver` command) should be 14393.2828 or higher.

2. If you're using Software Defined Networking with SET switches, open an elevated PowerShell session and run the following command to disable VM live migration verification checks on all VMs on the cluster:

   ```
   Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |
   Set-ClusterParameter -Create SkipMigrationDestinationCheck -Value 1
   ```

3. Perform the following steps on one cluster server at a time:

   a. Use Hyper-V VM live migration to move running VMs off the server you're about to upgrade.

   b. Pause the cluster server using the following PowerShell command—note that some internal groups are hidden. We recommend this step to be cautious — if you didn't already live migrate VMs off the server this cmdlet will do that for you, so you could skip the previous step if you prefer.

      ```
      Suspend-ClusterNode -Drain
      ```

   c. Place the server in storage maintenance mode by running the following PowerShell commands:

      ```
      Get-StorageFaultDomain -type StorageScaleUnit |
      Where FriendlyName -Eq <ServerName> |
      Enable-StorageMaintenanceMode
      ```

   d. Run the following cmdlet to check that the **OperationalStatus** value is **In Maintenance Mode**:

      ```
      Get-PhysicalDisk
      ```

   e. Perform an upgrade installation of Windows Server 2019 on the server by running **setup.exe** and using the "Keep personal files and apps" option. After installation is complete, the server remains in the cluster and the cluster service starts automatically.

f. Check that the newly upgraded server has the latest Windows Server 2019 updates. For more info, see Windows 10 and Windows Server 2019 update history. The build number (see `ver` command) should be 17763.292 or higher.

g. Remove the server from storage maintenance mode by using the following PowerShell command:

```
Get-StorageFaultDomain -type StorageScaleUnit |
Where FriendlyName -Eq <ServerName> |
Disable-StorageMaintenanceMode
```

h. Resume the server by using the following PowerShell command:

```
Resume-ClusterNode
```

i. Wait for storage repair jobs to finish and for all disks to return to a healthy state. This could take considerable time depending on the number of VMs running during the server upgrade. Here are the commands to run:

```
Get-StorageJob
Get-VirtualDisk
```

4. Upgrade the next server in the cluster.

5. After all servers have been upgraded to Windows Server 2019, use the following PowerShell cmdlet to update the cluster functional level.

```
Update-ClusterFunctionalLevel
```

> **NOTE**
> We recommend updating the cluster functional level as soon as possible, though technically you have up to four weeks to do so.

6. After the cluster functional level has been updated, use the following cmdlet to update the storage pool. At this point, new cmdlets such as `Get-ClusterPerf` will be fully operational on any server in the cluster.

```
Update-StoragePool
```

7. Optionally upgrade VM configuration levels by stopping each VM, using the `Update-VMVersion` cmdlet, and then starting the VMs again.

8. If you're using Software Defined Networking with SET switches and disabled VM live migration checks as instructed to above, use the following cmdlet to re-enable VM Live verification checks:

```
Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |
Set-ClusterParameter  SkipMigrationDestinationCheck -Value 0
```

9. Verify that the upgraded cluster functions as expected. Roles should fail-over correctly and if VM live migration is used on the cluster, VMs should successfully live migrate.

10. Validate the cluster by running Cluster Validation ( `Test-Cluster` ) and examining the cluster validation report.

## Performing a clean OS installation while VMs are running

This option incurs no VM downtime, but you'll need to wait for storage jobs (mirror repair) to complete after each server is upgraded. Although individual servers will be restarted sequentially during the upgrade process, the remaining servers in the cluster, as well as all VMs, will remain running.

1. Check that all the servers in the cluster are running the latest updates. For more info, see Windows 10 and Windows Server 2016 update history. At a minimum, install Microsoft Knowledge Base article 4487006 (Feb 19th, 2019). The build number (see `ver` command) should be 14393.2828 or higher.

2. If you're using Software Defined Networking with SET switches, open an elevated PowerShell session and run the following command to disable VM live migration verification checks on all VMs on the cluster:

   ```
   Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |
   Set-ClusterParameter -Create SkipMigrationDestinationCheck -Value 1
   ```

3. Perform the following steps on one cluster server at a time:

   a. Use Hyper-V VM live migration to move running VMs off the server you're about to upgrade.

   b. Pause the cluster server using the following PowerShell command—note that some internal groups are hidden. We recommend this step to be cautious — if you didn't already live migrate VMs off the server this cmdlet will do that for you, so you could skip the previous step if you prefer.

      ```
      Suspend-ClusterNode -Drain
      ```

   c. Place the server in storage maintenance mode by running the following PowerShell commands:

      ```
      Get-StorageFaultDomain -type StorageScaleUnit |
      Where FriendlyName -Eq <ServerName> |
      Enable-StorageMaintenanceMode
      ```

   d. Run the following cmdlet to check that the **OperationalStatus** value is **In Maintenance Mode**:

      ```
      Get-PhysicalDisk
      ```

   e. Evict the server from the cluster by running the following PowerShell command:

      ```
      Remove-ClusterNode <ServerName>
      ```

   f. Perform a clean installation of Windows Server 2019 on the server: format the system drive, run **setup.exe** and use the "Nothing" option. You'll have to configure the server identity, roles, features, and applications after setup completes and the server restarts.

   g. Install the Hyper-V role and Failover-Clustering feature on the server (you can use the `Install-WindowsFeature` cmdlet).

   h. Install the latest storage and networking drivers for your hardware that are approved by your server manufacturer for use with Storage Spaces Direct.

   i. Check that the newly upgraded server has the latest Windows Server 2019 updates. For more info, see Windows 10 and Windows Server 2019 update history. The build number (see `ver` command) should be 17763.292 or higher.

j. Rejoin the server to the cluster by using the following PowerShell command:

```
Add-ClusterNode
```

k. Remove the server from storage maintenance mode by using the following PowerShell commands:

```
Get-StorageFaultDomain -type StorageScaleUnit |
Where FriendlyName -Eq <ServerName> |
Disable-StorageMaintenanceMode
```

l. Wait for storage repair jobs to finish and for all disks to return to a healthy state. This could take considerable time depending on the number of VMs running during the server upgrade. Here are the commands to run:

```
Get-StorageJob
Get-VirtualDisk
```

4. Upgrade the next server in the cluster.

5. After all servers have been upgraded to Windows Server 2019, use the following PowerShell cmdlet to update the cluster functional level.

```
Update-ClusterFunctionalLevel
```

> **NOTE**
> We recommend updating the cluster functional level as soon as possible, though technically you have up to four weeks to do so.

6. After the cluster functional level has been updated, use the following cmdlet to update the storage pool. At this point, new cmdlets such as `Get-ClusterPerf` will be fully operational on any server in the cluster.

```
Update-StoragePool
```

7. Optionally upgrade VM configuration levels by stopping each VM and using the `Update-VMVersion` cmdlet, and then starting the VMs again.

8. If you're using Software Defined Networking with SET switches and disabled VM live migration checks as instructed to above, use the following cmdlet to re-enable VM Live verification checks:

```
Get-ClusterResourceType -Cluster {clusterName} -Name "Virtual Machine" |
Set-ClusterParameter SkipMigrationDestinationCheck -Value 0
```

9. Verify that the upgraded cluster functions as expected. Roles should fail-over correctly and if VM live migration is used on the cluster, VMs should successfully live migrate.

10. Validate the cluster by running Cluster Validation ( `Test-Cluster` ) and examining the cluster validation report.

## Performing an in-place upgrade while VMs are stopped

This option incurs VM downtime but can take less time than if you kept the VMs running during the upgrade because you don't need to wait for storage jobs (mirror repair) to complete after each server is upgraded. Although individual servers will be restarted sequentially during the upgrade process, the remaining servers in the cluster remain running.

1. Check that all the servers in the cluster are running the latest updates. For more info, see Windows 10 and Windows Server 2016 update history. At a minimum, install Microsoft Knowledge Base article 4487006 (Feb 19th, 2019). The build number (see `ver` command) should be 14393.2828 or higher.
2. Stop the VMs running on the cluster.
3. Perform the following steps on one cluster server at a time:
   a. Pause the cluster server using the following PowerShell command—note that some internal groups are hidden. We recommend this step to be cautious.

      ```
      Suspend-ClusterNode -Drain
      ```

   b. Place the server in storage maintenance mode by running the following PowerShell commands:

      ```
      Get-StorageFaultDomain -type StorageScaleUnit |
      Where FriendlyName -Eq <ServerName> |
      Enable-StorageMaintenanceMode
      ```

   c. Run the following cmdlet to check that the **OperationalStatus** value is **In Maintenance Mode**:

      ```
      Get-PhysicalDisk
      ```

   d. Perform an upgrade installation of Windows Server 2019 on the server by running **setup.exe** and using the "Keep personal files and apps" option. After installation is complete, the server remains in the cluster and the cluster service starts automatically.
   e. Check that the newly upgraded server has the latest Windows Server 2019 updates. For more info, see Windows 10 and Windows Server 2019 update history. The build number (see `ver` command) should be 17763.292 or higher.
   f. Remove the server from storage maintenance mode by using the following PowerShell commands:

      ```
      Get-StorageFaultDomain -type StorageScaleUnit |
      Where FriendlyName -Eq <ServerName> |
      Disable-StorageMaintenanceMode
      ```

   g. Resume the server by using the following PowerShell command:

      ```
      Resume-ClusterNode
      ```

   h. Wait for storage repair jobs to finish and for all disks to return to a healthy state. This should be relatively fast, since VMs are not running. Here are the commands to run:

      ```
      Get-StorageJob
      Get-VirtualDisk
      ```

4. Upgrade the next server in the cluster.

5. After all servers have been upgraded to Windows Server 2019, use the following PowerShell cmdlet to update the cluster functional level.

   ```
   Update-ClusterFunctionalLevel
   ```

   > **NOTE**
   > We recommend updating the cluster functional level as soon as possible, though technically you have up to four weeks to do so.

6. After the cluster functional level has been updated, use the following cmdlet to update the storage pool. At this point, new cmdlets such as `Get-ClusterPerf` will be fully operational on any server in the cluster.

   ```
   Update-StoragePool
   ```

7. Start the VMs on the cluster and check that they're working properly.
8. Optionally upgrade VM configuration levels by stopping each VM and using the `Update-VMVersion` cmdlet, and then starting the VMs again.
9. Verify that the upgraded cluster functions as expected. Roles should fail-over correctly and if VM live migration is used on the cluster, VMs should successfully live migrate.
10. Validate the cluster by running Cluster Validation ( `Test-Cluster` ) and examining the cluster validation report.

## Performing a clean OS installation while VMs are stopped

This option incurs VM downtime but can take less time than if you kept the VMs running during the upgrade because you don't need to wait for storage jobs (mirror repair) to complete after each server is upgraded. Although individual servers will be restarted sequentially during the upgrade process, the remaining servers in the cluster remain running.

1. Check that all the servers in the cluster are running the latest updates. For more info, see Windows 10 and Windows Server 2016 update history. At a minimum, install Microsoft Knowledge Base article 4487006 (Feb 19th, 2019). The build number (see `ver` command) should be 14393.2828 or higher.
2. Stop the VMs running on the cluster.
3. Perform the following steps on one cluster server at a time:

   b. Pause the cluster server using the following PowerShell command—note that some internal groups are hidden. We recommend this step to be cautious.

   ```
   Suspend-ClusterNode -Drain
   ```

   c. Place the server in storage maintenance mode by running the following PowerShell commands:

   ```
   Get-StorageFaultDomain -type StorageScaleUnit |
   Where FriendlyName -Eq <ServerName> |
   Enable-StorageMaintenanceMode
   ```

   d. Run the following cmdlet to check that the **OperationalStatus** value is **In Maintenance Mode**:

```
Get-PhysicalDisk
```

e. Evict the server from the cluster by running the following PowerShell command:

```
Remove-ClusterNode <ServerName>
```

f. Perform a clean installation of Windows Server 2019 on the server: format the system drive, run **setup.exe** and use the "Nothing" option. You'll have to configure the server identity, roles, features, and applications after setup completes and the server restarts.

g. Install the Hyper-V role and Failover-Clustering feature on the server (you can use the `Install-WindowsFeature` cmdlet).

h. Install the latest storage and networking drivers for your hardware that are approved by your server manufacturer for use with Storage Spaces Direct.

i. Check that the newly upgraded server has the latest Windows Server 2019 updates. For more info, see Windows 10 and Windows Server 2019 update history. The build number (see `ver` command) should be 17763.292 or higher.

j. Rejoin the server to the cluster by using the following PowerShell command:

```
Add-ClusterNode
```

k. Remove the server from storage maintenance mode by using the following PowerShell command:

```
Get-StorageFaultDomain -type StorageScaleUnit |
Where FriendlyName -Eq <ServerName> |
Disable-StorageMaintenanceMode
```

l. Wait for storage repair jobs to finish and for all disks to return to a healthy state. This could take considerable time depending on the number of VMs running during the server upgrade. Here are the commands to run:

```
Get-StorageJob
Get-VirtualDisk
```

4. Upgrade the next server in the cluster.

5. After all servers have been upgraded to Windows Server 2019, use the following PowerShell cmdlet to update the cluster functional level.

```
Update-ClusterFunctionalLevel
```

> **NOTE**
> We recommend updating the cluster functional level as soon as possible, though technically you have up to four weeks to do so.

6. After the cluster functional level has been updated, use the following cmdlet to update the storage pool. At this point, new cmdlets such as `Get-ClusterPerf` will be fully operational on any server in the cluster.

```
Update-StoragePool
```

7. Start the VMs on the cluster and check that they're working properly.
8. Optionally upgrade VM configuration levels by stopping each VM and using the `Update-VMVersion` cmdlet, and then starting the VMs again.
9. Verify that the upgraded cluster functions as expected. Roles should fail-over correctly and if VM live migration is used on the cluster, VMs should successfully live migrate.
10. Validate the cluster by running Cluster Validation ( `Test-Cluster` ) and examining the cluster validation report.

# Understand and deploy persistent memory

11/2/2020 • 10 minutes to read • Edit Online

Applies to: Windows Server 2019

Persistent memory (or PMem) is a new type of memory technology that delivers a unique combination of affordable large capacity and persistence. This article provides background on PMem and the steps to deploy it in Windows Server 2019 by using Storage Spaces Direct.

## Background

PMem is a type of non-volatile RAM (NVDIMM) that retains its content through power cycles. Memory contents remain even when system power goes down in the event of an unexpected power loss, user initiated shutdown, system crash, and so on. This unique characteristic means that you can also use PMem as storage. This is why you may hear people refer to PMem as "storage-class memory."

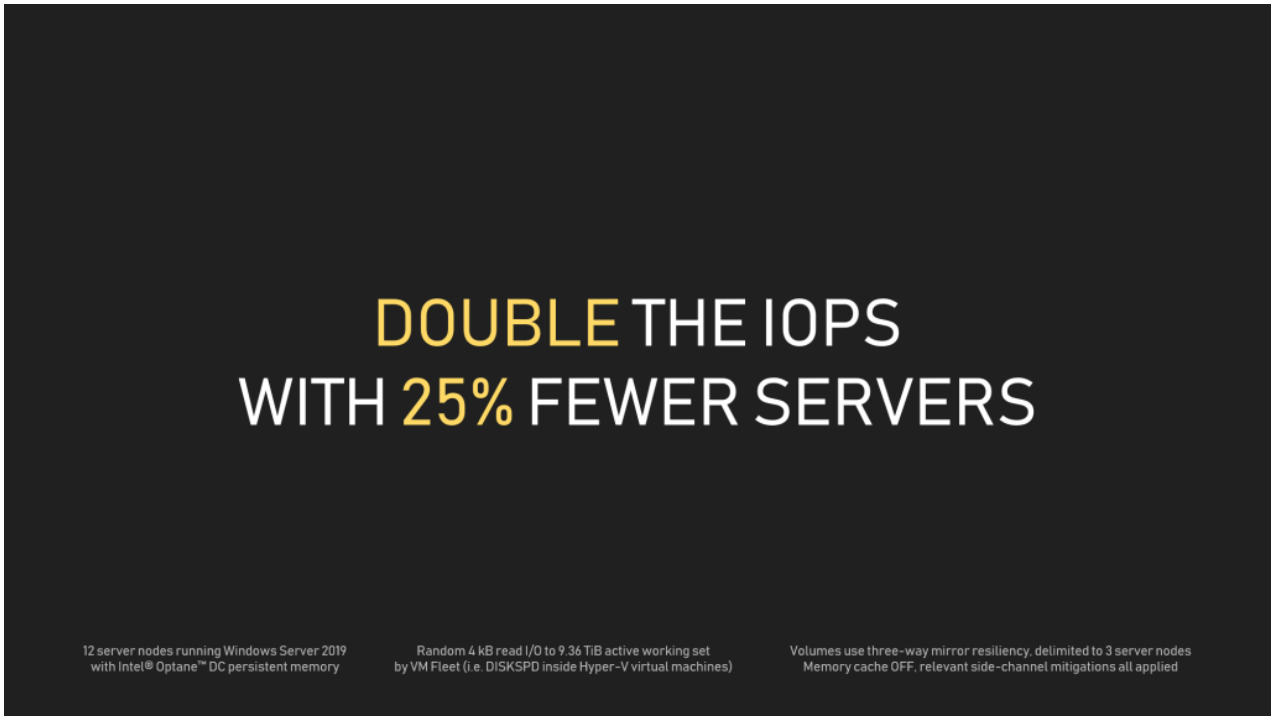
To see some of these benefits, let's look at the following demo from Microsoft Ignite 2018.


Any storage system that provides fault tolerance necessarily makes distributed copies of writes. Such operations must traverse the network and amplify backend write traffic. For this reason, the absolute largest IOPS benchmark numbers are typically achieved by measuring reads only, especially if the storage system has common-sense optimizations to read from the local copy whenever possible. Storage Spaces Direct is optimized to do so.

**When measured by using only read operations, the cluster delivers 13,798,674 IOPS.**


If you watch the video closely, you'll notice that what's even more jaw-dropping is the latency. Even at over 13.7 M IOPS, the file system in Windows is reporting latency that's consistently less than 40 µs! (That's the symbol for microseconds, one-millionth of a second.) This speed is an order of magnitude faster than what typical all-flash vendors proudly advertise today.

Together, Storage Spaces Direct in Windows Server 2019 and Intel® Optane™ DC persistent memory deliver breakthrough performance. This industry-leading HCI benchmark of over 13.7M IOPS, accompanied by predictable and extremely low latency, is more than double our previous industry-leading benchmark of 6.7M IOPS. What's more, this time we needed only 12 server nodes—25 percent fewer than two years ago.




The test hardware was a 12-server cluster that was configured to use three-way mirroring and delimited ReFS volumes, **12** x Intel® S2600WFT, **384 GiB** memory, 2 x 28-core "CascadeLake," **1.5 TB** Intel® Optane™ DC persistent memory as cache, **32 TB** NVMe (4 x 8 TB Intel® DC P4510) as capacity, **2** x Mellanox ConnectX-4 25 Gbps.

The following table shows the full performance numbers.

| BENCHMARK | PERFORMANCE |
| --- | --- |
| 4K 100% random read | 13.8 million IOPS |
| 4K 90/10% random read/write | 9.45 million IOPS |
| 2 MB sequential read | 549 GB/s throughput |

### Supported hardware

The following table shows supported persistent memory hardware for Windows Server 2019 and Windows Server 2016.

| PERSISTENT MEMORY TECHNOLOGY | WINDOWS SERVER 2016 | WINDOWS SERVER 2019 |
| --- | --- | --- |
| **NVDIMM-N** in persistent mode | Supported | Supported |
| **Intel Optane™ DC Persistent Memory** in App Direct Mode | Not Supported | Supported |
| **Intel Optane™ DC Persistent Memory** in Memory Mode | Supported | Supported |

> **NOTE**
>
> Intel Optane supports both *Memory* (volatile) and *App Direct* (persistent) modes.

> **NOTE**
>
> When you restart a system that has multiple Intel® Optane™ PMem modules in App Direct mode that are divided into multiple namespaces, you might lose access to some or all of the related logical storage disks. This issue occurs on Windows Server 2019 versions that are older than version 1903.
>
> This loss of access occurs because a PMem module is untrained or otherwise fails when the system starts. In such a case, all the storage namespaces on any PMem module on the system fail, including namespaces that do not physically map to the failed module.
>
> To restore access to all the namespaces, replace the failed module.
>
> If a module fails on Windows Server 2019 version 1903 or newer versions, you lose access to only namespaces that physically map to the affected module. Other namespaces are not affected.

Now, let's dive into how you configure persistent memory.

## Interleaved sets

### Understanding interleaved sets

Recall that an NVDIMM resides in a standard DIMM (memory) slot, which puts data closer to the processor. This configuration reduces latency and improves fetch performance. To further increase throughput, two or more NVDIMMs create an n-way interleaved set to stripe read/write operations. The most common configurations are two-way or four-way interleaving. An interleaved set also makes multiple persistent memory devices appear as a single logical disk to Windows Server. You can use the Windows PowerShell **get-PmemDisk** cmdlet to review the configuration of such logical disks, as follows:

```
Get-PmemDisk

DiskNumber Size   HealthStatus AtomicityType CanBeRemoved PhysicalDeviceIds UnsafeShutdownCount
---------- ----   ------------ ------------- ------------ ----------------- -------------------
2          252 GB Healthy      None          True         {20, 120}         0
3          252 GB Healthy      None          True         {1020, 1120}      0
```

We can see that the logical PMem disk #2 uses the physical devices Id20 and Id120, and logical PMem disk #3 uses the physical devices Id1020 and Id1120.

To retrieve further information about the interleaved set that a logical drive uses, run the **Get-PmemPhysicalDevice** cmdlet:

```
(Get-PmemDisk)[0] | Get-PmemPhysicalDevice

DeviceId DeviceType           HealthStatus OperationalStatus PhysicalLocation FirmwareRevision Persistent
memory size Volatile memory size
-------- ----------           ------------ ----------------- ---------------- ---------------- ---------------
-------- --------------------
20       Intel INVDIMM device Healthy      {Ok}              CPU1_DIMM_C1     102005310        126 GB
0 GB
120      Intel INVDIMM device Healthy      {Ok}              CPU1_DIMM_F1     102005310        126 GB
0 GB
```

**Configuring interleaved sets**

To configure an interleaved set, start by reviewing all the persistent memory regions that are not assigned to a logical PMem disk on the system. To do this, run the following PowerShell cmdlet:

```
Get-PmemUnusedRegion

RegionId TotalSizeInBytes DeviceId
-------- ---------------- --------
       1     270582939648 {20, 120}
       3     270582939648 {1020, 1120}
```

To see all the PMem device information in the system, including device type, location, health and operational status, and so on, run the following cmdlet on the local server:

```
Get-PmemPhysicalDevice

DeviceId DeviceType           HealthStatus OperationalStatus PhysicalLocation FirmwareRevision Persistent
memory size Volatile

memory size
-------- ----------           ------------ ----------------- ---------------- ---------------- ---------------
-------- --------------
1020     Intel INVDIMM device Healthy      {Ok}              CPU2_DIMM_C1     102005310        126 GB
0 GB
1120     Intel INVDIMM device Healthy      {Ok}              CPU2_DIMM_F1     102005310        126 GB
0 GB
120      Intel INVDIMM device Healthy      {Ok}              CPU1_DIMM_F1     102005310        126 GB
0 GB
20       Intel INVDIMM device Healthy      {Ok}              CPU1_DIMM_C1     102005310        126 GB
0 GB
```

Because we have an available unused PMem region, we can create new persistent memory disks. We can use the unused region to create multiple persistent memory disks by running the following cmdlets:

```
Get-PmemUnusedRegion | New-PmemDisk
Creating new persistent memory disk. This may take a few moments.
```

After this is done, we can see the results by running:

```
Get-PmemDisk

DiskNumber Size   HealthStatus AtomicityType CanBeRemoved PhysicalDeviceIds UnsafeShutdownCount
---------- ----   ------------ ------------- ------------ ----------------- -------------------
2          252 GB Healthy      None          True         {20, 120}         0
3          252 GB Healthy      None          True         {1020, 1120}      0
```

It is worth noting that we can run **Get-PhysicalDisk | Where MediaType -Eq SCM** instead of **Get-PmemDisk** to get the same results. The newly-created PMem disk corresponds one-to-one with drives that appear in PowerShell and in Windows Admin Center.

### Using persistent memory for cache or capacity

Storage Spaces Direct on Windows Server 2019 supports using persistent memory as either a cache or a capacity drive. For more information about how to set up cache and capacity drives, see Understanding the cache in Storage Spaces Direct.

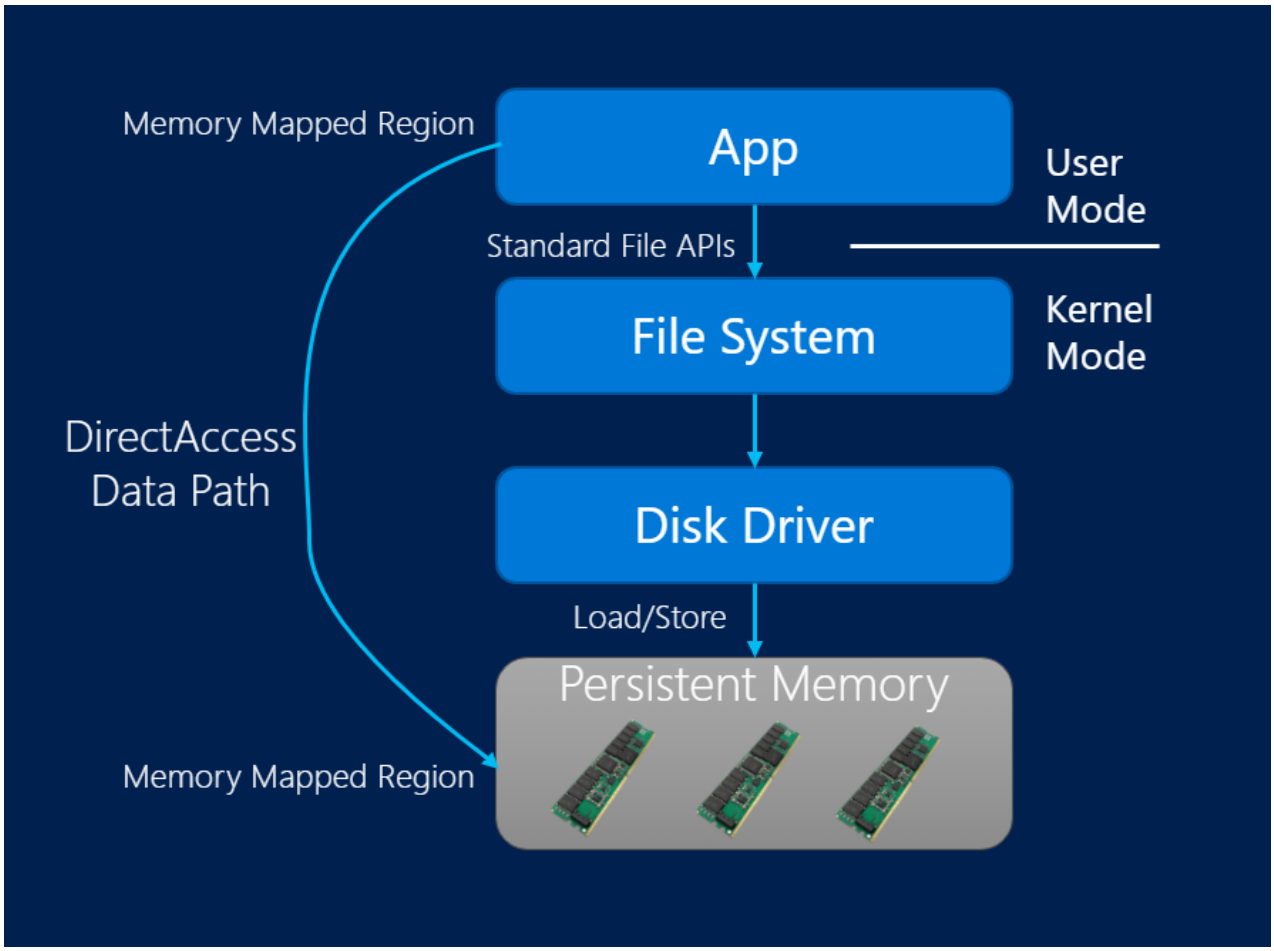
## Creating a DAX volume

### Understanding DAX

There are two methods for accessing persistent memory. They are:

1. **Direct access (DAX)**, which operates like memory to get the lowest latency. The app directly modifies the persistent memory, bypassing the stack. Note that you can only use DAX in combination with NTFS.
2. **Block access**, which operates like storage for app compatibility. In this configuraion, the data flows through the stack. You can use this configuration in combination with NTFS and ReFS.

The following figure shows an example of a DAX configuration:




**Configuring DAX**

We have to use PowerShell cmdlets to create a DAX volume on a persistent memory disk. By using the **-IsDax** switch, we can format a volume to be DAX-enabled.

```
Format-Volume -IsDax:$true
```

The following code snippet helps you create a DAX volume on a persistent memory disk.

```
# Here we use the first pmem disk to create the volume as an example
$disk = (Get-PmemDisk)[0] | Get-PhysicalDisk | Get-Disk
# Initialize the disk to GPT if it is not initialized
If ($disk.partitionstyle -eq "RAW") {$disk | Initialize-Disk -PartitionStyle GPT}
# Create a partition with drive letter 'S' (can use any available drive letter)
$disk | New-Partition -DriveLetter S -UseMaximumSize


   DiskPath: \\?
\scmld#ven_8980&dev_097a&subsys_89804151&rev_0018#3&1b1819f6&0&03018089fb63494db728d8418b3cbbf549997891#
{53f56307-b6
bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
2                S           16777216                                 251.98 GB Basic

# Format the volume with drive letter 'S' to DAX Volume
Format-Volume -FileSystem NTFS -IsDax:$true -DriveLetter S

DriveLetter FriendlyName FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining      Size
----------- ------------ -------------- --------- ------------ ----------------- -------------      ----
S                        NTFS           Fixed     Healthy      OK                    251.91 GB 251.98 GB

# Verify the volume is DAX enabled
Get-Partition -DriveLetter S | fl


UniqueId             : {00000000-0000-0000-0000-
000100000000}SCMLD\VEN_8980&DEV_097A&SUBSYS_89804151&REV_0018\3&1B1819F6&0&03018089F
                       B63494DB728D8418B3CBBF549997891:WIN-8KGI228ULGA
AccessPaths          : {S:\, \\?\Volume{cf468ffa-ae17-4139-a575-717547d4df09}\}
DiskNumber           : 2
DiskPath             : \\?
\scmld#ven_8980&dev_097a&subsys_89804151&rev_0018#3&1b1819f6&0&03018089fb63494db728d8418b3cbbf549997891#{5
                       3f56307-b6bf-11d0-94f2-00a0c91efb8b}
DriveLetter          : S
Guid                 : {cf468ffa-ae17-4139-a575-717547d4df09}
IsActive             : False
IsBoot               : False
IsHidden             : False
IsOffline            : False
IsReadOnly           : False
IsShadowCopy         : False
IsDAX                : True                  # <- True: DAX enabled
IsSystem             : False
NoDefaultDriveLetter : False
Offset               : 16777216
OperationalStatus    : Online
PartitionNumber      : 2
Size                 : 251.98 GB
Type                 : Basic
```

## Monitoring health

When you use persistent memory, there are a few differences in the monitoring experience:

- Persistent memory doesn't create Physical Disk performance counters, so you won't see it appear on charts in Windows Admin Center.
- Persistent memory doesn't create Storport 505 data, so you won't get proactive outlier detection.

Apart from that, the monitoring experience is the same as for any other physical disk. You can query for the health of a persistent memory disk by running the following cmdlets:

```
Get-PmemDisk

DiskNumber Size   HealthStatus AtomicityType CanBeRemoved PhysicalDeviceIds UnsafeShutdownCount
---------- ----   ------------ ------------- ------------ ----------------- -------------------
2          252 GB Unhealthy    None          True         {20, 120}         2
3          252 GB Healthy      None          True         {1020, 1120}      0

Get-PmemDisk | Get-PhysicalDisk | select SerialNumber, HealthStatus, OperationalStatus, OperationalDetails

SerialNumber               HealthStatus OperationalStatus  OperationalDetails
------------               ------------ ------------------ ------------------
802c-01-1602-117cb5fc      Healthy      OK
802c-01-1602-117cb64f      Warning      Predictive Failure {Threshold Exceeded,NVDIMM_N Error}
```

**HealthStatus** shows whether the PMem disk is healthy.

The **UnsafeshutdownCount** value tracks the number of shutdowns that may cause data loss on this logical disk. It is the sum of the unsafe shutdown counts of all the underlying PMem devices of this disk. For more information about the health status, use the **Get-PmemPhysicalDevice** cmdlet to find information such as **OperationalStatus**.

```
Get-PmemPhysicalDevice

DeviceId DeviceType           HealthStatus OperationalStatus PhysicalLocation FirmwareRevision Persistent
memory size Volatile memory size
-------- ----------           ------------ ----------------- ---------------- ---------------- ---------------
------- --------------------
1020     Intel INVDIMM device Healthy      {Ok}              CPU2_DIMM_C1     102005310        126 GB
0 GB
1120     Intel INVDIMM device Healthy      {Ok}              CPU2_DIMM_F1     102005310        126 GB
0 GB
120      Intel INVDIMM device Healthy      {Ok}              CPU1_DIMM_F1     102005310        126 GB
0 GB
20       Intel INVDIMM device Unhealthy    {HardwareError}   CPU1_DIMM_C1     102005310        126 GB
0 GB
```

This cmdlet shows which persistent memory device is unhealthy. The unhealthy device (**DeviceId** 20) matches the case in the previous example. The **PhysicalLocation** in BIOS can help identify which persistent memory device is in faulty state.

## Replacing persistent memory

This article describes how to view the health status of your persistent memory. If you have to replace a failed module, you have to re-provision the PMem disk (refer to the steps that we outlined previously).

When you troubleshoot, you might have to use **Remove-PmemDisk**. This cmdlet removes a specific persistent memory disk. We can remove all current PMem disks by running the following cmdlets:

```
Get-PmemDisk | Remove-PmemDisk

cmdlet Remove-PmemDisk at command pipeline position 1
Supply values for the following parameters:
DiskNumber: 2

This will remove the persistent memory disk(s) from the system and will result in data loss.
Remove the persistent memory disk(s)?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
Removing the persistent memory disk. This may take a few moments.
```

> **IMPORTANT**
>
> Removing a persistent memory disk causes data loss on that disk.

Another cmdlet you might need is **Initialize-PmemPhysicalDevice**. This cmdlet initializes the label storage areas on the physical persistent memory devices, and can clear corrupted label storage information on the PMem devices.

```
Get-PmemPhysicalDevice | Initialize-PmemPhysicalDevice

This will initialize the label storage area on the physical persistent memory device(s) and will result in
data loss.
Initializes the physical persistent memory device(s)?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
Initializing the physical persistent memory device. This may take a few moments.
Initializing the physical persistent memory device. This may take a few moments.
Initializing the physical persistent memory device. This may take a few moments.
Initializing the physical persistent memory device. This may take a few moments.
```

> **IMPORTANT**
>
> **Initialize-PmemPhysicalDevice** causes data loss in persistent memory. Use it as a last resort to fix persistent memory-related issues.

## Additional References

- Storage Spaces Direct overview
- Storage-class Memory (NVDIMM-N) Health Management in Windows
- Understand the cache

# Manage Hyper-Converged Infrastructure with Windows Admin Center

11/2/2020 • 12 minutes to read • Edit Online

Applies To: Windows Admin Center, Windows Admin Center Preview

## What is Hyper-Converged Infrastructure

Hyper-Converged Infrastructure consolidates software-defined compute, storage, and networking into one cluster to provide high-performance, cost-effective, and easily scalable virtualization. This capability was introduced in Windows Server 2016 with Storage Spaces Direct, Software Defined Networking and Hyper-V.

**TIP**

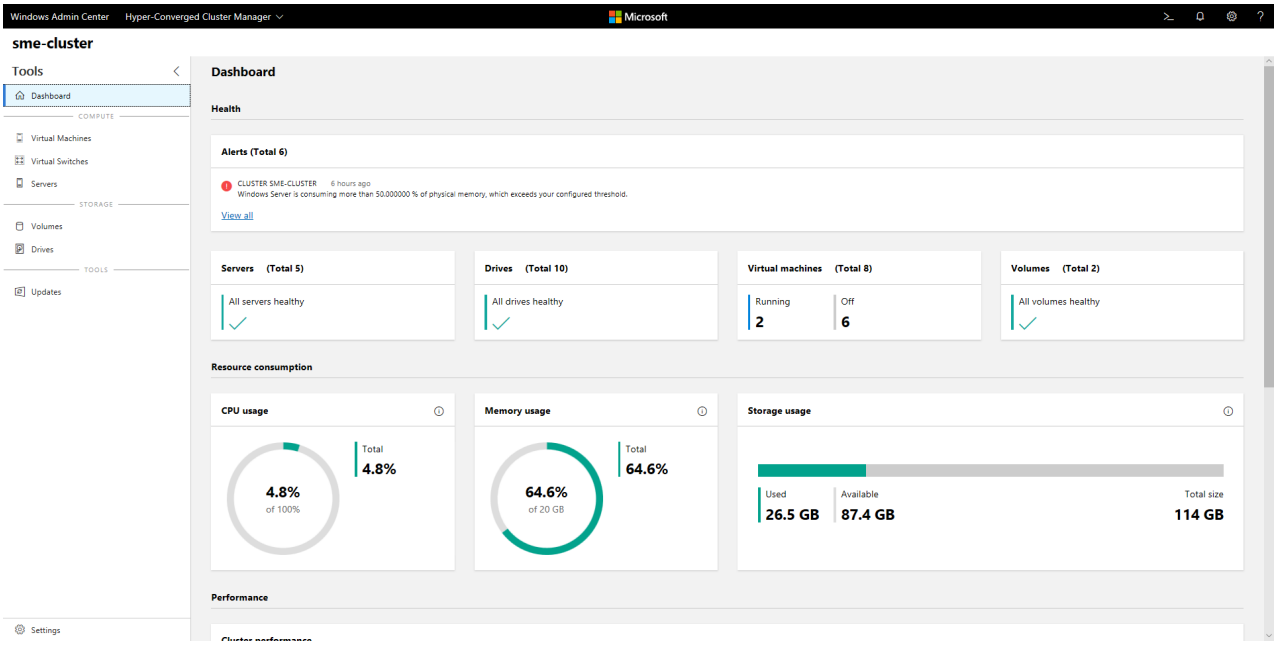
Looking to acquire Hyper-Converged Infrastructure? Microsoft recommends these Windows Server Software-Defined solutions from our partners. They are designed, assembled, and validated against our reference architecture to ensure compatibility and reliability, so you get up and running quickly.

**IMPORTANT**

Some of the features described in this article are only available in Windows Admin Center Preview. How do I get this version?

## What is Windows Admin Center

Windows Admin Center is the next-generation management tool for Windows Server, the successor to traditional "in-box" tools like Server Manager. It's free and can be installed and used without an Internet connection. You can use Windows Admin Center to manage and monitor Hyper-Converged Infrastructure running Windows Server 2016 or Windows Server 2019.




## Key features

Highlights of Windows Admin Center for Hyper-Converged Infrastructure include:

- **Unified single-pane-of-glass for compute, storage, and soon networking.** View your virtual machines, host servers, volumes, drives, and more within one purpose-built, consistent, interconnected experience.
- **Create and manage Storage Spaces and Hyper-V virtual machines.** Radically simple workflows to create, open, resize, and delete volumes; and create, start, connect to, and move virtual machines; and much more.
- **Powerful cluster-wide monitoring.** The dashboard graphs memory and CPU usage, storage capacity, IOPS, throughput, and latency in real-time, across every server in the cluster, with clear alerts when something's not right.
- **Software Defined Networking (SDN) support.** Manage and monitor virtual networks, subnets, connect virtual machines to virtual networks, and monitor SDN infrastructure.

Windows Admin Center for Hyper-Converged Infrastructure is being actively developed by Microsoft. It receives frequent updates that improve existing features and add new features.

## Before you start

To manage your cluster as Hyper-Converged Infrastructure in Windows Admin Center, it needs to be running Windows Server 2016 or Windows Server 2019, and have Hyper-V and Storage Spaces Direct enabled. Optionally, it can also have Software Defined Networking enabled and managed through Windows Admin Center.

> **TIP**
> Windows Admin Center also offers a general-purpose management experience for any cluster supporting any workload, available for Windows Server 2012 and later. If this sounds like a better fit, when you add your cluster to Windows Admin Center, select **Failover Cluster** instead of **Hyper-Converged Cluster**.

### Prepare your Windows Server 2016 cluster for Windows Admin Center

Windows Admin Center for Hyper-Converged Infrastructure depends on management APIs added after Windows Server 2016 was released. Before you can manage your Windows Server 2016 cluster with Windows Admin Center, you'll need to perform these two steps:

1. Verify that every server in the cluster has installed the 2018-05 Cumulative Update for Windows Server 2016 (KB4103723) or later. To download and install this update, go to **Settings** > **Update & Security** > **Windows Update** and select **Check online for updates from Microsoft Update**.
2. Run the following PowerShell cmdlet as Administrator on the cluster:

```
    Add-ClusterResourceType -Name "SDDC Management" -dll "$env:SystemRoot\Cluster\sddcres.dll" -DisplayName
"SDDC Management"
```

> **TIP**
> You only need to run the cmdlet once, on any server in the cluster. You can run it locally in Windows PowerShell or use Credential Security Service Provider (CredSSP) to run it remotely. Depending on your configuration, you may not be able to run this cmdlet from within Windows Admin Center.

### Prepare your Windows Server 2019 cluster for Windows Admin Center

If your cluster runs Windows Server 2019, the steps above are not necessary. Just add the cluster to Windows Admin Center as described in the next section and you're good to go!

### Configure Software Defined Networking (Optional)

You can configure your Hyper-Converged Infrastructure running Windows Server 2016 or 2019 to use Software Defined Networking (SDN) with the following steps:

1. Prepare the VHD of the OS which is the same OS you installed on the hyper-converged infrastructure hosts. This VHD will be used for all NC/SLB/GW VMs.
2. Download all the folder and files under SDN Express from https://github.com/Microsoft/SDN/tree/master/SDNExpress.
3. Prepare a different VM using the deployment console. This VM should be able to access the SDN hosts. Also, the VM should be have the RSAT Hyper-V tool installed.
4. Copy everything you downloaded for SDN Express to the deployment console VM. And share this **SDNExpress** folder. Make sure every host can access the **SDNExpress** shared folder, as defined in the configuration file line 8:

   ```
   \\$env:Computername\SDNExpress
   ```

5. Copy the VHD of the OS to the **images** folder under the **SDNExpress** folder on the deployment console VM.
6. Modify the SDN Express configuration with your environment setup. Finish the following two steps after you modify the SDN Express configuration based on your environment information.
7. Run PowerShell with Admin privilege to deploy SDN:

```
.\SDNExpress.ps1 -ConfigurationDataFile .\your_fabricconfig.PSD1 -verbose
```

The deployment will take around 30 – 45 minutes.

# Get started

Once your Hyper-Converged Infrastructure is deployed, you can manage it using Windows Admin Center.

### Install Windows Admin Center

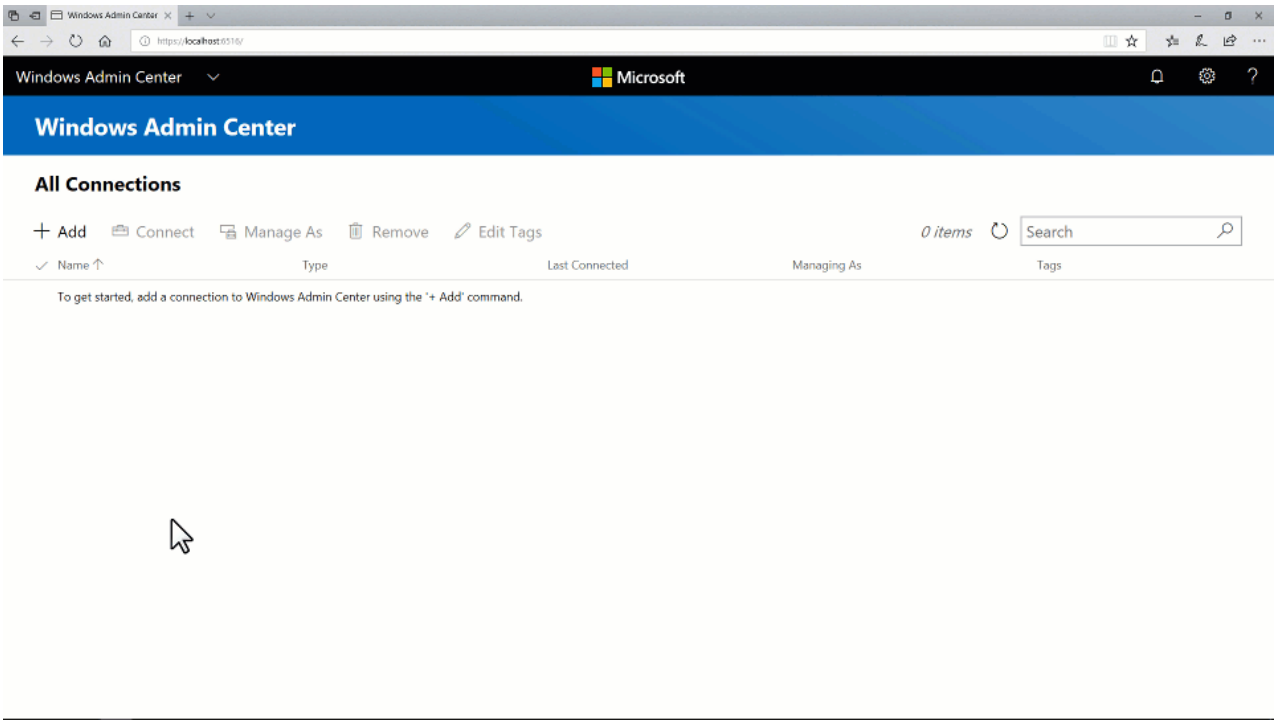
If you haven't already, download and install Windows Admin Center. The fastest way to get up and running is to install it on your Windows 10 computer and manage your servers remotely. This takes less than five minutes. Download now or learn more about other installation options.

### Add Hyper-Converged Cluster

To add your cluster to Windows Admin Center:

1. Click **+ Add** under All Connections.
2. Choose to add a **Hyper-Converged Cluster Connection**.
3. Type the name of the cluster and, if prompted, the credentials to use.
4. Click **Add** to finish.

The cluster will be added to your connections list. Click it to launch the Dashboard.



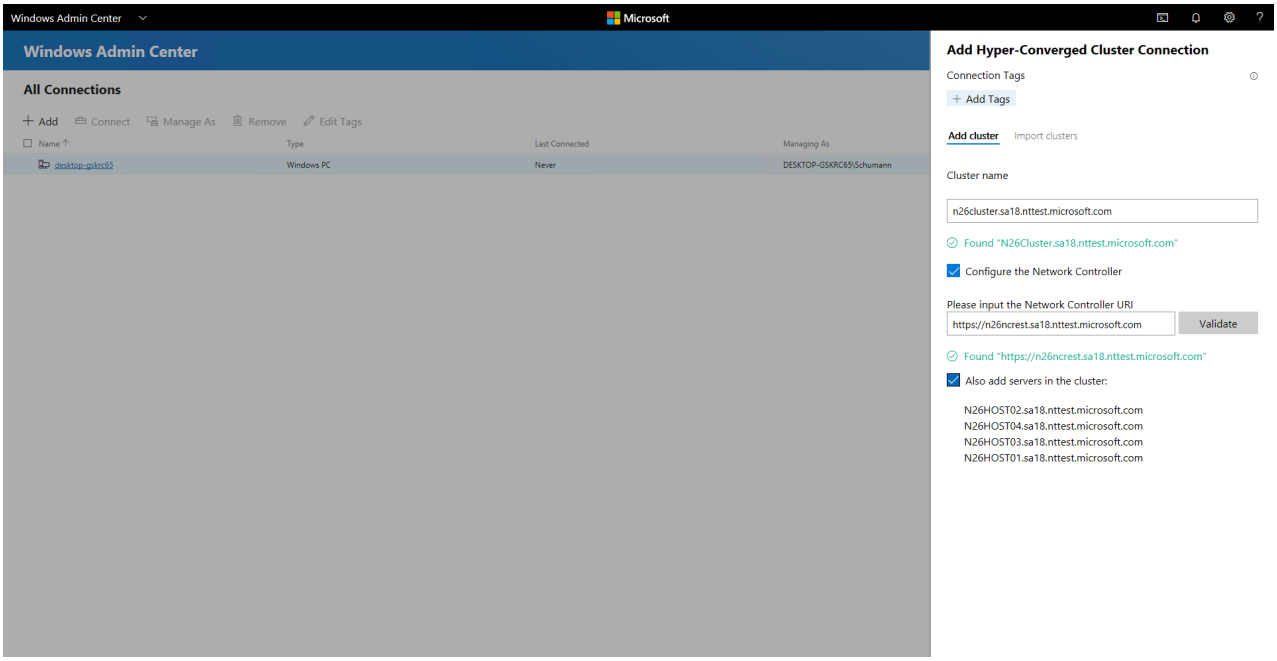

---

### Add SDN-enabled Hyper-Converged Cluster (Windows Admin Center Preview)

The latest Windows Admin Center Preview supports Software Defined Networking management for Hyper-Converged Infrastructure. By adding a Network Controller REST URI to your Hyper-Converged cluster connection, you can use Hyper-converged Cluster Manager to manage your SDN resources and monitor SDN infrastructure.

1. Click **+ Add** under All Connections.
2. Choose to add a **Hyper-Converged Cluster Connection**.
3. Type the name of the cluster and, if prompted, the credentials to use.
4. Check **Configure the Network Controller** to continue.
5. Enter the **Network Controller URI** and click **Validate**.
6. Click **Add** to finish.

The cluster will be added to your connections list. Click it to launch the Dashboard.



**IMPORTANT**

SDN environments with Kerberos authentication for Northbound communication are currently not supported.

# Frequently asked questions

**Are there differences between managing Windows Server 2016 and Windows Server 2019?**

Yes. Windows Admin Center for Hyper-Converged Infrastructure receives frequent updates that improve the experience for both Windows Server 2016 and Windows Server 2019. However, certain new features are only available for Windows Server 2019 – for example, the toggle switch for deduplication and compression.

**Can I use Windows Admin Center to manage Storage Spaces Direct for other use cases (not hyper-converged), such as converged Scale-Out File Server (SoFS) or Microsoft SQL Server?**

Windows Admin Center for Hyper-Converged Infrastructure does not provide management or monitoring options specifically for other use cases of Storage Spaces Direct – for example, it can't create file shares. However, the Dashboard and core features, such as creating volumes or replacing drives, work for any Storage Spaces Direct cluster.

**What's the difference between a Failover Cluster and a Hyper-Converged Cluster?**

In general, the term "hyper-converged" refers to running Hyper-V and Storage Spaces Direct on the same clustered servers to virtualize compute and storage resources. In the context of Windows Admin Center, when you click **+ Add** from the connections list, you can choose between adding a **Failover Cluster connection** or a **Hyper-Converged Cluster connection**:

- The **Failover Cluster connection** is the successor to the Failover Cluster Manager desktop app. It provides a familiar, general-purpose management experience for any cluster supporting any workload, including Microsoft SQL Server. It is available for Windows Server 2012 and later.
- The **Hyper-Converged Cluster connection** is an all-new experience tailored for Storage Spaces Direct and Hyper-V. It features the Dashboard and emphasizes charts and alerts for monitoring. It is available for Windows Server 2016 and Windows Server 2019.

**Why do I need the latest cumulative update for Windows Server 2016?**

Windows Admin Center for Hyper-Converged Infrastructure depends on management APIs developed since Windows Server 2016 was released. These APIs are added in the 2018-05 Cumulative Update for Windows Server 2016 (KB4103723), available as of May 8, 2018.

**How much does it cost to use Windows Admin Center?**

Windows Admin Center has no additional cost beyond Windows.

You can use Windows Admin Center (available as a separate download) with valid licenses of Windows Server or Windows 10 at no additional cost - it's licensed under a Windows Supplemental EULA.

**Does Windows Admin Center require System Center?**

No.

**Does it require an Internet connection?**

No.

Although Windows Admin Center offers powerful and convenient integration with the Microsoft Azure cloud, the core management and monitoring experience for Hyper-Converged Infrastructure is completely on-premises. It can be installed and used without an Internet connection.

# Things to try

If you're just getting started, here are some quick tutorials to help you learn how Windows Admin Center for Hyper-Converged Infrastructure is organized and works. Please exercise good judgement and be careful with production environments. These videos were recorded with Windows Admin Center version 1804 and an Insider Preview build of Windows Server 2019.

**Manage Storage Spaces Direct volumes**

- (0:37) How to create a three-way mirror volume
- (1:17) How to create a mirror-accelerated parity volume
- (1:02) How to open a volume and add files
- (0:51) How to turn on deduplication and compression
- (0:47) How to expand a volume
- (0:26) How to delete a volume

| | |
|---|---|
| **Create volume, three-way mirror** https://www.youtube-nocookie.com/embed/o66etKq70N8 | **Create volume, mirror-accelerated parity** https://www.youtube-nocookie.com/embed/R72QHudqWpE |
| **Open volume and add files** https://www.youtube-nocookie.com/embed/j59z7ulohs4 | **Turn on deduplication and compression** https://www.youtube-nocookie.com/embed/PRibTacyKko |
| **Expand volume** https://www.youtube-nocookie.com/embed/hqyBzipBoTI | **Delete volume** https://www.youtube-nocookie.com/embed/DbjF8r2F6Jo |

**Create a new virtual machine**

1. Click the **Virtual Machines** tool from the left side navigation pane.
2. At the top of the Virtual Machines tool, choose the **Inventory** tab, then click **New** to create a new virtual machine.
3. Enter the virtual machine name and choose between generation 1 and 2 virtual machines.
4. Uou can then choose which host to initially create the virtual machine on or use the recommended host.
5. Choose a path for the virtual machine files. Choose a volume from the dropdown list or click **Browse** to choose a folder using the folder picker. The virtual machine configuration files and virtual hard disk file will be saved in a single folder under the `\Hyper-V\[virtual machine name]` path of the selected volume or path.
6. Choose the number of virtual processors, whether you want nested virtualization enabled, configure memory settings, network adapters, virtual hard disks and choose whether you want to install an operating system from an .iso image file or from the network.
7. Click **Create** to create the virtual machine.
8. Once the virtual machine is created and appears in the virtual machine list, you can start the virtual machine.
9. Once the virtual machine is started, you can connect to the virtual machine's console via VMConnect to install the operating system. Select the virtual machine from the list, click **More** > **Connect** to download the .rdp file. Open the .rdp file in the Remote Desktop Connection app. Since this is connecting to the virtual machine's console, you will need to enter the Hyper-V host's admin credentials.

Learn more about virtual machine management with Windows Admin Center.

**Pause and safely restart a server**

1. From the **Dashboard**, select **Servers** from the navigation on the left side or by clicking the **VIEW SERVERS** > link on the tile in the lower right corner of the Dashboard.
2. At the top, switch from **Summary** to the **Inventory** tab.
3. Select a server by clicking its name to open the **Server** detail page.
4. Click **Pause server for maintenance**. If it's safe to proceed, this will move virtual machines to other servers in the cluster. The server will have status Draining while this happens. If you want, you can watch the virtual machines move on the **Virtual machines** > **Inventory** page, where their host server is shown clearly in the

grid. When all virtual machines have moved, the server status will be **Paused**.

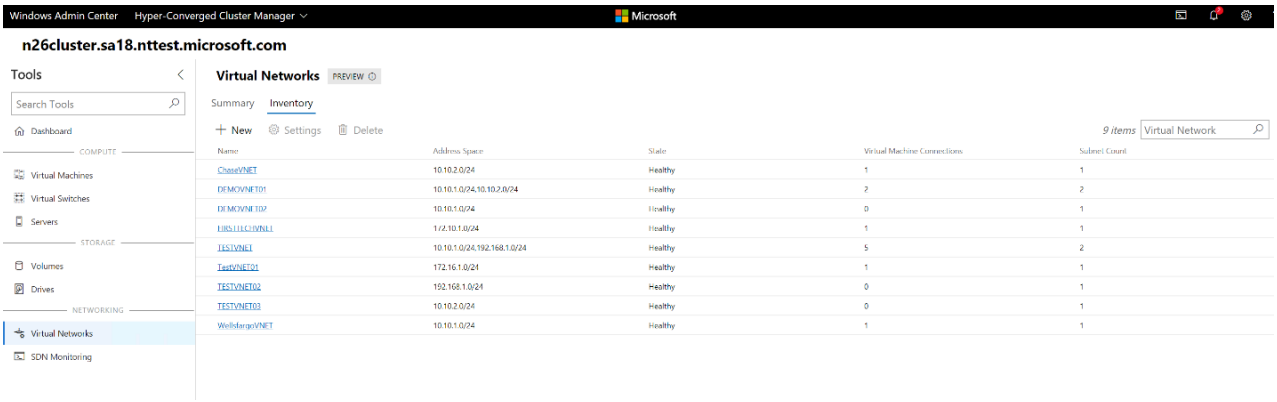
5. Click **Manage server** to access all the per-server management tools in Windows Admin Center.
6. Click **Restart**, then **Yes**. You'll be kicked back to the connections list.
7. Back on the **Dashboard**, the server is colored red while it's down.
8. Once it's back up, navigate again the **Server** page and click **Resume server from maintenance** to set the server status back to simply Up. In time, virtual machines will move back – no user action is required.

### Replace a failed drive

1. When a drive fails, an alert appears in the upper left **Alerts** area of the **Dashboard**.
2. You can also select **Drives** from the navigation on the left side or click the **VIEW DRIVES >** link on the tile in the lower right corner to browse drives and see their status for yourself. In the **Inventory** tab, the grid supports sorting, grouping, and keyword search.
3. From the **Dashboard**, click the alert to see details, like the drive's physical location.
4. To learn more, click the **Go to drive** shortcut to the **Drive** detail page.
5. If your hardware supports it, you can click **Turn light on/off** to control the drive's indicator light.
6. Storage Spaces Direct automatically retires and evacuates failed drives. When this has happened, the drive status is Retired, and its storage capacity bar is empty.
7. Remove the failed drive and insert its replacement.
8. In **Drives > Inventory**, the new drive will appear. In time, the alert will clear, volumes will repair back to OK status, and storage will rebalance onto the new drive – no user action is required.

### Manage virtual networks (SDN-enabled HCI clusters using Windows Admin Center Preview)

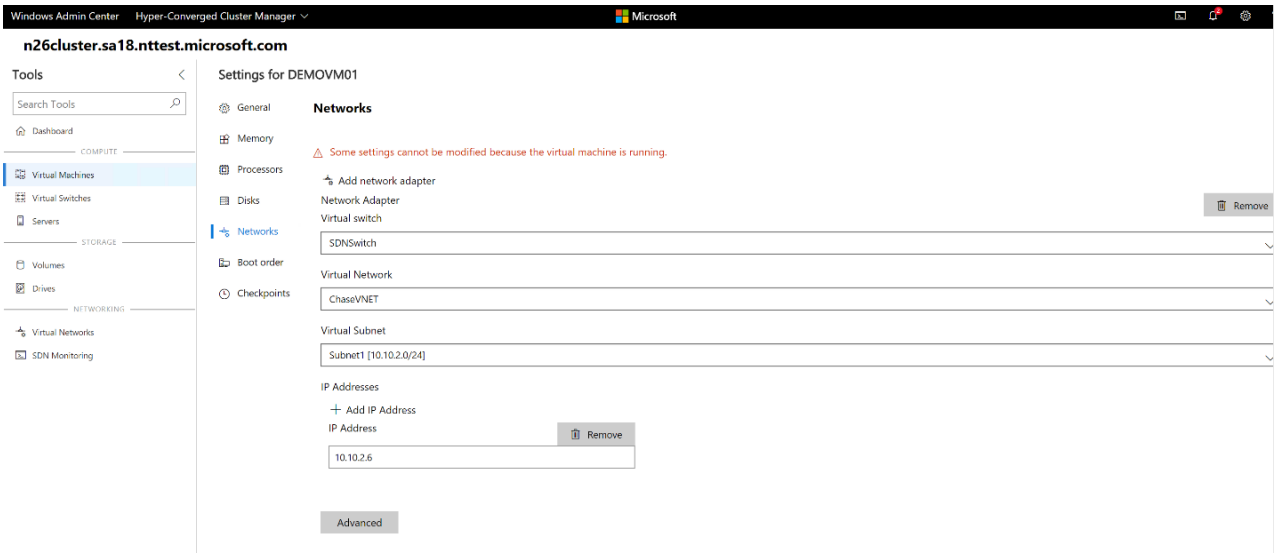
1. Select **Virtual Networks** from the navigation on the left side.
2. Click **New** to create a new virtual network and subnets, or choose an existing virtual network and click **Settings** to modify its configuration.
3. Click an existing virtual network to view VM connections to the virtual network subnets and access control lists applied to virtual network subnets.




### Connect a virtual machine to a virtual network (SDN-enabled HCI clusters using Windows Admin Center Preview)

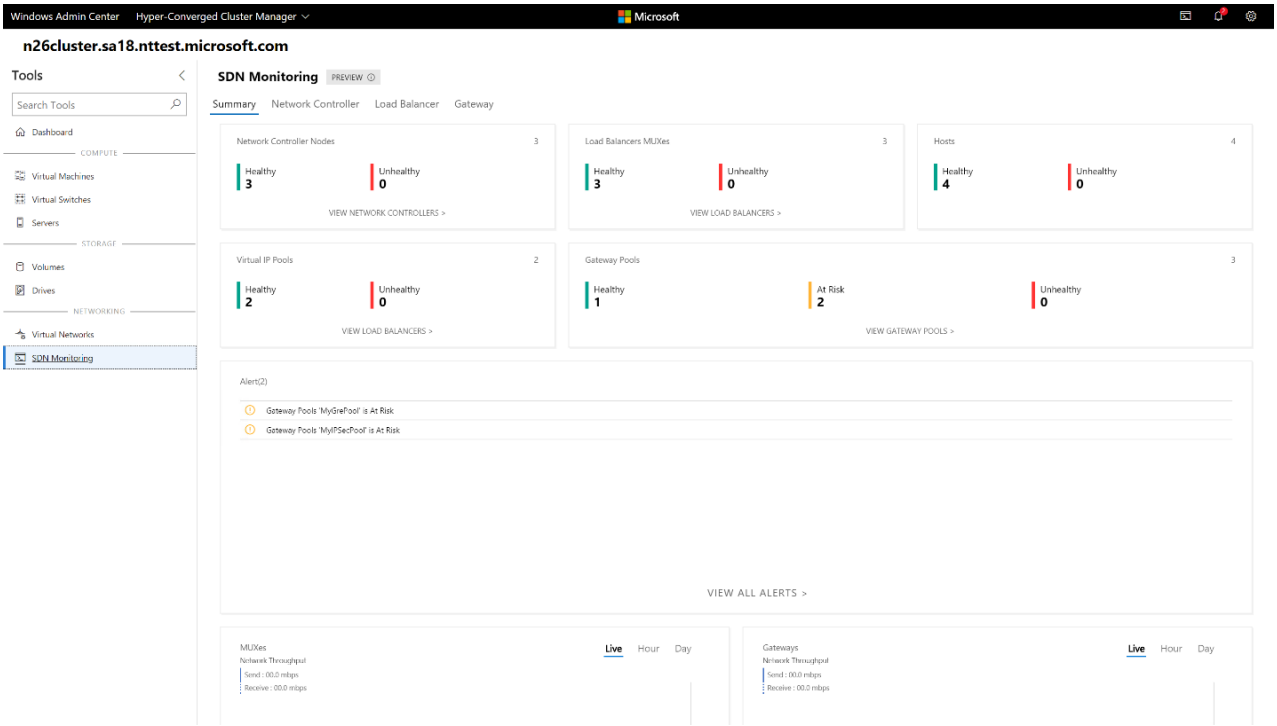
1. Select **Virtual Machines** from the navigation on the left side.
2. Choose an existing virtual machine > Click **Settings** > Open the **Networks** tab in **Settings**.
3. Configure the **Virtual Network** and **Virtual Subnet** fields to connect the virtual machine to a virtual network.

You can also configure the virtual network when creating a virtual machine.




**Monitor Software Defined Networking infrastructure (SDN-enabled HCI clusters using Windows Admin Center Preview)**

1. Select **SDN Monitoring** from the navigation on the left side.
2. View detailed information about the health of Network Controller, Software Load Balancer, Virtual Gateway and monitor your Virtual Gateway Pool, Public and Private IP Pool usage and SDN host status.




# Give us feedback

It's all about your feedback! The most important benefit of frequent updates is to hear what's working and what needs to be improved. Here are some ways to let us know what you're thinking:

- Submit and vote for feature requests on UserVoice
- Join the Windows Admin Center forum on Microsoft Tech Community
- Tweet to `@servermgmt`

### Additional References

- Windows Admin Center
- Storage Spaces Direct
- Hyper-V

- Software Defined Networking

# Adding servers or drives to Storage Spaces Direct

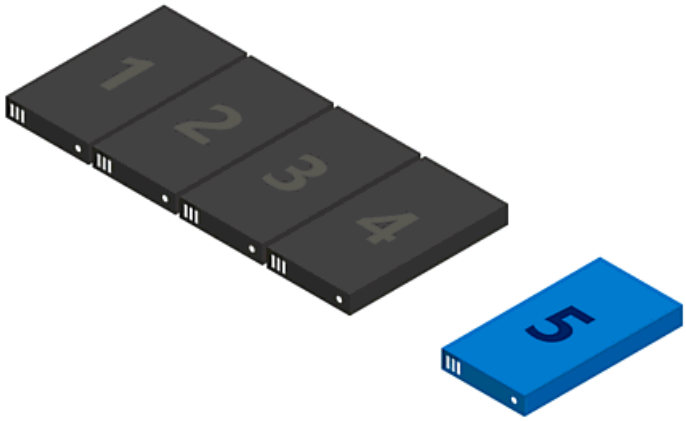
12/16/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic describes how to add servers or drives to Storage Spaces Direct.

## Adding servers

Adding servers, often called scaling out, adds storage capacity and can improve storage performance and unlock better storage efficiency. If your deployment is hyper-converged, adding servers also provides more compute resources for your workload.




Typical deployments are simple to scale out by adding servers. There are just two steps:

1. Run the cluster validation wizard using the Failover Cluster snap-in or with the **Test-Cluster** cmdlet in PowerShell (run as Administrator). Include the new server *<NewNode>* you wish to add.

   ```
   Test-Cluster -Node <Node>, <Node>, <Node>, <NewNode> -Include "Storage Spaces Direct", Inventory,
   Network, "System Configuration"
   ```

   This confirms that the new server is running Windows Server 2016 Datacenter Edition, has joined the same Active Directory Domain Services domain as the existing servers, has all the required roles and features, and has networking properly configured.

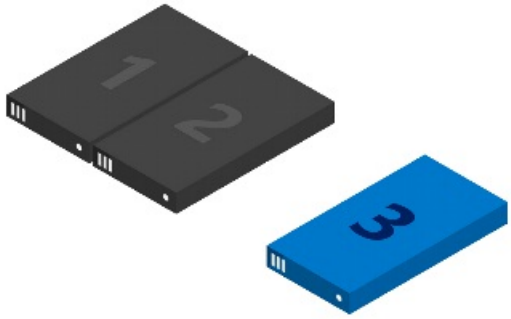
   > **IMPORTANT**
   > If you are re-using drives that contain old data or metadata you no longer need, clear them using **Disk Management** or the **Reset-PhysicalDisk** cmdlet. If old data or metadata is detected, the drives aren't pooled.

2. Run the following cmdlet on the cluster to finish adding the server:

```
Add-ClusterNode -Name NewNode
```

> **NOTE**
> Automatic pooling depends on you having only one pool. If you've circumvented the standard configuration to create multiple pools, you will need to add new drives to your preferred pool yourself using **Add-PhysicalDisk**.

### From 2 to 3 servers: unlocking three-way mirroring




With two servers, you can only create two-way mirrored volumes (compare with distributed RAID-1). With three servers, you can create three-way mirrored volumes for better fault tolerance. We recommend using three-way mirroring whenever possible.

Two-way mirrored volumes cannot be upgraded in-place to three-way mirroring. Instead, you can create a new volume and migrate (copy, such as by using Storage Replica) your data to it, and then remove the old volume.

To begin creating three-way mirrored volumes, you have several good options. You can use whichever you prefer.

**Option 1**

Specify **PhysicalDiskRedundancy = 2** on each new volume upon creation.

```
New-Volume -FriendlyName <Name> -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size <Size> -
PhysicalDiskRedundancy 2
```

**Option 2**

Instead, you can set **PhysicalDiskRedundancyDefault = 2** on the pool's **ResiliencySetting** object named **Mirror**. Then, any new mirrored volumes will automatically use *three-way* mirroring even if you don't specify it.

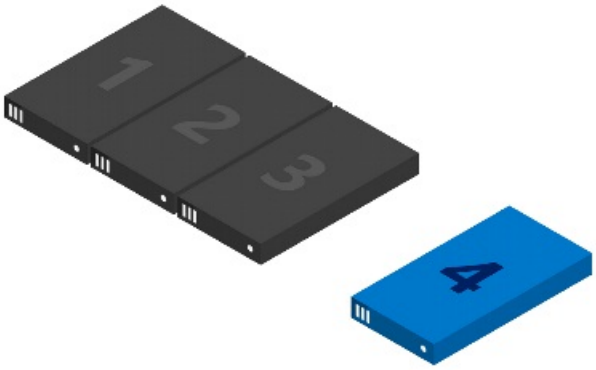
```
Get-StoragePool S2D* | Get-ResiliencySetting -Name Mirror | Set-ResiliencySetting -
PhysicalDiskRedundancyDefault 2

New-Volume -FriendlyName <Name> -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size <Size>
```

**Option 3**

Set **PhysicalDiskRedundancy = 2** on the **StorageTier** template called *Capacity*, and then create volumes by referencing the tier.

```
Set-StorageTier -FriendlyName Capacity -PhysicalDiskRedundancy 2

New-Volume -FriendlyName <Name> -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -StorageTierFriendlyNames
Capacity -StorageTierSizes <Size>
```

### From 3 to 4 servers: unlocking dual parity




With four servers, you can use dual parity, also commonly called erasure coding (compare to distributed RAID-6). This provides the same fault tolerance as three-way mirroring, but with better storage efficiency. To learn more, see Fault tolerance and storage efficiency.

If you're coming from a smaller deployment, you have several good options to begin creating dual parity volumes. You can use whichever you prefer.

**Option 1**

Specify **PhysicalDiskRedundancy = 2** and **ResiliencySettingName = Parity** on each new volume upon creation.

```
New-Volume -FriendlyName <Name> -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size <Size> -
PhysicalDiskRedundancy 2 -ResiliencySettingName Parity
```

**Option 2**

Set **PhysicalDiskRedundancy = 2** on the pool's **ResiliencySetting** object named **Parity**. Then, any new parity volumes will automatically use *dual* parity even if you don't specify it

```
Get-StoragePool S2D* | Get-ResiliencySetting -Name Parity | Set-ResiliencySetting -
PhysicalDiskRedundancyDefault 2

New-Volume -FriendlyName <Name> -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -Size <Size> -
ResiliencySettingName Parity
```

With four servers, you can also begin using mirror-accelerated parity, where an individual volume is part mirror and part parity.

For this, you will need to update your **StorageTier** templates to have both *Performance* and *Capacity* tiers, as they would be created if you had first run **Enable-ClusterS2D** at four servers. Specifically, both tiers should have the **MediaType** of your capacity devices (such as SSD or HDD) and **PhysicalDiskRedundancy = 2**. The *Performance* tier should be **ResiliencySettingName = Mirror**, and the *Capacity* tier should be **ResiliencySettingName = Parity**.

**Option 3**

You may find it easiest to simply remove the existing tier template and create the two new ones. This will not affect any pre-existing volumes which were created by referring the tier template: it's just a template.

```
Remove-StorageTier -FriendlyName Capacity

New-StorageTier -StoragePoolFriendlyName S2D* -MediaType HDD -PhysicalDiskRedundancy 2 -ResiliencySettingName
Mirror -FriendlyName Performance
New-StorageTier -StoragePoolFriendlyName S2D* -MediaType HDD -PhysicalDiskRedundancy 2 -ResiliencySettingName
Parity -FriendlyName Capacity
```

That's it! You are now ready to create mirror-accelerated parity volumes by referencing these tier templates.

**Example**

```
New-Volume -FriendlyName "Sir-Mix-A-Lot" -FileSystem CSVFS_ReFS -StoragePoolFriendlyName S2D* -
StorageTierFriendlyNames Performance, Capacity -StorageTierSizes <Size, Size>
```

### Beyond 4 servers: greater parity efficiency

As you scale beyond four servers, new volumes can benefit from ever-greater parity encoding efficiency. For example, between six and seven servers, efficiency improves from 50.0% to 66.7% as it becomes possible to use Reed-Solomon 4+2 (rather than 2+2). There are no steps you need to take to begin enjoying this new efficiency; the best possible encoding is determined automatically each time you create a volume.

However, any pre-existing volumes will *not* be "converted" to the new, wider encoding. One good reason is that to do so would require a massive calculation affecting literally *every single bit* in the entire deployment. If you would like pre-existing data to become encoded at the higher efficiency, you can migrate it to new volume(s).

For more details, see Fault tolerance and storage efficiency.

### Adding servers when using chassis or rack fault tolerance

If your deployment uses chassis or rack fault tolerance, you must specify the chassis or rack of new servers before adding them to the cluster. This tells Storage Spaces Direct how best to distribute data to maximize fault tolerance.

1. Create a temporary fault domain for the node by opening an elevated PowerShell session and then using the following command, where *<NewNode>* is the name of the new cluster node:

   ```
   New-ClusterFaultDomain -Type Node -Name <NewNode>
   ```

2. Move this temporary fault-domain into the chassis or rack where the new server is located in the real world, as specified by *<ParentName>*:

   ```
   Set-ClusterFaultDomain -Name <NewNode> -Parent <ParentName>
   ```

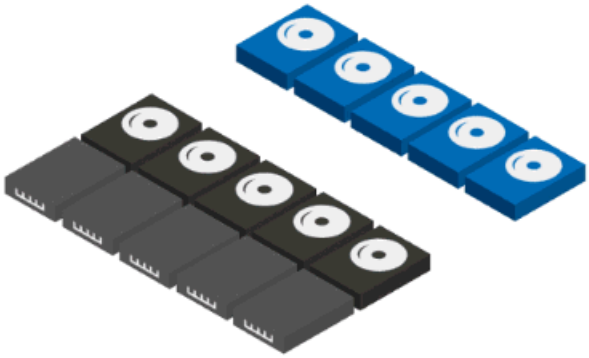
   For more information, see Fault domain awareness in Windows Server 2016.

3. Add the server to the cluster as described in Adding servers. When the new server joins the cluster, it's automatically associated (using its name) with the placeholder fault domain.

## Adding drives

Adding drives, also known as scaling up, adds storage capacity and can improve performance. If you have available slots, you can add drives to each server to expand your storage capacity without adding servers. You can add cache drives or capacity drives independently at any time.

> **IMPORTANT**
>
> We strongly recommend that all servers have identical storage configurations.



To scale up, connect the drives and verify that Windows discovers them. They should appear in the output of the **Get-PhysicalDisk** cmdlet in PowerShell with their **CanPool** property set to **True**. If they show as **CanPool = False**, you can see why by checking their **CannotPoolReason** property.

```
Get-PhysicalDisk | Select SerialNumber, CanPool, CannotPoolReason
```

Within a short time, eligible drives will automatically be claimed by Storage Spaces Direct, added to the storage pool, and volumes will automatically be redistributed evenly across all the drives. At this point, you're finished and ready to extend your volumes or create new ones.

If the drives don't appear, manually scan for hardware changes. This can be done using **Device Manager**, under the **Action** menu. If they contain old data or metadata, consider reformatting them. This can be done using **Disk Management** or with the **Reset-PhysicalDisk** cmdlet.

> **NOTE**
> Automatic pooling depends on you having only one pool. If you've circumvented the standard configuration to create multiple pools, you will need to add new drives to your preferred pool yourself using **Add-PhysicalDisk**.

## Optimizing drive usage after adding drives or servers

Over time, as drives are added or removed, the distribution of data among the drives in the pool can become uneven. In some cases, this can result in certain drives becoming full while other drives in pool have much lower consumption.

To help keep drive allocation even across the pool, Storage Spaces Direct automatically optimizes drive usage after you add drives or servers to the pool (this is a manual process for Storage Spaces systems that use Shared SAS enclosures). Optimization starts 15 minutes after you add a new drive to the pool. Pool optimization runs as a low-priority background operation, so it can take hours or days to complete, especially if you're using large hard drives.

Optimization uses two jobs - one called *Optimize* and one called *Rebalance* - and you can monitor their progress with the following command:

```
Get-StorageJob
```

You can manually optimize a storage pool with the Optimize-StoragePool cmdlet. Here's an example:

```
Get-StoragePool <PoolName> | Optimize-StoragePool
```

# Taking a Storage Spaces Direct server offline for maintenance

12/16/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic provides guidance on how to properly restart or shutdown servers with Storage Spaces Direct.

With Storage Spaces Direct, taking a server offline (bringing it down) also means taking offline portions of the storage that is shared across all servers in the cluster. Doing so requires pausing (suspending) the server you want to take offline, moving roles to other servers in the cluster, and verifying that all data is available on the other servers in the cluster so that the data remains safe and accessible throughout the maintenance.

Use the following procedures to properly pause a server in a Storage Spaces Direct cluster before taking it offline.

> **IMPORTANT**
> To install updates on a Storage Spaces Direct cluster, use Cluster-Aware Updating (CAU), which automatically performs the procedures in this topic so you don't have to when installing updates. For more info, see Cluster Aware Updating (CAU).

## Verifying it's safe to take the server offline

Before taking a server offline for maintenance, verify that all your volumes are healthy.

To do so, open a PowerShell session with Administrator permissions and then run the following command to view volume status:

```
Get-VirtualDisk
```

Here's an example of what the output might look like:

```
FriendlyName ResiliencySettingName OperationalStatus HealthStatus IsManualAttach Size
------------ --------------------- ----------------- ------------ -------------- ----
MyVolume1    Mirror                OK                Healthy      True           1 TB
MyVolume2    Mirror                OK                Healthy      True           1 TB
MyVolume3    Mirror                OK                Healthy      True           1 TB
```

Verify that the **HealthStatus** property for every volume (virtual disk) is **Healthy**.

To do this in Failover Cluster Manager, go to **Storage** > **Disks**.

Verify that the **Status** column for every volume (virtual disk) shows **Online**.

## Pausing and draining the server

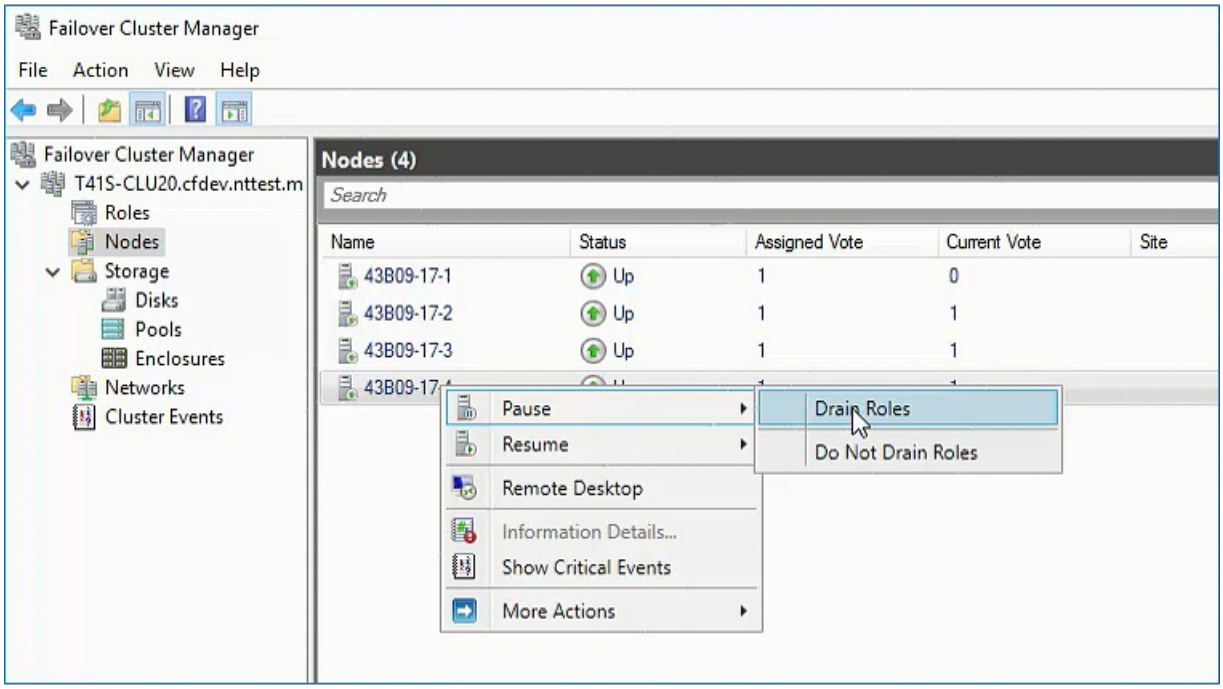
Before restarting or shutting down the server, pause and drain (move off) any roles such as virtual machines running on it. This also gives Storage Spaces Direct an opportunity to gracefully flush and commit data to ensure the shutdown is transparent to any applications running on that server.

> **IMPORTANT**
> Always pause and drain clustered servers before restarting or shutting them down.

In PowerShell, run the following cmdlet (as Administrator) to pause and drain.

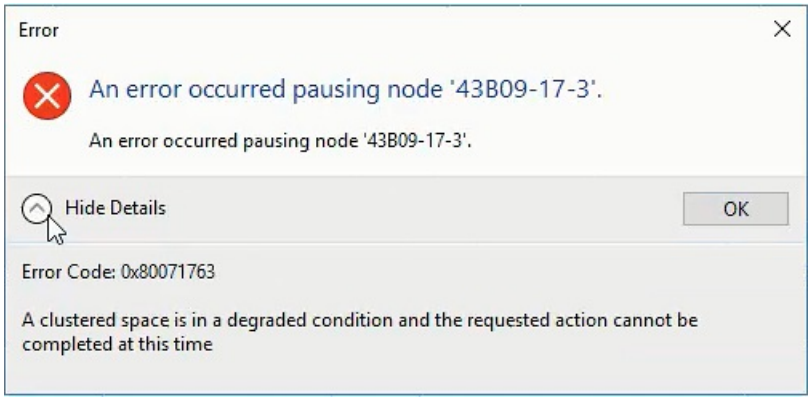
```
Suspend-ClusterNode -Drain
```

To do this in Failover Cluster Manager, go to **Nodes**, right-click the node, and then select **Pause** > **Drain Roles**.



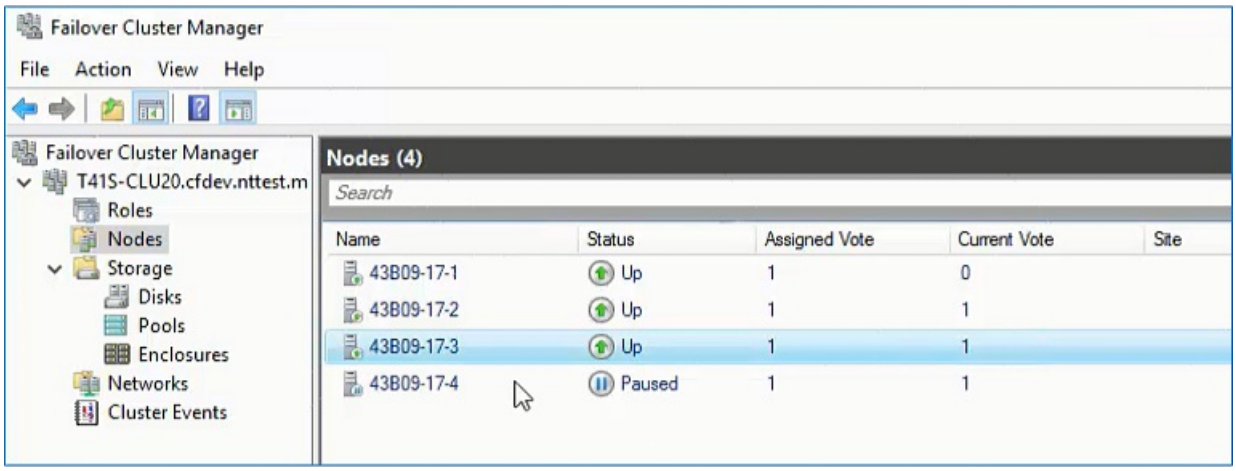

All virtual machines will begin live migrating to other servers in the cluster. This can take a few minutes.

> **NOTE**
> When you pause and drain the cluster node properly, Windows performs an automatic safety check to ensure it is safe to proceed. If there are unhealthy volumes, it will stop and alert you that it's not safe to proceed.




## Shutting down the server

Once the server has completed draining, it will show as **Paused** in Failover Cluster Manager and PowerShell.




You can now safely restart or shut it down, just like you would normally (for example, by using the Restart-Computer or Stop-Computer PowerShell cmdlets).

```
Get-VirtualDisk

FriendlyName ResiliencySettingName OperationalStatus HealthStatus IsManualAttach Size
------------ --------------------- ----------------- ------------ -------------- ----
MyVolume1    Mirror                Incomplete        Warning      True           1 TB
MyVolume2    Mirror                Incomplete        Warning      True           1 TB
MyVolume3    Mirror                Incomplete        Warning      True           1 TB
```

Incomplete or Degraded Operational Status is normal when nodes are shutting down or starting/stopping the cluster service on a node and should not cause concern. All your volumes remain online and accessible.

## Resuming the server

When you are ready for the server to begin hosting workloads again, resume it.

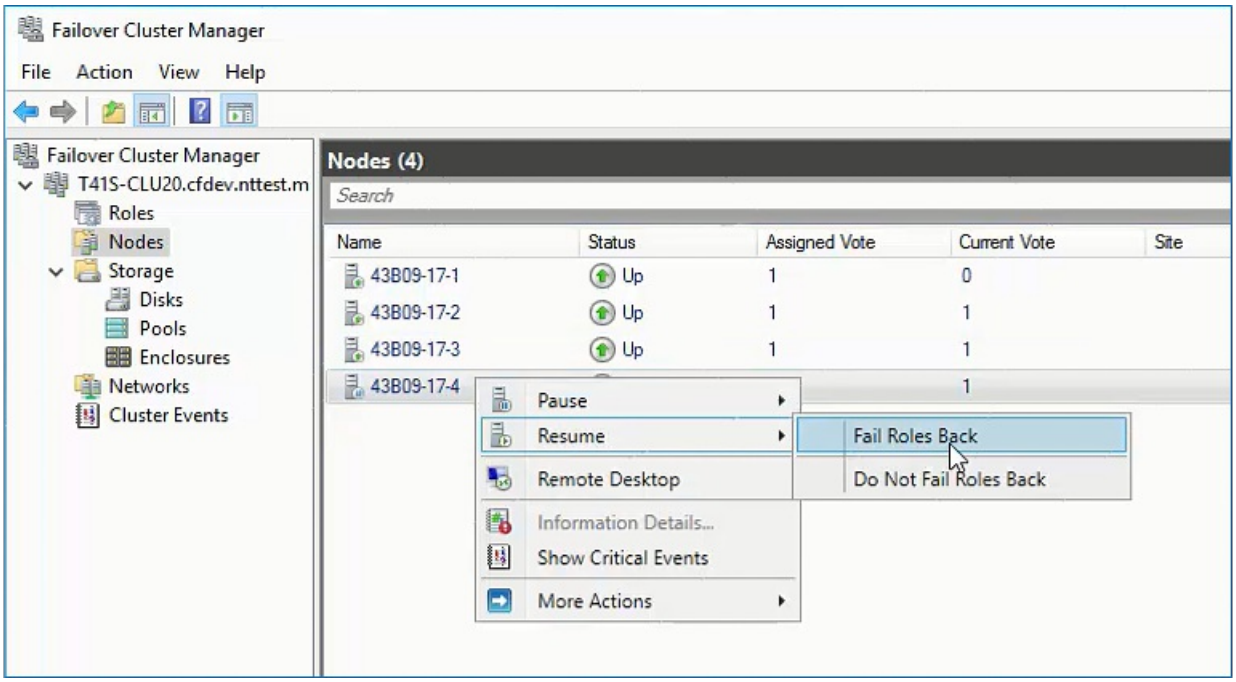
In PowerShell, run the following cmdlet (as Administrator) to resume.

```
Resume-ClusterNode
```

To move the roles that were previously running on this server back, use the optional **-Failback** flag.

```
Resume-ClusterNode –Failback Immediate
```

To do this in Failover Cluster Manager, go to **Nodes**, right-click the node, and then select **Resume** > **Fail Roles Back**.




## Waiting for storage to resync

When the server resumes, any new writes that happened while it was unavailable need to resync. This happens automatically. Using intelligent change tracking, it's not necessary for *all* data to be scanned or synchronized; only the changes. This process is throttled to mitigate impact to production workloads. Depending on how long the server was paused, and how much new data as written, it may take many minutes to complete.

You must wait for re-syncing to complete before taking any others servers in the cluster offline.

In PowerShell, run the following cmdlet (as Administrator) to monitor progress.

```
Get-StorageJob
```

Here's some example output, showing the resync (repair) jobs:

```
Name   IsBackgroundTask ElapsedTime JobState  PercentComplete BytesProcessed BytesTotal
----   ---------------- ----------- --------  --------------- -------------- ----------
Repair True             00:06:23    Running   65              11477975040    17448304640
Repair True             00:06:40    Running   66              15987900416    23890755584
Repair True             00:06:52    Running   68              20104802841    22104819713
```

The **BytesTotal** shows how much storage needs to resync. The **PercentComplete** displays progress.

> **WARNING**
> It's not safe to take another server offline until these repair jobs finish.

During this time, your volumes will continue to show as **Warning**, which is normal.

For example, if you use the `Get-VirtualDisk` cmdlet, you might see the following output:

```
FriendlyName ResiliencySettingName OperationalStatus HealthStatus IsManualAttach Size
------------ --------------------- ----------------- ------------ -------------- ----
MyVolume1    Mirror                InService         Warning      True           1 TB
MyVolume2    Mirror                InService         Warning      True           1 TB
MyVolume3    Mirror                InService         Warning      True           1 TB
```

Once the jobs complete, verify that volumes show **Healthy** again by using the `Get-VirtualDisk` cmdlet. Here's some example output:

```
FriendlyName ResiliencySettingName OperationalStatus HealthStatus IsManualAttach Size
------------ --------------------- ----------------- ------------ -------------- ----
MyVolume1    Mirror                OK                Healthy      True           1 TB
MyVolume2    Mirror                OK                Healthy      True           1 TB
MyVolume3    Mirror                OK                Healthy      True           1 TB
```

It's now safe to pause and restart other servers in the cluster.

## How to update Storage Spaces Direct nodes offline

Use the following steps to update your Storage Spaces Direct system quickly. It involves scheduling a maintenance window and taking the system down for updating. If there is a critical security update that you need applied quickly or maybe you need to ensure updating completes in your maintenance window, this method may be for you. This process brings down the Storage Spaces Direct cluster, updates it, and brings it all up again. The trade-off is downtime to the hosted resources.

1. Plan your maintenance window.
2. Take the virtual disks offline.
3. Stop the cluster to take the storage pool offline. Run the **Stop-Cluster** cmdlet or use Failover Cluster Manager to stop the cluster.
4. Set the cluster service to **Disabled** in Services.msc on each node. This prevents the cluster service from starting up while being patched.
5. Apply the Windows Server Cumulative Update and any required Servicing Stack Updates to all nodes. (You can update all nodes at the same time, no need to wait since the cluster is down).
6. Restart the nodes, and ensure everything looks good.
7. Set the cluster service back to **Automatic** on each node.
8. Start the cluster. Run the **Start-Cluster** cmdlet or use Failover Cluster Manager.

   Give it a few minutes. Make sure the storage pool is healthy.
9. Bring the virtual disks back online.
10. Monitor the status of the virtual disks by running the **Get-Volume** and **Get-VirtualDisk** cmdlets.

## Additional References

- Storage Spaces Direct overview
- Cluster Aware Updating (CAU)

# Removing servers in Storage Spaces Direct

11/2/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic describes how to remove servers in Storage Spaces Direct using PowerShell.

## Remove a server but leave its drives

If you intend to add the server back into the cluster soon, or if you intend to keep its drives by moving them to another server, you can remove the server from the cluster *without* removing its drives from the storage pool. This is the default behavior if you use Failover Cluster Manager to remove the server.

Use the Remove-ClusterNode cmdlet in PowerShell:

```
Remove-ClusterNode <Name>
```

This cmdlet succeeds quickly, regardless of any capacity considerations, because the storage pool "remembers" the missing drives and expects them to come back. There is no data movement away from the missing drives. While they remain missing, their **OperationalStatus** will show as "Lost Communication", and your volumes will show "Incomplete".

When the drives come back, they are automatically detected and re-associated with the pool, even if they are now in a new server.

> **WARNING**
> Do not distribute drives with pool data from one server into multiple other servers. For example, if one server with ten drives fails (because its motherboard or boot drive failed, for instance), you **can** move all ten drives into one new server, but you **cannot** move each of them separately into different other servers.

## Remove a server and its drives

If you want to permanently remove a server from the cluster (sometimes referred to as scaling-in), you can remove the server from the cluster *and* remove its drives from the storage pool.

Use the **Remove-ClusterNode** cmdlet with the optional **-CleanUpDisks** flag:

```
Remove-ClusterNode <Name> -CleanUpDisks
```

This cmdlet might take a long time (sometimes many hours) to run because Windows must move all the data stored on that server to other servers in the cluster. Once this is complete, the drives are permanently removed from the storage pool, returning affected volumes to a healthy state.

### Requirements

To permanently scale-in (remove a server *and* its drives), your cluster must meet the following two requirements. If it doesn't, the **Remove-ClusterNode -CleanUpDisks** cmdlet will return an error immediately, before it begins any data movement, to minimize disruption.

#### Enough capacity

First, you must have enough storage capacity in the remaining servers to accommodate all your volumes.

For example, if you have four servers, each with 10 x 1 TB drives, you have 40 TB of total physical storage capacity. After removing one server and all its drives, you will have 30 TB of capacity left. If the footprints of your volumes are more than 30 TB together, they won't fit in the remaining servers, so the cmdlet will return an error and not move any data.

#### Enough fault domains

Second, you must have enough fault domains (typically servers) to provide the resiliency of your volumes.

For example, if your volumes use three-way mirroring at the server level for resiliency, they cannot be fully healthy unless you have at least three servers. If you have exactly three servers, and then attempt to remove one and all its drives, the cmdlet will return an error and not move any data.

This table shows the minimum number of fault domains required for each resiliency type.

| RESILIENCY | MINIMUM REQUIRED FAULT DOMAINS |
|---|---|
| Two-way mirror | 2 |
| Three-way mirror | 3 |
| Dual parity | 4 |

> **NOTE**
> It is okay to briefly have fewer servers, such as during failures or maintenance. However, in order for volumes to return to a fully healthy state, you must have the minimum number of servers listed above.

## Additional References

- Storage Spaces Direct overview

# Updating drive firmware

12/16/2020 • 9 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows 10

Updating the firmware for drives has historically been a cumbersome task with a potential for downtime, which is why we're making improvements to Storage Spaces, Windows Server, and Windows 10, version 1703 and newer. If you have drives that support the new firmware update mechanism included in Windows, you can update drive firmware of in-production drives without downtime. However, if you're going to update the firmware of a production drive, make sure to read our tips on how to minimize the risk while using this powerful new functionality.

**WARNING**

Firmware updates are a potentially risky maintenance operation and you should only apply them after thorough testing of the new firmware image. It is possible that new firmware on unsupported hardware could negatively affect reliability and stability, or even cause data loss. Administrators should read the release notes a given update comes with to determine its impact and applicability.

## Drive compatibility

To use Windows Server to update drive firmware, you must have supported drives. To ensure common device behavior, we began by defining new and - for Windows 10 and Windows Server 2016 - optional Hardware Lab Kit (HLK) requirements for SAS, SATA, and NVMe devices. These requirements outline which commands a SATA, SAS, or NVMe device must support to be firmware-updatable using these new, Windows-native PowerShell cmdlets. To support these requirements, there is a new HLK test to verify if vendor products support the right commands and get them implemented in future revisions.

Contact your solution vendor for info about whether your hardware supports Windows updating the drive firmware. Here are links to the various requirements:

- SATA: Device.Storage.Hd.Sata - in the **[If Implemented] Firmware Download & Activate** section
- SAS: Device.Storage.Hd.Sas - in the **[If Implemented] Firmware Download & Activate** section
- NVMe: Device.Storage.ControllerDrive.NVMe - in sections **5.7** and **5.8**.

## PowerShell cmdlets

The two cmdlets added to Windows are:

- Get-StorageFirmwareInformation
- Update-StorageFirmware

The first cmdlet provides you with detailed information about the device's capabilities, firmware images, and revisions. In this case, the machine only contains a single SATA SSD with 1 firmware slot. Here's an example:

```
Get-PhysicalDisk | Get-StorageFirmwareInformation

SupportsUpdate        : True
NumberOfSlots         : 1
ActiveSlotNumber      : 0
SlotNumber            : {0}
IsSlotWritable        : {True}
FirmwareVersionInSlot : {J3E16101}
```

Note that SAS devices always report "SupportsUpdate" as "True", since there is no way of explicitly querying the device for support of these commands.

The second cmdlet, Update-StorageFirmware, enables administrators to update the drive firmware with an image file, if the drive supports the new firmware update mechanism. You should obtain this image file from the OEM or drive vendor directly.

> **NOTE**
> Before updating any production hardware, test the particular firmware image on identical hardware in a lab setting.

The drive will first load the new firmware image to an internal staging area. While this happens, I/O typically continues. The image activates after downloading. During this time the drive will not be able to respond to I/O commands as an internal reset occurs. This means that this drive serves no data during the activation. An application accessing data on this drive would have to wait for a response until the firmware activation completes. Here's an example of the cmdlet in action:

```
$pd | Update-StorageFirmware -ImagePath C:\Firmware\J3E160@3.enc -SlotNumber 0
$pd | Get-StorageFirmwareInformation

SupportsUpdate        : True
NumberOfSlots         : 1
ActiveSlotNumber      : 0
SlotNumber            : {0}
IsSlotWritable        : {True}
FirmwareVersionInSlot : {J3E160@3}
```

Drives typically do not complete I/O requests when they activate a new firmware image. How long a drive takes to activate depends on its design and the type of firmware you update. We have observed update times range from fewer than 5 seconds to more than 30 seconds.

This drive performed the firmware update within ~5.8 seconds, as shown here:

```
Measure-Command {$pd | Update-StorageFirmware -ImagePath C:\\Firmware\\J3E16101.enc -SlotNumber 0}

 Days : 0
 Hours : 0
 Minutes : 0
 Seconds : 5
 Milliseconds : 791
 Ticks : 57913910
 TotalDays : 6.70299884259259E-05
 TotalHours : 0.00160871972222222
 TotalMinutes : 0.0965231833333333
 TotalSeconds : 5.791391
 TotalMilliseconds : 5791.391
```

# Updating drives in production

Before placing a server into production, we highly recommend updating the firmware of your drives to the firmware recommended by the hardware vendor or OEM that sold and supports your solution (storage enclosures, drives, and servers).

Once a server is in production, it's a good idea to make as few changes to the server as is practical. However, there may be times when your solution vendor advises you that there is a critically important firmware update for your drives. If this occurs, here are a few good practices to follow before applying any drive firmware updates:

1. Review the firmware release notes and confirm that the update addresses issues that could affect your environment, and that the firmware doesn't contain any known issues that could adversely affect you.

2. Install the firmware on a server in your lab that has identical drives (including the revision of the drive if there are multiple revisions of the same drive), and test the drive under load with the new firmware. For info about doing synthetic load testing, see Test Storage Spaces Performance Using Synthetic Workloads.

# Automated firmware updates with Storage Spaces Direct

Windows Server 2016 includes a Health Service for Storage Spaces Direct deployments (including Microsoft Azure Stack solutions). The main purpose of the Health Service is to make monitoring and management of your hardware deployment easier. As part of its management functions, it has the capability to roll-out drive firmware across an entire cluster without taking any workloads offline or incurring downtime. This capability is policy-driven, with the control in the admin's hands.

Using the Health Service to roll-out firmware across a cluster is very simple and involves the following steps:

- Identify what HDD and SSD drives you expect to be part of your Storage Spaces Direct cluster, and whether the drives support Windows performing firmware updates
- List those drives in the Supported Components xml file
- Identify the firmware versions you expect those drives to have in the Supported Components xml (including location paths of the firmware images)
- Upload the xml file to the cluster DB

At this point, the Health Service will inspect and parse the xml and identify any drives that do not have the desired firmware version deployed. It will then proceed to re-direct I/O away from the affected drives – going node-by-node – and updating the firmware on them. A Storage Spaces Direct cluster achieves resiliency by spreading data across multiple server nodes; it is possible for the health service to isolate an entire node worth of drives for updates. Once a node updates, it will initiate a repair in Storage Spaces, bringing all copies of data across the cluster back in sync with each other, before moving on to the next node. It is expected and normal for Storage Spaces to transition to a "degraded" mode of operation while firmware is rolled out.

To ensure a stable roll-out and sufficient validation time of a new firmware image, there exists a significant delay between the updates of several servers. Per default, the Health Service will wait 7 days before updating the 2$^{nd}$ server. Any subsequent server (3$^{rd}$, 4$^{th}$, ...) updates with a 1 day delay. Should an administrator find the firmware to be unstable or otherwise undesirable, she can stop further roll-out by the health service at any time. If the firmware has been previously validated and a quicker roll-out is desired, these default values can be modified from days, to hours or minutes.

Here is an example of the supported components xml for a generic Storage Spaces Direct cluster:

```
<Components>
    <Disks>
       <Disk>
           <Manufacturer>Contoso</Manufacturer>
           <Model>XYZ9000</Model>
           <AllowedFirmware>
             <Version>2.0</Version>
             <Version>2.1>/Version>
             <Version>2.2</Version>
           </AllowedFirmware>
           <TargetFirmware>
             <Version>2.2</Version>
             <BinaryPath>\\path\to\image.bin</BinaryPath>
           </TargetFirmware>
       </Disk>
       ...
       ...
   </Disks>
</Components>
```

To get the roll-out of the new firmware started in this Storage Spaces Direct cluster, simply upload the .xml to the cluster DB:

```
$SpacesDirect = Get-StorageSubSystem Clus*

$CurrentDoc = $SpacesDirect | Get-StorageHealthSetting -Name "System.Storage.SupportedComponents.Document"

$CurrentDoc.Value | Out-File <Path>
```

Edit the file in your favorite editor, such as Visual Studio Code or Notepad, then save it.

```
$NewDoc = Get-Content <Path> | Out-String

$SpacesDirect | Set-StorageHealthSetting -Name "System.Storage.SupportedComponents.Document" -Value $NewDoc
```

If you would like to see the Health Service in action and learn more about its roll-out mechanism, have a look at this video: https://channel9.msdn.com/Blogs/windowsserver/Update-Drive-Firmware-Without-Downtime-in-Storage-Spaces-Direct

# Frequently asked questions

Also see Troubleshooting drive firmware updates.

**Will this work on any storage device**

This will work on storage devices that implement the correct commands in their firmware. The Get-StorageFirmwareInformation cmdlet will show if a drive's firmware indeed does support the correct commands (for SATA/NVMe) and the HLK test allows vendors and OEMs to test this behavior.

**After I update a SATA drive, it reports to no longer support the update mechanism. Is something wrong with the drive**

No, the drive is fine, unless the new firmware doesn't allow updates anymore. You are hitting a known issue whereby a cached version of the drive's capabilities is incorrect. Running "Update-StorageProviderCache -DiscoveryLevel Full" will re-enumerate the drive capabilities and update the cached copy. As a work-around, we recommend running the above command once before initiating a firmware update or complete roll-out on a Spaces Direct cluster.

**Can I update firmware on my SAN through this mechanism**

No - SANs usually have their own utilities and interfaces for such maintenance operations. This new mechanism is for directly attached storage, such as SATA, SAS, or NVMe devices.

**From where do I get the firmware image**

You should always obtain any firmware directly from your OEM, solution vendor, or drive vendor and not download it from other parties. Windows provides the mechanism to get the image to the drive, but cannot verify its integrity.

**Will this work on clustered drives**

The cmdlets can perform their function on clustered drives as well, but keep in mind that the Health Service orchestration mitigates the I/O impact on running workloads. If the cmdlets are used directly on clustered drives, I/O is likely to stall. In general, it is a best practice to perform drive firmware updates when there is no, or just a minimal workload on the underlying drives.

**What happens when I update firmware on Storage Spaces**

On Windows Server 2016 with the Health Service deployed on Storage Spaces Direct, you can perform this operation without taking your workloads offline, assuming the drives support Windows Server updating the firmware.

**What happens if the update fails**

The update could fail for various reasons, some of them are: 1) The drive doesn't support the correct commands for Windows to update its firmware. In this case the new firmware image never activates and the drive continues functioning with the old image. 2) The image cannot download to or be applied to this drive (version mismatch, corrupt image, ...). In this case the drive fails the activate command. Again, the old firmware image will continue function.

If the drive does not respond at all after a firmware update, you are likely hitting a bug in the drive firmware itself. Test all firmware updates in a lab environment before putting them in production. The only remediation may be to replace the drive.

For more info, see Troubleshooting drive firmware updates.

**How do I stop an in-progress firmware roll-out**

Disable the roll-out in PowerShell via:

```
Get-StorageSubSystem Cluster* | Set-StorageHealthSetting -Name
"System.Storage.PhysicalDisk.AutoFirmwareUpdate.RollOut.Enabled" -Value false
```

**I am seeing an access denied or path-not-found error during roll out. How do I fix this**

Ensure that the firmware image you would like to use for the update is accessible by all cluster nodes. The easiest way to ensure this is to place it on a cluster shared volume.

# Extending volumes in Storage Spaces Direct

11/2/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

This topic provides instructions for resizing volumes on a Storage Spaces Direct cluster by using Windows Admin Center.

> **WARNING**
>
> **Not supported: resizing the underlying storage used by Storage Spaces Direct.** If you are running Storage Spaces Direct in a virtualized storage environment, including in Azure, resizing or changing the characteristics of the storage devices used by the virtual machines isn't supported and will cause data to become inaccessible. Instead, follow the instructions in the Add servers or drives section to add additional capacity before extending volumes.

Watch a quick video on how to resize a volume.

## Extending volumes using Windows Admin Center

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab, and then select the volume that you want to resize.

   On the volume detail page, the storage capacity for the volume is indicated. You can also open the volumes detail page directly from the Dashboard. On the Dashboard, in the Alerts pane, select the alert, which notifies you if a volume is running low on storage capacity, and then select **Go To Volume**.
3. At the top of the volumes detail page, select **Resize**.
4. Enter a new larger size, and then select **Resize**.

   On the volumes detail page, the larger storage capacity for the volume is indicated, and the alert on the Dashboard is cleared.

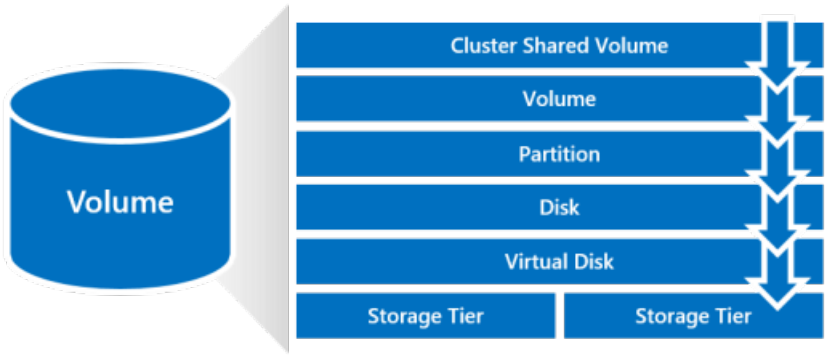
## Extending volumes using PowerShell

### Capacity in the storage pool

Before you resize a volume, make sure you have enough capacity in the storage pool to accommodate its new, larger footprint. For example, when resizing a three-way mirror volume from 1 TB to 2 TB, its footprint would grow from 3 TB to 6 TB. For the resize to succeed, you would need at least (6 - 3) = 3 TB of available capacity in the storage pool.

### Familiarity with volumes in Storage Spaces

In Storage Spaces Direct, every volume is comprised of several stacked objects: the cluster shared volume (CSV), which is a volume; the partition; the disk, which is a virtual disk; and one or more storage tiers (if applicable). To resize a volume, you will need to resize several of these objects.




To familiarize yourself with them, try running **Get-** with the corresponding noun in PowerShell.

For example:

```
Get-VirtualDisk
```

To follow associations between objects in the stack, pipe one **Get-** cmdlet into the next.

For example, here's how to get from a virtual disk up to its volume:

```
Get-VirtualDisk <FriendlyName> | Get-Disk | Get-Partition | Get-Volume
```

**Step 1 – Resize the virtual disk**

The virtual disk may use storage tiers, or not, depending on how it was created.

To check, run the following cmdlet:

```
Get-VirtualDisk <FriendlyName> | Get-StorageTier
```

If the cmdlet returns nothing, the virtual disk doesn't use storage tiers.

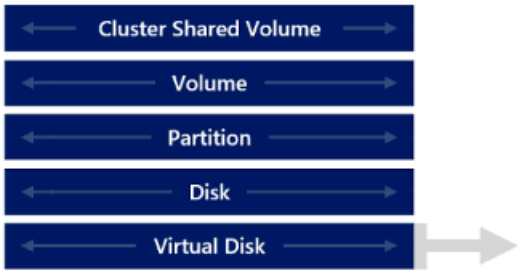
**No storage tiers**

If the virtual disk has no storage tiers, you can resize it directly using the **Resize-VirtualDisk** cmdlet.

Provide the new size in the **-Size** parameter.

```
Get-VirtualDisk <FriendlyName> | Resize-VirtualDisk -Size <Size>
```

When you resize the **VirtualDisk**, the **Disk** follows automatically and is resized too.




**With storage tiers**

If the virtual disk uses storage tiers, you can resize each tier separately using the **Resize-StorageTier** cmdlet.

Get the names of the storage tiers by following the associations from the virtual disk.

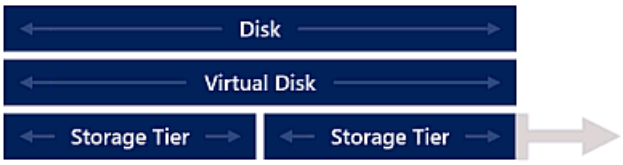
```
Get-VirtualDisk <FriendlyName> | Get-StorageTier | Select FriendlyName
```

Then, for each tier, provide the new size in the **-Size** parameter.

```
Get-StorageTier <FriendlyName> | Resize-StorageTier -Size <Size>
```

> **TIP**
> If your tiers are different physical media types (such as **MediaType = SSD** and **MediaType = HDD**) you need to ensure you have enough capacity of each media type in the storage pool to accommodate the new, larger footprint of each tier.

When you resize the **StorageTier**(s), the **VirtualDisk** and **Disk** follow automatically and are resized too.



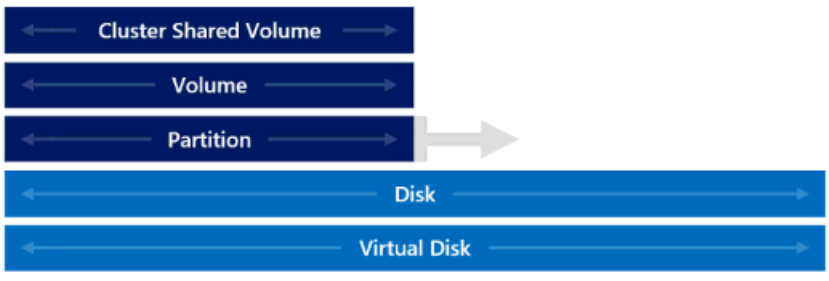

**Step 2 – Resize the partition**

Next, resize the partition using the **Resize-Partition** cmdlet. The virtual disk is expected to have two partitions: the first is Reserved and should not be modified; the one you need to resize has **PartitionNumber = 2** and **Type = Basic**.

Provide the new size in the **-Size** parameter. We recommend using the maximum supported size, as shown below.

```
# Choose virtual disk
$VirtualDisk = Get-VirtualDisk <FriendlyName>

# Get its partition
$Partition = $VirtualDisk | Get-Disk | Get-Partition | Where PartitionNumber -Eq 2

# Resize to its maximum supported size
$Partition | Resize-Partition -Size ($Partition | Get-PartitionSupportedSize).SizeMax
```

When you resize the **Partition**, the **Volume** and **ClusterSharedVolume** follow automatically and are resized too.




That's it!

**TIP**

You can verify the volume has the new size by running **Get-Volume**.

## Additional References

- Storage Spaces Direct in Windows Server 2016
- Planning volumes in Storage Spaces Direct
- Creating volumes in Storage Spaces Direct
- Deleting volumes in Storage Spaces Direct

# Deleting volumes in Storage Spaces Direct

11/2/2020 • 2 minutes to read • Edit Online

> Applies to: Windows Server 2019, Windows Server 2016

This topic provides instructions for deleting volumes in on a Storage Spaces Direct cluster by using Windows Admin Center.

Watch a quick video on how to delete a volume.

To delete a volume in Windows Admin Center:

1. In Windows Admin Center, connect to a Storage Spaces Direct cluster, and then select **Volumes** from the **Tools** pane.
2. On the Volumes page, select the **Inventory** tab, and then select the volume that you want to delete.
3. At the top of the volumes detail page, select **Delete**.
4. In the confirmations dialog, select the check box to confirm that you want to delete the volume, and select **Delete**.

## Additional References

- Storage Spaces Direct in Windows Server 2016
- Planning volumes in Storage Spaces Direct
- Creating volumes in Storage Spaces Direct
- Extending volumes in Storage Spaces Direct

# Performance history for Storage Spaces Direct

12/16/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server 2019

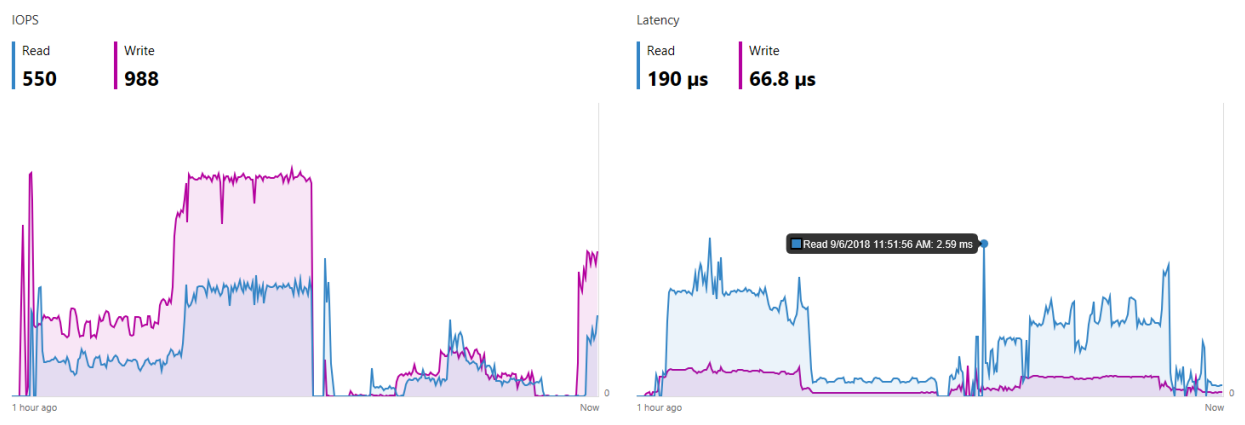
Performance history is a new feature that gives Storage Spaces Direct administrators easy access to historical compute, memory, network, and storage measurements across host servers, drives, volumes, virtual machines, and more. Performance history is collected automatically and stored on the cluster for up to one year.

> **IMPORTANT**
>
> This feature is new in Windows Server 2019. It is not available in Windows Server 2016.

## Get started

Performance history is collected by default with Storage Spaces Direct in Windows Server 2019. You do not need to install, configure, or start anything. An Internet connection is not required, System Center is not required, and an external database is not required.

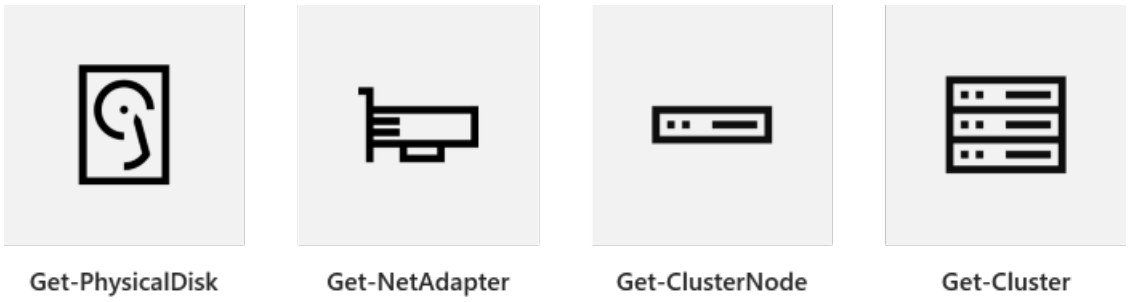
To see your cluster's performance history graphically, use Windows Admin Center:




To query and process it programmatically, use the new `Get-ClusterPerf` cmdlet. See Usage in PowerShell.

## What's collected

Performance history is collected for 7 types of objects:





Each object type has many series: for example, `ClusterNode.Cpu.Usage` is collected for each server.

For details of what's collected for each object type and how to interpret them, refer to these sub-topics:

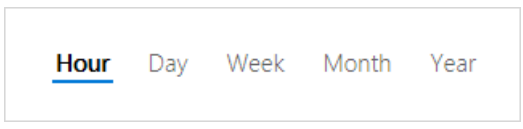
| OBJECT | SERIES |
|---|---|
| Drives | What's collected for drives |
| Network adapters | What's collected for network adapters |
| Servers | What's collected for servers |
| Virtual hard disks | What's collected for virtual hard disks |
| Virtual machines | What's collected for virtual machines |
| Volumes | What's collected for volumes |
| Clusters | What's collected for clusters |

Many series are aggregated across peer objects to their parent: for example, `NetAdapter.Bandwidth.Inbound` is collected for each network adapter separately and aggregated to the overall server; likewise `ClusterNode.Cpu.Usage` is aggregated to the overall cluster; and so on.

## Timeframes

Performance history is stored for up to one year, with diminishing granularity. For the most recent hour, measurements are available every ten seconds. Thereafter, they are intelligently merged (by averaging or summing, as appropriate) into less granular series that span more time. For the most recent day, measurements are available every five minutes; for the most recent week, every fifteen minutes; and so on.

In Windows Admin Center, you can select the timeframe in the upper-right above the chart.



In PowerShell, use the `-TimeFrame` parameter.

Here are the available timeframes:

| TIMEFRAME | MEASUREMENT FREQUENCY | RETAINED FOR |
|---|---|---|
| `LastHour` | Every 10 secs | 1 hour |
| `LastDay` | Every 5 minutes | 25 hours |
| `LastWeek` | Every 15 minutes | 8 days |
| `LastMonth` | Every 1 hour | 35 days |
| `LastYear` | Every 1 day | 400 days |

## Usage in PowerShell

Use the `Get-ClusterPerformanceHistory` cmdlet to query and process performance history in PowerShell.

```
Get-ClusterPerformanceHistory
```

> **TIP**
> Use the **Get-ClusterPerf** alias to save some keystrokes.

### Example

Get the CPU usage of virtual machine *MyVM* for the last hour:

```
Get-VM "MyVM" | Get-ClusterPerf -VMSeriesName "VM.Cpu.Usage" -TimeFrame LastHour
```

For more advanced examples, see the published sample scripts that provide starter code to find peak values, calculate averages, plot trend lines, run outlier detection, and more.

### Specify the object

You can specify the object you want by the pipeline. This works with 7 types of objects:

| OBJECT FROM PIPELINE | EXAMPLE |
|---|---|
| `Get-PhysicalDisk` | `Get-PhysicalDisk -SerialNumber "XYZ456" \| Get-ClusterPerf` |
| `Get-NetAdapter` | `Get-NetAdapter "Ethernet" \| Get-ClusterPerf` |
| `Get-ClusterNode` | `Get-ClusterNode "Server123" \| Get-ClusterPerf` |
| `Get-VHD` | `Get-VHD "C:\ClusterStorage\MyVolume\MyVHD.vhdx" \| Get-ClusterPerf` |
| `Get-VM` | `Get-VM "MyVM" \| Get-ClusterPerf` |

| OBJECT FROM PIPELINE | EXAMPLE |
| --- | --- |
| `Get-Volume` | `Get-Volume -FriendlyName "MyVolume" \| Get-ClusterPerf` |
| `Get-Cluster` | `Get-Cluster "MyCluster" \| Get-ClusterPerf` |

If you don't specify, performance history for the overall cluster is returned.

### Specify the series

You can specify the series you want with these parameters:

| PARAMETER | EXAMPLE | LIST |
| --- | --- | --- |
| `-PhysicalDiskSeriesName` | `"PhysicalDisk.Iops.Read"` | What's collected for drives |
| `-NetAdapterSeriesName` | `"NetAdapter.Bandwidth.Outbound"` | What's collected for network adapters |
| `-ClusterNodeSeriesName` | `"ClusterNode.Cpu.Usage"` | What's collected for servers |
| `-VHDSeriesName` | `"Vhd.Size.Current"` | What's collected for virtual hard disks |
| `-VMSeriesName` | `"Vm.Memory.Assigned"` | What's collected for virtual machines |
| `-VolumeSeriesName` | `"Volume.Latency.Write"` | What's collected for volumes |
| `-ClusterSeriesName` | `"PhysicalDisk.Size.Total"` | What's collected for clusters |

> **TIP**
> Use tab completion to discover available series.

If you don't specify, every series available for the specified object is returned.

### Specify the timeframe

You can specify the timeframe of history you want with the `-TimeFrame` parameter.

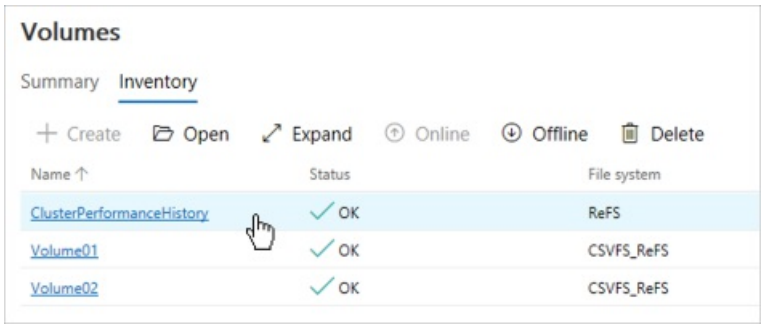
> **TIP**
> Use tab completion to discover available timeframes.

If you don't specify, the `MostRecent` measurement is returned.

## How it works

### Performance history storage

Shortly after Storage Spaces Direct is enabled, an approximately 10 GB volume named `ClusterPerformanceHistory` is created and an instance of the Extensible Storage Engine (also known as Microsoft JET) is provisioned there. This lightweight database stores the performance history without any Administrator involvement or management.




The volume is backed by Storage Spaces and uses either simple, two-way mirror, or three-way mirror resiliency, depending on the number of nodes in the cluster. It is repaired after drive or server failures just like any other volume in Storage Spaces Direct.

The volume uses ReFS but is not Cluster Shared Volume (CSV), so it only appears on the Cluster Group owner node. Besides being automatically created, there is nothing special about this volume: you can see it, browse it, resize it, or delete it (not recommended). If something goes wrong, see Troubleshooting.

#### Object discovery and data collection

Performance history automatically discovers relevant objects, such as virtual machines, anywhere in the cluster and begins streaming their performance counters. The counters are aggregated, synchronized, and inserted into the database. Streaming runs continuously and is optimized for minimal system impact.

Collection is handled by the Health Service, which is highly available: if the node where it's running goes down, it will resume moments later on another node in the cluster. Performance history may lapse briefly, but it will resume automatically. You can see the Health Service and its owner node by running `Get-ClusterResource Health` in PowerShell.

#### Handling measurement gaps

When measurements are merged into less granular series that span more time, as described in Timeframes, periods of missing data are excluded. For example, if the server was down for 30 minutes, then running at 50% CPU for the next 30 minutes, the `ClusterNode.Cpu.Usage` average for the hour will be recorded correctly as 50% (not 25%).

#### Extensibility and customization

Performance history is scripting-friendly. Use PowerShell to pull any available history directly from the database to build automated reporting or alerting, export history for safekeeping, roll your own visualizations, etc. See the published sample scripts for helpful starter code.

It's not possible to collect history for additional objects, timeframes, or series.

The measurement frequency and retention period are not currently configurable.

## Start or stop performance history

#### How do I enable this feature?

Unless you `Stop-ClusterPerformanceHistory`, performance history is enabled by default.

To re-enable it, run this PowerShell cmdlet as Administrator:

```
Start-ClusterPerformanceHistory
```

#### How do I disable this feature?

To stop collecting performance history, run this PowerShell cmdlet as Administrator:

```
Stop-ClusterPerformanceHistory
```

To delete existing measurements, use the `-DeleteHistory` flag:

```
Stop-ClusterPerformanceHistory -DeleteHistory
```

> **TIP**
> During initial deployment, you can prevent performance history from starting by setting the `-CollectPerformanceHistory` parameter of `Enable-ClusterStorageSpacesDirect` to `$False`.

# Troubleshooting

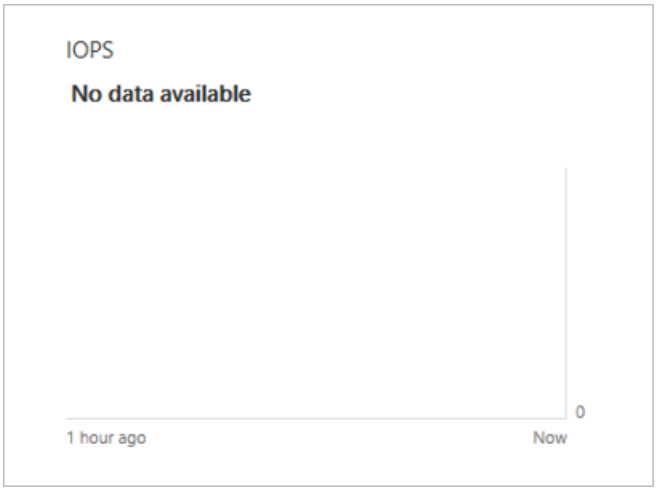
### The cmdlet doesn't work

An error message like "*The term 'Get-ClusterPerf' is not recognized as the name of a cmdlet*" means the feature is not available or installed. Verify that you have Windows Server Insider Preview build 17692 or later, that you've installed Failover Clustering, and that you're running Storage Spaces Direct.

> **NOTE**
> This feature is not available on Windows Server 2016 or earlier.

### No data available

If a chart shows "*No data available*" as pictured, here's how to troubleshoot:




1. If the object was newly added or created, wait for it to be discovered (up to 15 minutes).
2. Refresh the page, or wait for the next background refresh (up to 30 seconds).
3. Certain special objects are excluded from performance history – for example, virtual machines that aren't clustered, and volumes that don't use the Cluster Shared Volume (CSV) filesystem. Check the sub-topic for the object type, like Performance history for volumes, for the fine print.
4. If the problem persists, open PowerShell as Administrator and run the `Get-ClusterPerf` cmdlet. The cmdlet includes troubleshooting logic to identify common problems, such as if the ClusterPerformanceHistory volume is missing, and provides remediation instructions.
5. If the command in the previous step returns nothing, you can try restarting the Health Service (which collects performance history) by running `Stop-ClusterResource Health ; Start-ClusterResource Health` in

PowerShell.

## Additional References

- Storage Spaces Direct overview

# Performance history for drives

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for drives. Performance history is available for every drive in the cluster storage subsystem, regardless of bus or media type. However, it is not available for OS boot drives.

> **NOTE**
> Performance history cannot be collected for drives in a server that is down. Collection will resume automatically when the server comes back up.

## Series names and units

These series are collected for every eligible drive:

| SERIES | UNIT |
| --- | --- |
| `physicaldisk.iops.read` | per second |
| `physicaldisk.iops.write` | per second |
| `physicaldisk.iops.total` | per second |
| `physicaldisk.throughput.read` | bytes per second |
| `physicaldisk.throughput.write` | bytes per second |
| `physicaldisk.throughput.total` | bytes per second |
| `physicaldisk.latency.read` | seconds |
| `physicaldisk.latency.write` | seconds |
| `physicaldisk.latency.average` | seconds |
| `physicaldisk.size.total` | bytes |
| `physicaldisk.size.used` | bytes |

## How to interpret

| SERIES | HOW TO INTERPRET |
| --- | --- |

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `physicaldisk.iops.read` | Number of read operations per second completed by the drive. |
| `physicaldisk.iops.write` | Number of write operations per second completed by the drive. |
| `physicaldisk.iops.total` | Total number of read or write operations per second completed by the drive. |
| `physicaldisk.throughput.read` | Quantity of data read from the drive per second. |
| `physicaldisk.throughput.write` | Quantity of data written to the drive per second. |
| `physicaldisk.throughput.total` | Total quantity of data read from or written to the drive per second. |
| `physicaldisk.latency.read` | Average latency of read operations from the drive. |
| `physicaldisk.latency.write` | Average latency of write operations to the drive. |
| `physicaldisk.latency.average` | Average latency of all operations to or from the drive. |
| `physicaldisk.size.total` | The total storage capacity of the drive. |
| `physicaldisk.size.used` | The used storage capacity of the drive. |

## Where they come from

The `iops.*`, `throughput.*`, and `latency.*` series are collected from the `Physical Disk` performance counter set on the server where the drive is connected, one instance per drive. These counters are measured by `partmgr.sys` and do not include much of the Windows software stack nor any network hops. They are representative of device hardware performance.

| SERIES | SOURCE COUNTER |
| --- | --- |
| `physicaldisk.iops.read` | `Disk Reads/sec` |
| `physicaldisk.iops.write` | `Disk Writes/sec` |
| `physicaldisk.iops.total` | `Disk Transfers/sec` |
| `physicaldisk.throughput.read` | `Disk Read Bytes/sec` |
| `physicaldisk.throughput.write` | `Disk Write Bytes/sec` |
| `physicaldisk.throughput.total` | `Disk Bytes/sec` |
| `physicaldisk.latency.read` | `Avg. Disk sec/Read` |

| SERIES | SOURCE COUNTER |
| --- | --- |
| `physicaldisk.latency.write` | `Avg. Disk sec/Writes` |
| `physicaldisk.latency.average` | `Avg. Disk sec/Transfer` |

> **NOTE**
> Counters are measured over the entire interval, not sampled. For example, if the drive is idle for 9 seconds but completes 30 IOs in the 10th second, its `physicaldisk.iops.total` will be recorded as 3 IOs per second on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

The `size.*` series are collected from the `MSFT_PhysicalDisk` class in WMI, one instance per drive.

| SERIES | SOURCE PROPERTY |
| --- | --- |
| `physicaldisk.size.total` | `Size` |
| `physicaldisk.size.used` | `VirtualDiskFootprint` |

## Usage in PowerShell

Use the Get-PhysicalDisk cmdlet:

```
Get-PhysicalDisk -SerialNumber <SerialNumber> | Get-ClusterPerf
```

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for network adapters

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for network adapters. Network adapter performance history is available for every physical network adapter in every server in the cluster. Remote Direct Memory Access (RDMA) performance history is available for every physical network adapter with RDMA enabled.

> **NOTE**
> Performance history cannot be collected for network adapters in a server that is down. Collection will resume automatically when the server comes back up.

## Series names and units

These series are collected for every eligible network adapter:

| SERIES | UNIT |
|---|---|
| `netadapter.bandwidth.inbound` | bits per second |
| `netadapter.bandwidth.outbound` | bits per second |
| `netadapter.bandwidth.total` | bits per second |
| `netadapter.bandwidth.rdma.inbound` | bits per second |
| `netadapter.bandwidth.rdma.outbound` | bits per second |
| `netadapter.bandwidth.rdma.total` | bits per second |

> **NOTE**
> Network adapter performance history is recorded in **bits** per second, not bytes per second. One 10 GbE network adapter can send and receive approximately 1,000,000,000 bits = 125,000,000 bytes = 1.25 GB per second at its theoretical maximum.

## How to interpret

| SERIES | HOW TO INTERPRET |
|---|---|
| `netadapter.bandwidth.inbound` | Rate of data received by the network adapter. |
| `netadapter.bandwidth.outbound` | Rate of data sent by the network adapter. |

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `netadapter.bandwidth.total` | Total rate of data received or sent by the network adapter. |
| `netadapter.bandwidth.rdma.inbound` | Rate of data received over RDMA by the network adapter. |
| `netadapter.bandwidth.rdma.outbound` | Rate of data sent over RDMA by the network adapter. |
| `netadapter.bandwidth.rdma.total` | Total rate of data received or sent over RDMA by the network adapter. |

## Where they come from

The `bytes.*` series are collected from the `Network Adapter` performance counter set on the server where the network adapter is installed, one instance per network adapter.

| SERIES | SOURCE COUNTER |
| --- | --- |
| `netadapter.bandwidth.inbound` | 8 × `Bytes Received/sec` |
| `netadapter.bandwidth.outbound` | 8 × `Bytes Sent/sec` |
| `netadapter.bandwidth.total` | 8 × `Bytes Total/sec` |

The `rdma.*` series are collected from the `RDMA Activity` performance counter set on the server where the network adapter is installed, one instance per network adapter with RDMA enabled.

| SERIES | SOURCE COUNTER |
| --- | --- |
| `netadapter.bandwidth.rdma.inbound` | 8 × `Inbound bytes/sec` |
| `netadapter.bandwidth.rdma.outbound` | 8 × `Outbound bytes/sec` |
| `netadapter.bandwidth.rdma.total` | 8 × *sum of the above* |

> **NOTE**
> Counters are measured over the entire interval, not sampled. For example, if the network adapter is idle for 9 seconds but transfers 200 bits in the 10th second, its `netadapter.bandwidth.total` will be recorded as 20 bits per second on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

## Usage in PowerShell

Use the Get-NetAdapter cmdlet:

```
Get-NetAdapter <Name> | Get-ClusterPerf
```

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for servers

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for servers. Performance history is available for every server in the cluster.

> **NOTE**
> Performance history cannot be collected for a server that is down. Collection will resume automatically when the server comes back up.

## Series names and units

These series are collected for every eligible server:

| SERIES | UNIT |
|---|---|
| `clusternode.cpu.usage` | percent |
| `clusternode.cpu.usage.guest` | percent |
| `clusternode.cpu.usage.host` | percent |
| `clusternode.memory.total` | bytes |
| `clusternode.memory.available` | bytes |
| `clusternode.memory.usage` | bytes |
| `clusternode.memory.usage.guest` | bytes |
| `clusternode.memory.usage.host` | bytes |

In addition, drive series such as `physicaldisk.size.total` are aggregated for all eligible drives attached to the server, and network adapter series such as `networkadapter.bytes.total` are aggregated for all eligible network adapters attached to the server.

## How to interpret

| SERIES | HOW TO INTERPRET |
|---|---|
| `clusternode.cpu.usage` | Percentage of processor time that is not idle. |
| `clusternode.cpu.usage.guest` | Percentage of processor time used for guest (virtual machine) demand. |

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `clusternode.cpu.usage.host` | Percentage of processor time used for host demand. |
| `clusternode.memory.total` | The total physical memory of the server. |
| `clusternode.memory.available` | The available memory of the server. |
| `clusternode.memory.usage` | The allocated (not available) memory of the server. |
| `clusternode.memory.usage.guest` | The memory allocated to guest (virtual machine) demand. |
| `clusternode.memory.usage.host` | The memory allocated to host demand. |

## Where they come from

The `cpu.*` series are collected from different performance counters depending on whether or not Hyper-V is enabled.

If Hyper-V is enabled:

| SERIES | SOURCE COUNTER |
| --- | --- |
| `clusternode.cpu.usage` | `Hyper-V Hypervisor Logical Processor` > `_Total` > `% Total Run Time` |
| `clusternode.cpu.usage.guest` | `Hyper-V Hypervisor Virtual Processor` > `_Total` > `% Total Run Time` |
| `clusternode.cpu.usage.host` | `Hyper-V Hypervisor Root Virtual Processor` > `_Total` > `% Total Run Time` |

Using the `% Total Run Time` counters ensures that performance history attributes all usage.

If Hyper-V is NOT enabled:

| SERIES | SOURCE COUNTER |
| --- | --- |
| `clusternode.cpu.usage` | `Processor` > `_Total` > `% Processor Time` |
| `clusternode.cpu.usage.guest` | *zero* |
| `clusternode.cpu.usage.host` | *same as total usage* |

Notwithstanding imperfect synchronization, `clusternode.cpu.usage` is always `clusternode.cpu.usage.host` plus `clusternode.cpu.usage.guest`.

With the same caveat, `clusternode.cpu.usage.guest` is always the sum of `vm.cpu.usage` for all virtual machines on the host server.

The `memory.*` series are (COMING SOON).

> **NOTE**
>
> Counters are measured over the entire interval, not sampled. For example, if the server is idle for 9 seconds but spikes to 100% CPU in the 10th second, its `clusternode.cpu.usage` will be recorded as 10% on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

## Usage in PowerShell

Use the Get-ClusterNode cmdlet:

```
Get-ClusterNode <Name> | Get-ClusterPerf
```

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for virtual hard disks

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for virtual hard disk (VHD) files. Performance history is available for every VHD attached to a running, clustered virtual machine. Performance history is available for both VHD and VHDX formats, however it is not available for Shared VHDX files.

> **NOTE**
> It may take several minutes for collection to begin for newly created or moved VHD files.

## Series names and units

These series are collected for every eligible virtual hard disk:

| SERIES | UNIT |
| --- | --- |
| `vhd.iops.read` | per second |
| `vhd.iops.write` | per second |
| `vhd.iops.total` | per second |
| `vhd.throughput.read` | bytes per second |
| `vhd.throughput.write` | bytes per second |
| `vhd.throughput.total` | bytes per second |
| `vhd.latency.average` | seconds |
| `vhd.size.current` | bytes |
| `vhd.size.maximum` | bytes |

## How to interpret

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `vhd.iops.read` | Number of read operations per second completed by the virtual hard disk. |
| `vhd.iops.write` | Number of write operations per second completed by the virtual hard disk. |

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `vhd.iops.total` | Total number of read or write operations per second completed by the virtual hard disk. |
| `vhd.throughput.read` | Quantity of data read from the virtual hard disk per second. |
| `vhd.throughput.write` | Quantity of data written to the virtual hard disk per second. |
| `vhd.throughput.total` | Total quantity of data read from or written to the virtual hard disk per second. |
| `vhd.latency.average` | Average latency of all operations to or from the virtual hard disk. |
| `vhd.size.current` | The current file size of the virtual hard disk, if dynamically expanding. If fixed, the series is not collected. |
| `vhd.size.maximum` | The maximum size of the virtual hard disk, if dynamically expanding. If fixed, the is the size. |

## Where they come from

The `iops.*`, `throughput.*`, and `latency.*` series are collected from the `Hyper-V Virtual Storage Device` performance counter set on the server where the virtual machine is running, one instance per VHD or VHDX.

| SERIES | SOURCE COUNTER |
| --- | --- |
| `vhd.iops.read` | `Read Operations/Sec` |
| `vhd.iops.write` | `Write Operations/Sec` |
| `vhd.iops.total` | *sum of the above* |
| `vhd.throughput.read` | `Read Bytes/sec` |
| `vhd.throughput.write` | `Write Bytes/sec` |
| `vhd.throughput.total` | *sum of the above* |
| `vhd.latency.average` | `Latency` |

> **NOTE**
> Counters are measured over the entire interval, not sampled. For example, if the VHD is inactive for 9 seconds but completes 30 IOs in the 10th second, its `vhd.iops.total` will be recorded as 3 IOs per second on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

## Usage in PowerShell

Use the Get-VHD cmdlet:

```
Get-VHD <Path> | Get-ClusterPerf
```

To get the path of every VHD from the virtual machine:

```
(Get-VM <Name>).HardDrives | Select Path
```

> **NOTE**
> The Get-VHD cmdlet requires a file path to be provided. It does not support enumeration.

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for virtual machines

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for virtual machines (VM). Performance history is available for every running, clustered VM.

> **NOTE**
> It may take several minutes for collection to begin for newly created or renamed VMs.

## Series names and units

These series are collected for every eligible VM:

| SERIES | UNIT |
|---|---|
| `vm.cpu.usage` | percent |
| `vm.memory.assigned` | bytes |
| `vm.memory.available` | bytes |
| `vm.memory.maximum` | bytes |
| `vm.memory.minimum` | bytes |
| `vm.memory.pressure` | - |
| `vm.memory.startup` | bytes |
| `vm.memory.total` | bytes |
| `vmnetworkadapter.bandwidth.inbound` | bits per second |
| `vmnetworkadapter.bandwidth.outbound` | bits per second |
| `vmnetworkadapter.bandwidth.total` | bits per second |

In addition, all virtual hard disk (VHD) series, such as `vhd.iops.total`, are aggregated for every VHD attached to the VM.

## How to interpret

| SERIES | DESCRIPTION |
| --- | --- |
| `vm.cpu.usage` | Percentage the virtual machine is using of its host server's processor(s). |
| `vm.memory.assigned` | The quantity of memory assigned to the virtual machine. |
| `vm.memory.available` | The quantity of memory that remains available, of the amount assigned. |
| `vm.memory.maximum` | If using dynamic memory, this is the maximum quantity of memory that may be assigned to the virtual machine. |
| `vm.memory.minimum` | If using dynamic memory, this is the minimum quantity of memory that may be assigned to the virtual machine. |
| `vm.memory.pressure` | The ratio of memory demanded by the virtual machine over memory allocated to the virtual machine. |
| `vm.memory.startup` | The quantity of memory required for the virtual machine to start. |
| `vm.memory.total` | Total memory. |
| `vmnetworkadapter.bandwidth.inbound` | Rate of data received by the virtual machine across all its virtual network adapters. |
| `vmnetworkadapter.bandwidth.outbound` | Rate of data sent by the virtual machine across all its virtual network adapters. |
| `vmnetworkadapter.bandwidth.total` | Total rate of data received or sent by the virtual machine across all its virtual network adapters. |

**NOTE**

Counters are measured over the entire interval, not sampled. For example, if the VM is idle for 9 seconds but spikes to use 50% of host CPU in the 10th second, its `vm.cpu.usage` will be recorded as 5% on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

## Usage in PowerShell

Use the Get-VM cmdlet:

```
Get-VM <Name> | Get-ClusterPerf
```

**NOTE**

The Get-VM cmdlet only returns virtual machines on the local (or specified) server, not across the cluster.

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for volumes

12/16/2020 • 2 minutes to read • Edit Online

Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes in detail the performance history collected for volumes. Performance history is available for every Cluster Shared Volume (CSV) in the cluster. However, it is not available for OS boot volumes nor any other non-CSV storage.

> **NOTE**
> It may take several minutes for collection to begin for newly created or renamed volumes.

## Series names and units

These series are collected for every eligible volume:

| SERIES | UNIT |
|---|---|
| `volume.iops.read` | per second |
| `volume.iops.write` | per second |
| `volume.iops.total` | per second |
| `volume.throughput.read` | bytes per second |
| `volume.throughput.write` | bytes per second |
| `volume.throughput.total` | bytes per second |
| `volume.latency.read` | seconds |
| `volume.latency.write` | seconds |
| `volume.latency.average` | seconds |
| `volume.size.total` | bytes |
| `volume.size.available` | bytes |

## How to interpret

| SERIES | HOW TO INTERPRET |
|---|---|
| `volume.iops.read` | Number of read operations per second completed by this volume. |

| SERIES | HOW TO INTERPRET |
| --- | --- |
| `volume.iops.write` | Number of write operations per second completed by this volume. |
| `volume.iops.total` | Total number of read or write operations per second completed by this volume. |
| `volume.throughput.read` | Quantity of data read from this volume per second. |
| `volume.throughput.write` | Quantity of data written to this volume per second. |
| `volume.throughput.total` | Total quantity of data read from or written to this volume per second. |
| `volume.latency.read` | Average latency of read operations from this volume. |
| `volume.latency.write` | Average latency of write operations to this volume. |
| `volume.latency.average` | Average latency of all operations to or from this volume. |
| `volume.size.total` | The total storage capacity of the volume. |
| `volume.size.available` | The available storage capacity of the volume. |

## Where they come from

The `iops.*`, `throughput.*`, and `latency.*` series are collected from the `Cluster CSVFS` performance counter set. Every server in the cluster has an instance for every CSV volume, regardless of ownership. The performance history recorded for volume `MyVolume` is the aggregate of the `MyVolume` instances on every server in the cluster.

| SERIES | SOURCE COUNTER |
| --- | --- |
| `volume.iops.read` | `Reads/sec` |
| `volume.iops.write` | `Writes/sec` |
| `volume.iops.total` | *sum of the above* |
| `volume.throughput.read` | `Read bytes/sec` |
| `volume.throughput.write` | `Write bytes/sec` |
| `volume.throughput.total` | *sum of the above* |
| `volume.latency.read` | `Avg. sec/Read` |
| `volume.latency.write` | `Avg. sec/Write` |
| `volume.latency.average` | *average of the above* |

> **NOTE**
>
> Counters are measured over the entire interval, not sampled. For example, if the volume is idle for 9 seconds but completes 30 IOs in the 10th second, its `volume.iops.total` will be recorded as 3 IOs per second on average during this 10-second interval. This ensures its performance history captures all activity and is robust to noise.

> **TIP**
>
> These are the same counters used by the popular VM Fleet benchmark framework.

The `size.*` series are collected from the `MSFT_Volume` class in WMI, one instance per volume.

| SERIES | SOURCE PROPERTY |
| --- | --- |
| `volume.size.total` | `Size` |
| `volume.size.available` | `SizeRemaining` |

## Usage in PowerShell

Use the Get-Volume cmdlet:

```
Get-Volume -FriendlyName <FriendlyName> | Get-ClusterPerf
```

## Additional References

- Performance history for Storage Spaces Direct

# Performance history for clusters

12/16/2020 • 2 minutes to read • Edit Online

> Applies to: Windows Server 2019

This sub-topic of Performance history for Storage Spaces Direct describes the performance history collected for clusters.

There are no series that originate at the cluster level. Instead, server series, such as `clusternode.cpu.usage`, are aggregated for all servers in the cluster. Volume series, such as `volume.iops.total`, are aggregated for all volumes in the cluster. And drive series, such as `physicaldisk.size.total`, are aggregated for all drives in the cluster.

## Usage in PowerShell

Use the Get-Cluster cmdlet:

```
Get-Cluster | Get-ClusterPerf
```

## Additional References

- Performance history for Storage Spaces Direct

# Scripting with PowerShell and Storage Spaces Direct performance history

12/16/2020 • 13 minutes to read • Edit Online

> Applies to: Windows Server 2019

In Windows Server 2019, Storage Spaces Direct records and stores extensive performance history for virtual machines, servers, drives, volumes, network adapters, and more. Performance history is easy to query and process in PowerShell so you can quickly go from *raw data* to *actual answers* to questions like:

1. Were there any CPU spikes last week?
2. Is any physical disk exhibiting abnormal latency?
3. Which VMs are consuming the most storage IOPS right now?
4. Is my network bandwidth saturated?
5. When will this volume run out of free space?
6. In the past month, which VMs used the most memory?

The `Get-ClusterPerf` cmdlet is built for scripting. It accepts input from cmdlets like `Get-VM` or `Get-PhysicalDisk` by the pipeline to handle association, and you can pipe its output into utility cmdlets like `Sort-Object`, `Where-Object`, and `Measure-Object` to quickly compose powerful queries.

**This topic provides and explains 6 sample scripts that answer the 6 questions above.** They present patterns you can apply to find peaks, find averages, plot trend lines, run outlier detection, and more, across a variety of data and timeframes. They are provided as free starter code for you to copy, extend, and reuse.

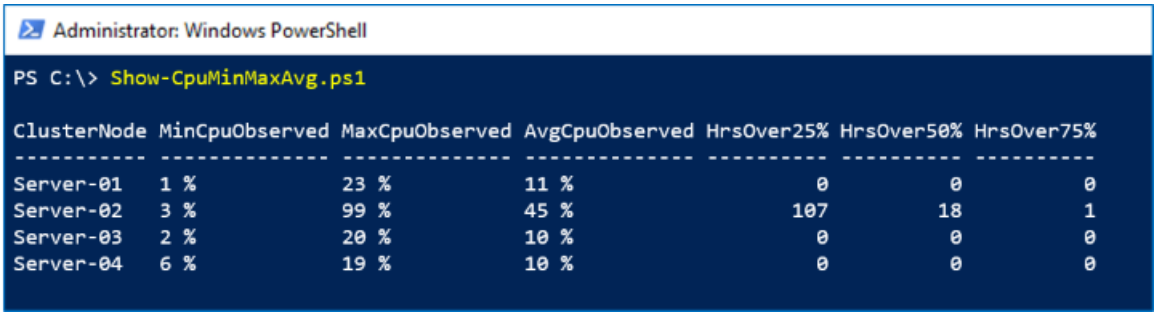
> **NOTE**
> For brevity, the sample scripts omit things like error handling that you might expect of high-quality PowerShell code. They are intended primarily for inspiration and education rather than production use.

## Sample 1: CPU, I see you!

This sample uses the `ClusterNode.Cpu.Usage` series from the `LastWeek` timeframe to show the maximum ("high water mark"), minimum, and average CPU usage for every server in the cluster. It also does simple quartile analysis to show how many hours CPU usage was over 25%, 50%, and 75% in the last 8 days.

### Screenshot

In the screenshot below, we see that *Server-02* had an unexplained spike last week:




### How it works

The output from `Get-ClusterPerf` pipes nicely into the built-in `Measure-Object` cmdlet, we just specify the `Value` property. With its `-Maximum`, `-Minimum`, and `-Average` flags, `Measure-Object` gives us the first three columns almost for free. To do the quartile analysis, we can pipe to `Where-Object` and count how many values were `-Gt` (greater than) 25, 50, or 75. The last step is to beautify with `Format-Hours` and `Format-Percent` helper functions – certainly optional.

**Script**

Here's the script:

```
Function Format-Hours {
    Param (
        $RawValue
    )
    # Weekly timeframe has frequency 15 minutes = 4 points per hour
    [Math]::Round($RawValue/4)
}

Function Format-Percent {
    Param (
        $RawValue
    )
    [String][Math]::Round($RawValue) + " " + "%"
}

$Output = Get-ClusterNode | ForEach-Object {
    $Data = $_ | Get-ClusterPerf -ClusterNodeSeriesName "ClusterNode.Cpu.Usage" -TimeFrame "LastWeek"

    $Measure = $Data | Measure-Object -Property Value -Minimum -Maximum -Average
    $Min = $Measure.Minimum
    $Max = $Measure.Maximum
    $Avg = $Measure.Average

    [PsCustomObject]@{
        "ClusterNode"    = $_.Name
        "MinCpuObserved" = Format-Percent $Min
        "MaxCpuObserved" = Format-Percent $Max
        "AvgCpuObserved" = Format-Percent $Avg
        "HrsOver25%"     = Format-Hours ($Data | Where-Object Value -Gt 25).Length
        "HrsOver50%"     = Format-Hours ($Data | Where-Object Value -Gt 50).Length
        "HrsOver75%"     = Format-Hours ($Data | Where-Object Value -Gt 75).Length
    }
}

$Output | Sort-Object ClusterNode | Format-Table
```

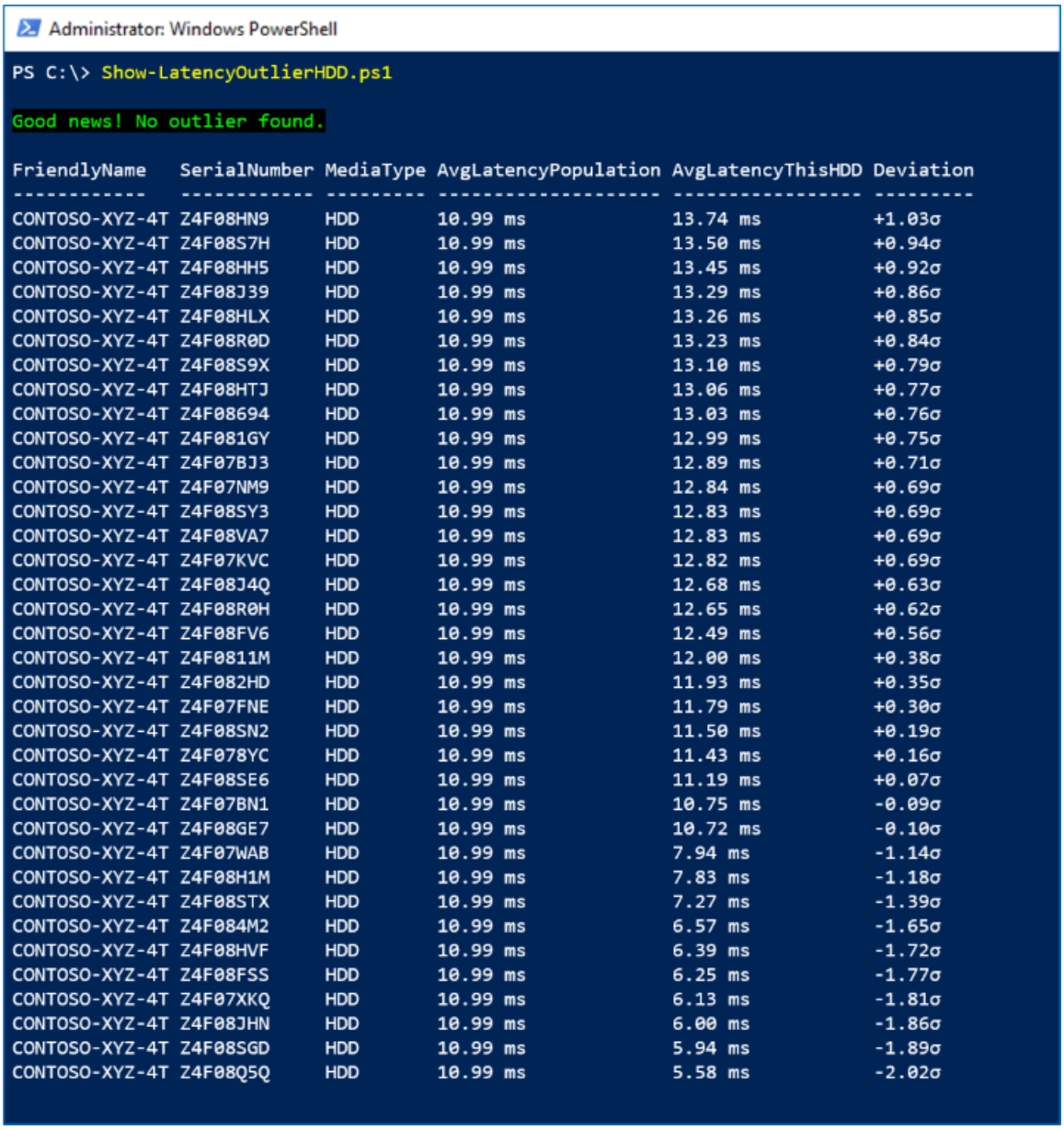
## Sample 2: Fire, fire, latency outlier

This sample uses the `PhysicalDisk.Latency.Average` series from the `LastHour` timeframe to look for statistical outliers, defined as drives with an hourly average latency exceeding +3σ (three standard deviations) above the population average.

> **IMPORTANT**
> For brevity, this script does not implement safeguards against low variance, does not handle partial missing data, does not distinguish by model or firmware, etc. Please exercise good judgement and do not rely on this script alone to determine whether to replace a hard disk. It is presented here for educational purposes only.

**Screenshot**

In the screenshot below, we see there are no outliers:




### How it works

First, we exclude idle or nearly idle drives by checking that `PhysicalDisk.Iops.Total` is consistently `-Gt 1`. For every active HDD, we pipe its `LastHour` timeframe, comprised of 360 measurements at 10 second intervals, to `Measure-Object -Average` to obtain its average latency in the last hour. This sets up our population.

We implement the widely-known formula to find the mean `μ` and standard deviation `σ` of the population. For every active HDD, we compare its average latency to the population average and divide by the standard deviation. We keep the raw values, so we can `Sort-Object` our results, but use `Format-Latency` and `Format-StandardDeviation` helper functions to beautify what we'll show – certainly optional.

If any drive is more than +3σ, we `Write-Host` in red; if not, in green.

### Script

Here's the script:

```
Function Format-Latency {
    Param (
        $RawValue
    )
    $i = 0 ; $Labels = ("s", "ms", "µs", "ns") # Petabits, just in case!
    Do { $RawValue *= 1000 ; $i++ } While ( $RawValue -Lt 1 )
    # Return
    [String][Math]::Round($RawValue, 2) + " " + $Labels[$i]
}
```

```
}

Function Format-StandardDeviation {
    Param (
        $RawValue
    )
    If ($RawValue -Gt 0) {
        $Sign = "+"
    }
    Else {
        $Sign = "-"
    }
    # Return
    $Sign + [String][Math]::Round([Math]::Abs($RawValue), 2) + "σ"
}

$HDD = Get-StorageSubSystem Cluster* | Get-PhysicalDisk | Where-Object MediaType -Eq HDD

$Output = $HDD | ForEach-Object {

    $Iops = $_ | Get-ClusterPerf -PhysicalDiskSeriesName "PhysicalDisk.Iops.Total" -TimeFrame "LastHour"
    $AvgIops = ($Iops | Measure-Object -Property Value -Average).Average

    If ($AvgIops -Gt 1) { # Exclude idle or nearly idle drives

        $Latency = $_ | Get-ClusterPerf -PhysicalDiskSeriesName "PhysicalDisk.Latency.Average" -TimeFrame
"LastHour"
        $AvgLatency = ($Latency | Measure-Object -Property Value -Average).Average

        [PsCustomObject]@{
            "FriendlyName"  = $_.FriendlyName
            "SerialNumber"  = $_.SerialNumber
            "MediaType"     = $_.MediaType
            "AvgLatencyPopulation" = $null # Set below
            "AvgLatencyThisHDD"    = Format-Latency $AvgLatency
            "RawAvgLatencyThisHDD" = $AvgLatency
            "Deviation"            = $null # Set below
            "RawDeviation"         = $null # Set below
        }
    }
}

If ($Output.Length -Ge 3) { # Minimum population requirement

    # Find mean μ and standard deviation σ
    $μ = ($Output | Measure-Object -Property RawAvgLatencyThisHDD -Average).Average
    $d = $Output | ForEach-Object { ($_.RawAvgLatencyThisHDD - $μ) * ($_.RawAvgLatencyThisHDD - $μ) }
    $σ = [Math]::Sqrt(($d | Measure-Object -Sum).Sum / $Output.Length)

    $FoundOutlier = $False

    $Output | ForEach-Object {
        $Deviation = ($_.RawAvgLatencyThisHDD - $μ) / $σ
        $_.AvgLatencyPopulation = Format-Latency $μ
        $_.Deviation = Format-StandardDeviation $Deviation
        $_.RawDeviation = $Deviation
        # If distribution is Normal, expect >99% within 3σ
        If ($Deviation -Gt 3) {
            $FoundOutlier = $True
        }
    }

    If ($FoundOutlier) {
        Write-Host -BackgroundColor Black -ForegroundColor Red "Oh no! There's an HDD significantly slower
than the others."
    }
    Else {
        Write-Host -BackgroundColor Black -ForegroundColor Green "Good news! No outlier found."
    }
```

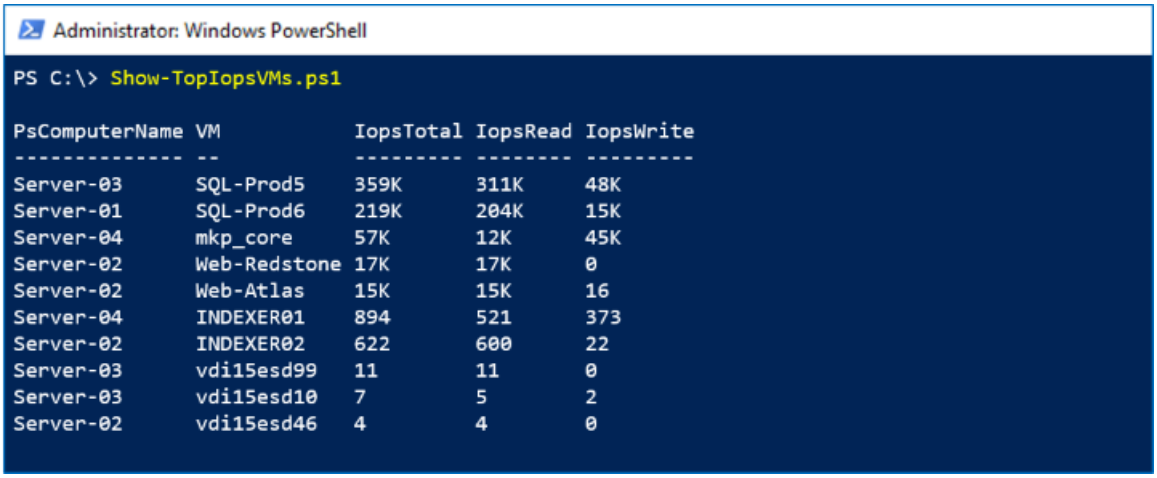
```
    $Output | Sort-Object RawDeviation -Descending | Format-Table FriendlyName, SerialNumber, MediaType,
AvgLatencyPopulation, AvgLatencyThisHDD, Deviation

}
Else {
    Write-Warning "There aren't enough active drives to look for outliers right now."
}
```

## Sample 3: Noisy neighbor? That's write!

Performance history can answer questions about *right now*, too. New measurements are available in real-time, every 10 seconds. This sample uses the `VHD.Iops.Total` series from the `MostRecent` timeframe to identify the busiest (some might say "noisiest") virtual machines consuming the most storage IOPS, across every host in the cluster, and show the read/write breakdown of their activity.

### Screenshot

In the screenshot below, we see the Top 10 virtual machines by storage activity:




### How it works

Unlike `Get-PhysicalDisk`, the `Get-VM` cmdlet isn't cluster-aware – it only returns VMs on the local server. To query from every server in parallel, we wrap our call in `Invoke-Command (Get-ClusterNode).Name { ... }`. For every VM, we get the `VHD.Iops.Total`, `VHD.Iops.Read`, and `VHD.Iops.Write` measurements. By not specifying the `-TimeFrame` parameter, we get the `MostRecent` single data point for each.

> **TIP**
>
> These series reflect the sum of this VM's activity to all its VHD/VHDX files. This is an example where performance history is being automatically aggregated for us. To get the per-VHD/VHDX breakdown, you could pipe an individual `Get-VHD` into `Get-ClusterPerf` instead of the VM.

The results from every server come together as `$Output`, which we can `Sort-Object` and then `Select-Object -First 10`. Notice that `Invoke-Command` decorates results with a `PsComputerName` property indicating where they came from, which we can print to know where the VM is running.

### Script

Here's the script:

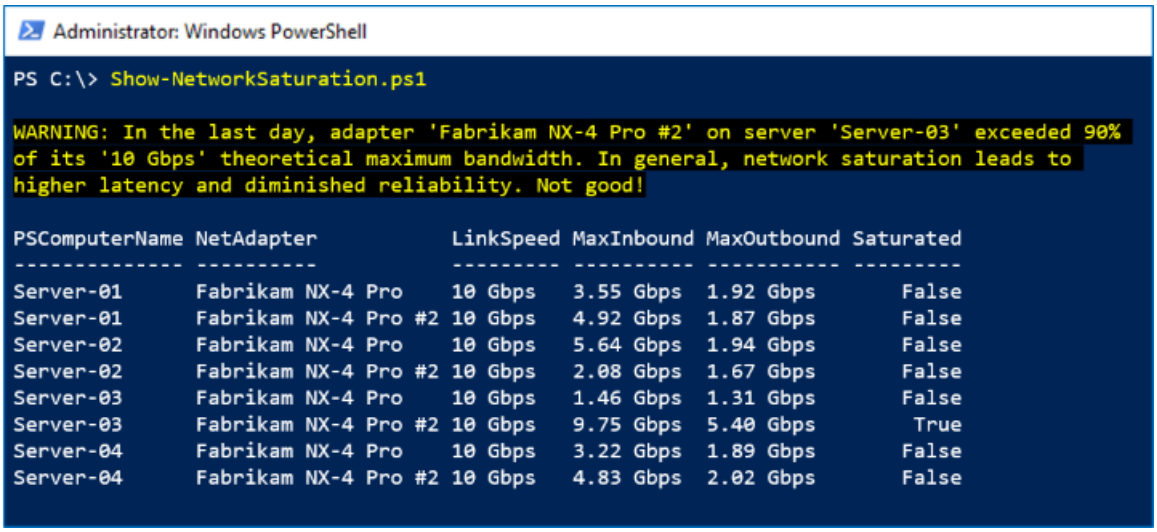
```
$Output = Invoke-Command (Get-ClusterNode).Name {
    Function Format-Iops {
        Param (
            $RawValue
        )
        $i = 0 ; $Labels = (" ", "K", "M", "B", "T") # Thousands, millions, billions, trillions...
        Do { if($RawValue -Gt 1000){$RawValue /= 1000 ; $i++ } } While ( $RawValue -Gt 1000 )
        # Return
        [String][Math]::Round($RawValue) + " " + $Labels[$i]
    }

    Get-VM | ForEach-Object {
        $IopsTotal = $_ | Get-ClusterPerf -VMSeriesName "VHD.Iops.Total"
        $IopsRead  = $_ | Get-ClusterPerf -VMSeriesName "VHD.Iops.Read"
        $IopsWrite = $_ | Get-ClusterPerf -VMSeriesName "VHD.Iops.Write"
        [PsCustomObject]@{
            "VM" = $_.Name
            "IopsTotal" = Format-Iops $IopsTotal.Value
            "IopsRead"  = Format-Iops $IopsRead.Value
            "IopsWrite" = Format-Iops $IopsWrite.Value
            "RawIopsTotal" = $IopsTotal.Value # For sorting...
        }
    }
}

$Output | Sort-Object RawIopsTotal -Descending | Select-Object -First 10 | Format-Table PsComputerName, VM,
IopsTotal, IopsRead, IopsWrite
```

# Sample 4: As they say, "25-gig is the new 10-gig"

This sample uses the `NetAdapter.Bandwidth.Total` series from the `LastDay` timeframe to look for signs of network saturation, defined as >90% of theoretical maximum bandwidth. For every network adapter in the cluster, it compares the highest observed bandwidth usage in the last day to its stated link speed.

### Screenshot

In the screenshot below, we see that one *Fabrikam NX-4 Pro #2* peaked in the last day:




### How it works

We repeat our `Invoke-Command` trick from above to `Get-NetAdapter` on every server and pipe into `Get-ClusterPerf`. Along the way, we grab two relevant properties: its `LinkSpeed` string like "10 Gbps", and its raw `Speed` integer like 10000000000. We use `Measure-Object` to obtain the average and peak from the last day (reminder: each measurement in the `LastDay` timeframe represents 5 minutes) and multiply by 8 bits per byte to get an apples-to-apples comparison.

> **NOTE**
>
> Some vendors, like Chelsio, include remote-direct memory access (RDMA) activity in their *Network Adapter* performance counters, so it's included in the `NetAdapter.Bandwidth.Total` series. Others, like Mellanox, may not. If your vendor doesn't, simply add the `NetAdapter.Bandwidth.RDMA.Total` series in your version of this script.

### Script

Here's the script:

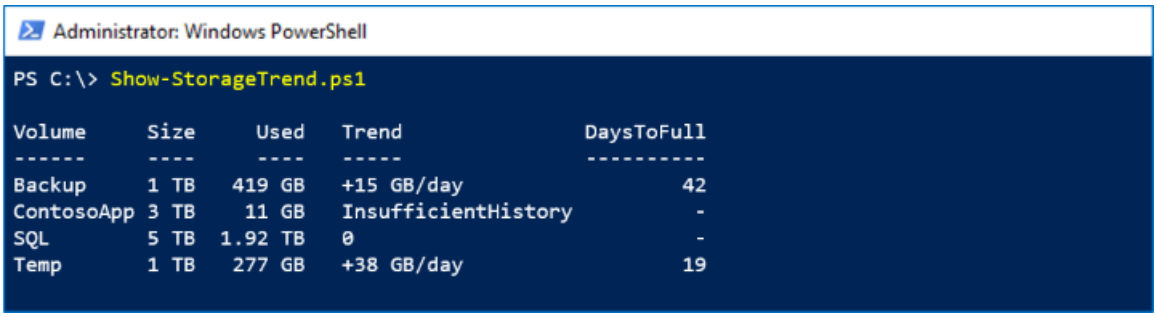
```
$Output = Invoke-Command (Get-ClusterNode).Name {

    Function Format-BitsPerSec {
        Param (
            $RawValue
        )
        $i = 0 ; $Labels = ("bps", "kbps", "Mbps", "Gbps", "Tbps", "Pbps") # Petabits, just in case!
        Do { $RawValue /= 1000 ; $i++ } While ( $RawValue -Gt 1000 )
        # Return
        [String][Math]::Round($RawValue) + " " + $Labels[$i]
    }

    Get-NetAdapter | ForEach-Object {

        $Inbound = $_ | Get-ClusterPerf -NetAdapterSeriesName "NetAdapter.Bandwidth.Inbound" -TimeFrame
"LastDay"
        $Outbound = $_ | Get-ClusterPerf -NetAdapterSeriesName "NetAdapter.Bandwidth.Outbound" -TimeFrame
"LastDay"

        If ($Inbound -Or $Outbound) {

            $InterfaceDescription = $_.InterfaceDescription
            $LinkSpeed = $_.LinkSpeed

            $MeasureInbound = $Inbound | Measure-Object -Property Value -Maximum
            $MaxInbound = $MeasureInbound.Maximum * 8 # Multiply to bits/sec

            $MeasureOutbound = $Outbound | Measure-Object -Property Value -Maximum
            $MaxOutbound = $MeasureOutbound.Maximum * 8 # Multiply to bits/sec

            $Saturated = $False

            # Speed property is Int, e.g. 10000000000
            If (($MaxInbound -Gt (0.90 * $_.Speed)) -Or ($MaxOutbound -Gt (0.90 * $_.Speed))) {
                $Saturated = $True
                Write-Warning "In the last day, adapter '$InterfaceDescription' on server '$Env:ComputerName'
exceeded 90% of its '$LinkSpeed' theoretical maximum bandwidth. In general, network saturation leads to higher
latency and diminished reliability. Not good!"
            }

            [PsCustomObject]@{
                "NetAdapter"  = $InterfaceDescription
                "LinkSpeed"   = $LinkSpeed
                "MaxInbound"  = Format-BitsPerSec $MaxInbound
                "MaxOutbound" = Format-BitsPerSec $MaxOutbound
                "Saturated"   = $Saturated
            }
        }
    }
}

$Output | Sort-Object PsComputerName, InterfaceDescription | Format-Table PsComputerName, NetAdapter,
LinkSpeed, MaxInbound, MaxOutbound, Saturated
```

# Sample 5: Make storage trendy again!

To look at macro trends, performance history is retained for up to 1 year. This sample uses the `Volume.Size.Available` series from the `LastYear` timeframe to determine the rate that storage is filling up and estimate when it will be full.

### Screenshot

In the screenshot below, we see the *Backup* volume is adding about 15 GB per day:




At this rate, it will reach its capacity in another 42 days.

### How it works

The `LastYear` timeframe has one data point per day. Although you only strictly need two points to fit a trend line, in practice it's better to require more, like 14 days. We use `Select-Object -Last 14` to set up an array of *(x, y)* points, for *x* in the range [1, 14]. With these points, we implement the straightforward linear least squares algorithm to find `$A` and `$B` that parameterize the line of best fit $y = ax + b$. Welcome to high school all over again.

Dividing the volume's `SizeRemaining` property by the trend (the slope `$A`) lets us crudely estimate how many days, at the current rate of storage growth, until the volume is full. The `Format-Bytes`, `Format-Trend`, and `Format-Days` helper functions beautify the output.

> **IMPORTANT**
> This estimate is linear and based only on the most recent 14 daily measurements. More sophisticated and accurate techniques exist. Please exercise good judgement and do not rely on this script alone to determine whether to invest in expanding your storage. It is presented here for educational purposes only.

### Script

Here's the script:

```
Function Format-Bytes {
    Param (
        $RawValue
    )
    $i = 0 ; $Labels = ("B", "KB", "MB", "GB", "TB", "PB", "EB", "ZB", "YB")
    Do { $RawValue /= 1024 ; $i++ } While ( $RawValue -Gt 1024 )
    # Return
    [String][Math]::Round($RawValue) + " " + $Labels[$i]
}

Function Format-Trend {
    Param (
        $RawValue
    )
    If ($RawValue -Eq 0) {
        "0"
    }
```

```
    Else {
        If ($RawValue -Gt 0) {
            $Sign = "+"
        }
        Else {
            $Sign = "-"
        }
        # Return
        $Sign + $(Format-Bytes [Math]::Abs($RawValue)) + "/day"
    }
}

Function Format-Days {
    Param (
        $RawValue
    )
    [Math]::Round($RawValue)
}

$CSV = Get-Volume | Where-Object FileSystem -Like "*CSV*"

$Output = $CSV | ForEach-Object {

    $N = 14 # Require 14 days of history

    $Data = $_ | Get-ClusterPerf -VolumeSeriesName "Volume.Size.Available" -TimeFrame "LastYear" | Sort-Object
Time | Select-Object -Last $N

    If ($Data.Length -Ge $N) {

        # Last N days as (x, y) points
        $PointsXY = @()
        1..$N | ForEach-Object {
            $PointsXY += [PsCustomObject]@{ "X" = $_ ; "Y" = $Data[$_-1].Value }
        }

        # Linear (y = ax + b) least squares algorithm
        $MeanX = ($PointsXY | Measure-Object -Property X -Average).Average
        $MeanY = ($PointsXY | Measure-Object -Property Y -Average).Average
        $XX = $PointsXY | ForEach-Object { $_.X * $_.X }
        $XY = $PointsXY | ForEach-Object { $_.X * $_.Y }
        $SSXX = ($XX | Measure-Object -Sum).Sum - $N * $MeanX * $MeanX
        $SSXY = ($XY | Measure-Object -Sum).Sum - $N * $MeanX * $MeanY
        $A = ($SSXY / $SSXX)
        $B = ($MeanY - $A * $MeanX)
        $RawTrend = -$A # Flip to get daily increase in Used (vs decrease in Remaining)
        $Trend = Format-Trend $RawTrend

        If ($RawTrend -Gt 0) {
            $DaysToFull = Format-Days ($_.SizeRemaining / $RawTrend)
        }
        Else {
            $DaysToFull = "-"
        }
    }
    Else {
        $Trend = "InsufficientHistory"
        $DaysToFull = "-"
    }

    [PsCustomObject]@{
        "Volume"     = $_.FileSystemLabel
        "Size"       = Format-Bytes ($_.Size)
        "Used"       = Format-Bytes ($_.Size - $_.SizeRemaining)
        "Trend"      = $Trend
        "DaysToFull" = $DaysToFull
    }
}
```

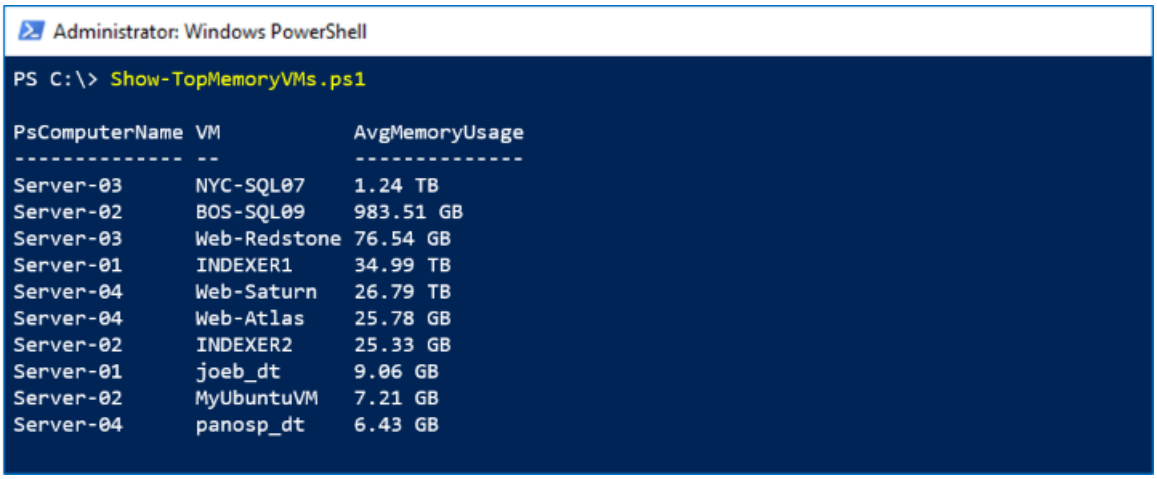
```
$Output | Format-Table
```

# Sample 6: Memory hog, you can run but you can't hide

Because performance history is collected and stored centrally for the whole cluster, you never need to stitch together data from different machines, no matter how many times VMs move between hosts. This sample uses the `VM.Memory.Assigned` series from the `LastMonth` timeframe to identify the virtual machines consuming the most memory over the last 35 days.

### Screenshot

In the screenshot below, we see the Top 10 virtual machines by memory usage last month:




### How it works

We repeat our `Invoke-Command` trick, introduced above, to `Get-VM` on every server. We use `Measure-Object -Average` to obtain the monthly average for every VM, then `Sort-Object` followed by `Select-Object -First 10` to obtain our leaderboard. (Or maybe it's our *Most Wanted* list?)

### Script

Here's the script:

```
$Output = Invoke-Command (Get-ClusterNode).Name {
    Function Format-Bytes {
        Param (
            $RawValue
        )
        $i = 0 ; $Labels = ("B", "KB", "MB", "GB", "TB", "PB", "EB", "ZB", "YB")
        Do { if( $RawValue -Gt 1024 ){ $RawValue /= 1024 ; $i++ } } While ( $RawValue -Gt 1024 )
        # Return
        [String][Math]::Round($RawValue) + " " + $Labels[$i]
    }

    Get-VM | ForEach-Object {
        $Data = $_ | Get-ClusterPerf -VMSeriesName "VM.Memory.Assigned" -TimeFrame "LastMonth"
        If ($Data) {
            $AvgMemoryUsage = ($Data | Measure-Object -Property Value -Average).Average
            [PsCustomObject]@{
                "VM" = $_.Name
                "AvgMemoryUsage" = Format-Bytes $AvgMemoryUsage.Value
                "RawAvgMemoryUsage" = $AvgMemoryUsage.Value # For sorting...
            }
        }
    }
}

$Output | Sort-Object RawAvgMemoryUsage -Descending | Select-Object -First 10 | Format-Table PsComputerName,
VM, AvgMemoryUsage
```

That's it! Hopefully these samples inspire you and help you get started. With Storage Spaces Direct performance history and the powerful, scripting-friendly `Get-ClusterPerf` cmdlet, you are empowered to ask – and answer! – complex questions as you manage and monitor your Windows Server 2019 infrastructure.

## Additional References

- Getting started with Windows PowerShell
- Storage Spaces Direct overview
- Performance history

# Delimit the allocation of volumes in Storage Spaces Direct

12/16/2020 • 9 minutes to read • Edit Online

Applies to: Windows Server 2019

Windows Server 2019 introduces an option to manually delimit the allocation of volumes in Storage Spaces Direct. Doing so can significantly increase fault tolerance under certain conditions, but imposes some added management considerations and complexity. This topic explains how it works and gives examples in PowerShell.

> **IMPORTANT**
> This feature is new in Windows Server 2019. It is not available in Windows Server 2016.

## Prerequisites

**Consider using this option if:**

- Your cluster has six or more servers; and
- Your cluster uses only three-way mirror resiliency

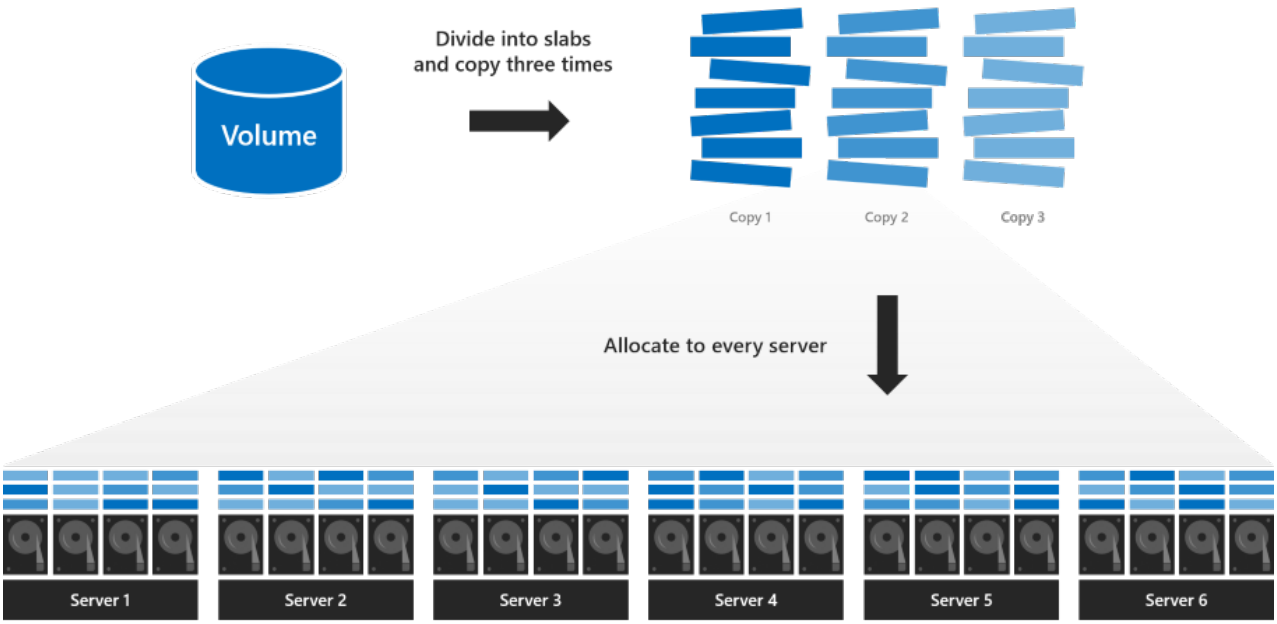
**Do not use this option if:**

- Your cluster has fewer than six servers; or
- Your cluster uses parity or mirror-accelerated parity resiliency

## Understand

### Review: regular allocation

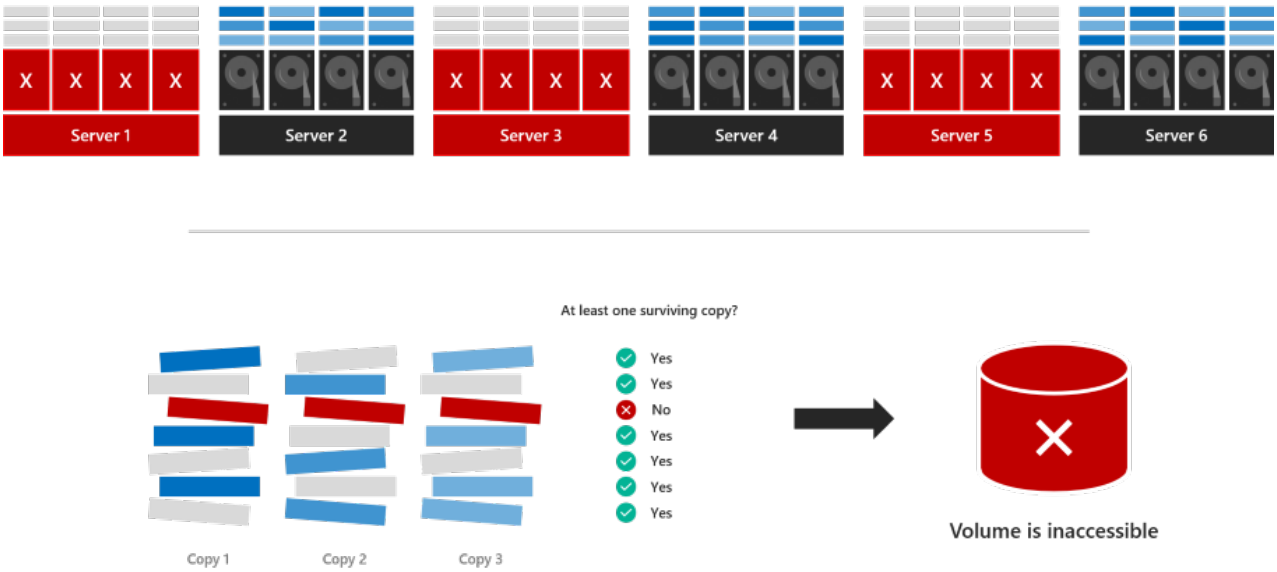
With regular three-way mirroring, the volume is divided into many small "slabs" that are copied three times and distributed evenly across every drive in every server in the cluster. For more details, read this deep dive blog.




This default allocation maximizes parallel reads and writes, leading to better performance, and is appealing in its simplicity: every server is equally busy, every drive is equally full, and all volumes stay online or go offline together. Every volume is guaranteed to survive up to two concurrent failures, as these examples illustrate.

However, with this allocation, volumes can't survive three concurrent failures. If three servers fail at once, or if drives in three servers fail at once, volumes become inaccessible because at least some slabs were (with very high probability) allocated to the exact three drives or servers that failed.

In the example below, servers 1, 3, and 5 fail at the same time. Although many slabs have surviving copies, some do not:




The volume goes offline and becomes inaccessible until the servers are recovered.

**New: delimited allocation**

With delimited allocation, you specify a subset of servers to use (minimum four). The volume is divided into slabs that are copied three times, like before, but instead of allocating across every server, **the slabs are allocated only to the subset of servers you specify**.

For example, if you have an 8 node cluster (nodes 1 through 8), you can specify a volume to be located only on disks in nodes 1, 2, 3, 4.

#### Advantages

With the example allocation, the volume is likely to survive three concurrent failures. If nodes 1, 2, and 6 go down, only 2 of the nodes that hold the 3 copies of data for the volume are down and the volume will stay online.

Survival probability depends on the number of servers and other factors – see Analysis for details.

#### Disadvantages

Delimited allocation imposes some added management considerations and complexity:

1. The administrator is responsible for delimiting the allocation of each volume to balance storage utilization across servers and uphold high probability of survival, as described in the Best practices section.
2. With delimited allocation, reserve the equivalent of **one capacity drive per server (with no maximum)**. This is more than the published recommendation for regular allocation, which maxes out at four capacity drives total.
3. If a server fails and needs to be replaced, as described in Remove a server and its drives, the administrator is responsible for updating the delimitation of affected volumes by adding the new server and removing the failed one – example below.

## Usage in PowerShell

You can use the `New-Volume` cmdlet to create volumes in Storage Spaces Direct.

For example, to create a regular three-way mirror volume:

```
New-Volume -FriendlyName "MyRegularVolume" -Size 100GB
```

### Create a volume and delimit its allocation

To create a three-way mirror volume and delimit its allocation:

1. First assign the servers in your cluster to the variable `$Servers`:

   ```
   $Servers = Get-StorageFaultDomain -Type StorageScaleUnit | Sort FriendlyName
   ```

   > **TIP**
   > In Storage Spaces Direct, the term 'Storage Scale Unit' refers to all the raw storage attached to one server, including direct-attached drives and direct-attached external enclosures with drives. In this context, it's the same as 'server'.

2. Specify which servers to use with the new `-StorageFaultDomainsToUse` parameter and by indexing into `$Servers`. For example, to delimit the allocation to the first, second, third, and fourth servers (indices 0, 1, 2, and 3):

   ```
   New-Volume -FriendlyName "MyVolume" -Size 100GB -StorageFaultDomainsToUse $Servers[0,1,2,3]
   ```

### See a delimited allocation

To see how *MyVolume* is allocated, use the `Get-VirtualDiskFootprintBySSU.ps1` script in Appendix:

```
PS C:\> .\Get-VirtualDiskFootprintBySSU.ps1

VirtualDiskFriendlyName TotalFootprint Server1 Server2 Server3 Server4 Server5 Server6
----------------------- -------------- ------- ------- ------- ------- ------- -------
MyVolume                300 GB         100 GB  100 GB  100 GB  100 GB  0       0
```

Note that only Server1, Server2, Server3, and Server4 contain slabs of *MyVolume*.

#### Change a delimited allocation

Use the new `Add-StorageFaultDomain` and `Remove-StorageFaultDomain` cmdlets to change how the allocation is delimited.

For example, to move *MyVolume* over by one server:

1. Specify that the fifth server **can** store slabs of *MyVolume*:

   ```
   Get-VirtualDisk MyVolume | Add-StorageFaultDomain -StorageFaultDomains $Servers[4]
   ```

2. Specify that the first server **cannot** store slabs of *MyVolume*:

   ```
   Get-VirtualDisk MyVolume | Remove-StorageFaultDomain -StorageFaultDomains $Servers[0]
   ```

3. Rebalance the storage pool for the change to take effect:

   ```
   Get-StoragePool S2D* | Optimize-StoragePool
   ```

You can monitor the progress of the rebalance with `Get-StorageJob`.

Once it is complete, verify that *MyVolume* has moved by running `Get-VirtualDiskFootprintBySSU.ps1` again.

```
PS C:\> .\Get-VirtualDiskFootprintBySSU.ps1

VirtualDiskFriendlyName TotalFootprint Server1 Server2 Server3 Server4 Server5 Server6
----------------------- -------------- ------- ------- ------- ------- ------- -------
MyVolume                300 GB         0       100 GB  100 GB  100 GB  100 GB  0
```

Note that Server1 does not contain slabs of *MyVolume* anymore – instead, Server5 does.

## Best practices

Here are the best practices to follow when using delimited volume allocation:

#### Choose four servers

Delimit each three-way mirror volume to four servers, not more.

#### Balance storage

Balance how much storage is allocated to each server, accounting for volume size.

#### Stagger delimited allocation volumes

To maximize fault tolerance, make each volume's allocation unique, meaning it does not share *all* its servers with another volume (some overlap is okay).

For example on an eight-node system: Volume 1: Servers 1, 2, 3, 4 Volume 2: Servers 5, 6, 7, 8 Volume 3: Servers 3, 4, 5, 6 Volume 4: Servers 1, 2, 7, 8

# Analysis

This section derives the mathematical probability that a volume stays online and accessible (or equivalently, the expected fraction of overall storage that stays online and accessible) as a function of the number of failures and the cluster size.

> **NOTE**
>
> This section is optional reading. If you're keen to see the math, read on! But if not, don't worry: Usage in PowerShell and Best practices is all you need to implement delimited allocation successfully.

#### Up to two failures is always okay

Every three-way mirror volume can survive up to two failures at the same time, regardless of its allocation. If two drives fail, or two servers fail, or one of each, every three-way mirror volume stays online and accessible, even with regular allocation.

#### More than half the cluster failing is never okay

Conversely, in the extreme case that more than half of servers or drives in the cluster fail at once, quorum is lost and every three-way mirror volume goes offline and becomes inaccessible, regardless of its allocation.

#### What about in between?

If three or more failures occur at once, but at least half of the servers and the drives are still up, volumes with delimited allocation may stay online and accessible, depending on which servers have failures.

# Frequently asked questions

#### Can I delimit some volumes but not others?

Yes. You can choose per-volume whether or not to delimit allocation.

#### Does delimited allocation change how drive replacement works?

No, it's the same as with regular allocation.

# Additional References

- Storage Spaces Direct overview
- Fault tolerance in Storage Spaces Direct

# Appendix

This script helps you see how your volumes are allocated.

To use it as described above, copy/paste and save as `Get-VirtualDiskFootprintBySSU.ps1`.

```
Function ConvertTo-PrettyCapacity {
    Param (
        [Parameter(
            Mandatory = $True,
            ValueFromPipeline = $True
            )
        ]
    [Int64]$Bytes,
    [Int64]$RoundTo = 0
    )
    If ($Bytes -Gt 0) {
        $Base = 1024
        $Labels = ("bytes", "KB", "MB", "GB", "TB", "PB", "EB", "ZB", "YB")
        $Order = [Math]::Floor( [Math]::Log($Bytes, $Base) )
```

```
        $Order = [Math]::Floor( [Math]::Log($Bytes, $Base) )
        $Rounded = [Math]::Round($Bytes/( [Math]::Pow($Base, $Order) ), $RoundTo)
        [String]($Rounded) + " " + $Labels[$Order]
    }
    Else {
        "0"
    }
    Return
}

Function Get-VirtualDiskFootprintByStorageFaultDomain {

    ###############################################
    ### Step 1: Gather Configuration Information ###
    ###############################################

    Write-Progress -Activity "Get-VirtualDiskFootprintByStorageFaultDomain" -CurrentOperation "Gathering
configuration information..." -Status "Step 1/4" -PercentComplete 00

    $ErrorCannotGetCluster = "Cannot proceed because 'Get-Cluster' failed."
    $ErrorNotS2DEnabled = "Cannot proceed because the cluster is not running Storage Spaces Direct."
    $ErrorCannotGetClusterNode = "Cannot proceed because 'Get-ClusterNode' failed."
    $ErrorClusterNodeDown = "Cannot proceed because one or more cluster nodes is not Up."
    $ErrorCannotGetStoragePool = "Cannot proceed because 'Get-StoragePool' failed."
    $ErrorPhysicalDiskFaultDomainAwareness = "Cannot proceed because the storage pool is set to 'PhysicalDisk'
fault domain awareness. This cmdlet only supports 'StorageScaleUnit', 'StorageChassis', or 'StorageRack' fault
domain awareness."

    Try  {
        $GetCluster = Get-Cluster -ErrorAction Stop
    }
    Catch {
        throw $ErrorCannotGetCluster
    }

    If ($GetCluster.S2DEnabled -Ne 1) {
        throw $ErrorNotS2DEnabled
    }

    Try  {
        $GetClusterNode = Get-ClusterNode -ErrorAction Stop
    }
    Catch {
        throw $ErrorCannotGetClusterNode
    }

    If ($GetClusterNode | Where State -Ne Up) {
        throw $ErrorClusterNodeDown
    }

    Try {
        $GetStoragePool = Get-StoragePool -IsPrimordial $False -ErrorAction Stop
    }
    Catch {
        throw $ErrorCannotGetStoragePool
    }

    If ($GetStoragePool.FaultDomainAwarenessDefault -Eq "PhysicalDisk") {
        throw $ErrorPhysicalDiskFaultDomainAwareness
    }

    ###########################################################
    ### Step 2: Create SfdList[] and PhysicalDiskToSfdMap{} ###
    ###########################################################

    Write-Progress -Activity "Get-VirtualDiskFootprintByStorageFaultDomain" -CurrentOperation "Analyzing
physical disk information..." -Status "Step 2/4" -PercentComplete 25

    $SfdList = Get-StorageFaultDomain -Type ($GetStoragePool.FaultDomainAwarenessDefault) | Sort FriendlyName
```

```
# StorageScaleUnit, StorageChassis, or StorageRack

    $PhysicalDiskToSfdMap = @{} # Map of PhysicalDisk.UniqueId -> StorageFaultDomain.FriendlyName
    $SfdList | ForEach {
        $StorageFaultDomain = $_
        $_ | Get-StorageFaultDomain -Type PhysicalDisk | ForEach {
            $PhysicalDiskToSfdMap[$_.UniqueId] = $StorageFaultDomain.FriendlyName
        }
    }

    ###############################################################################################################
    ### Step 3: Create VirtualDisk.FriendlyName -> { StorageFaultDomain.FriendlyName -> Size } Map ###
    ###############################################################################################################

    Write-Progress -Activity "Get-VirtualDiskFootprintByStorageFaultDomain" -CurrentOperation "Analyzing
virtual disk information..." -Status "Step 3/4" -PercentComplete 50

    $GetVirtualDisk = Get-VirtualDisk | Sort FriendlyName

    $VirtualDiskMap = @{}

    $GetVirtualDisk | ForEach {
        # Map of PhysicalDisk.UniqueId -> Size for THIS virtual disk
        $PhysicalDiskToSizeMap = @{}
        $_ | Get-PhysicalExtent | ForEach {
            $PhysicalDiskToSizeMap[$_.PhysicalDiskUniqueId] += $_.Size
        }
        # Map of StorageFaultDomain.FriendlyName -> Size for THIS virtual disk
        $SfdToSizeMap = @{}
        $PhysicalDiskToSizeMap.keys | ForEach {
            $SfdToSizeMap[$PhysicalDiskToSfdMap[$_]] += $PhysicalDiskToSizeMap[$_]
        }
        # Store
        $VirtualDiskMap[$_.FriendlyName] = $SfdToSizeMap
    }

    ##########################
    ### Step 4: Write-Out ###
    ##########################

    Write-Progress -Activity "Get-VirtualDiskFootprintByStorageFaultDomain" -CurrentOperation "Formatting
output..." -Status "Step 4/4" -PercentComplete 75

    $Output = $GetVirtualDisk | ForEach {
        $Row = [PsCustomObject]@{}

        $VirtualDiskFriendlyName = $_.FriendlyName
        $Row | Add-Member -MemberType NoteProperty "VirtualDiskFriendlyName" $VirtualDiskFriendlyName

        $TotalFootprint = $_.FootprintOnPool | ConvertTo-PrettyCapacity
        $Row | Add-Member -MemberType NoteProperty "TotalFootprint" $TotalFootprint

        $SfdList | ForEach {
            $Size = $VirtualDiskMap[$VirtualDiskFriendlyName][$_.FriendlyName] | ConvertTo-PrettyCapacity
            $Row | Add-Member -MemberType NoteProperty $_.FriendlyName $Size
        }

        $Row
    }

    # Calculate width, in characters, required to Format-Table
    $RequiredWindowWidth = ("TotalFootprint").length + 1 + ("VirtualDiskFriendlyName").length + 1
    $SfdList | ForEach {
        $RequiredWindowWidth += $_.FriendlyName.Length + 1
    }

    $ActualWindowWidth = (Get-Host).UI.RawUI.WindowSize.Width

    If (!($ActualWindowWidth)) {
```

```
        # Cannot get window width, probably ISE, Format-List
        Write-Warning "Could not determine window width. For the best experience, use a Powershell window
instead of ISE"
        $Output | Format-Table
    }
    ElseIf ($ActualWindowWidth -Lt $RequiredWindowWidth) {
        # Narrower window, Format-List
        Write-Warning "For the best experience, try making your PowerShell window at least
$RequiredWindowWidth characters wide. Current width is $ActualWindowWidth characters."
        $Output | Format-List
    }
    Else {
        # Wider window, Format-Table
        $Output | Format-Table
    }
}

Get-VirtualDiskFootprintByStorageFaultDomain
```

# Use Azure Monitor to send emails for Health Service Faults

11/2/2020 • 12 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

This is particularly helpful for your on-premises hyper-converged cluster. With Azure Monitor integrated, you will be able to configure email, text (SMS), and other alerts to ping you when something is wrong with your cluster (or when you want to flag some other activity based on the data collected). Below, we will briefly explain how Azure Monitor works, how to install Azure Monitor, and how to configure it to send you notifications.

If you are using System Center, check out the Storage Spaces Direct management pack that monitors both Windows Server 2019 and Windows Server 2016 Storage Spaces Direct clusters.

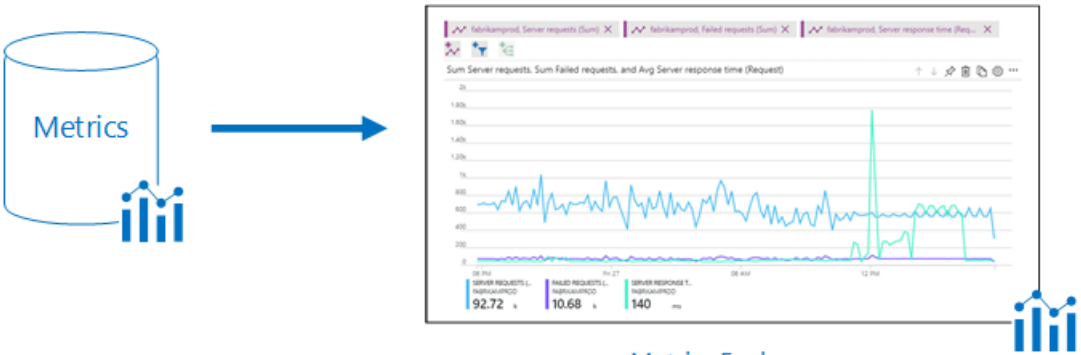
This management pack includes:

- Physical disk health and performance monitoring
- Storage Node health and performance monitoring
- Storage Pool health and performance monitoring
- Volume resiliency type and Deduplication status

## Understanding Azure Monitor

All data collected by Azure Monitor fits into one of two fundamental types: metrics and logs.

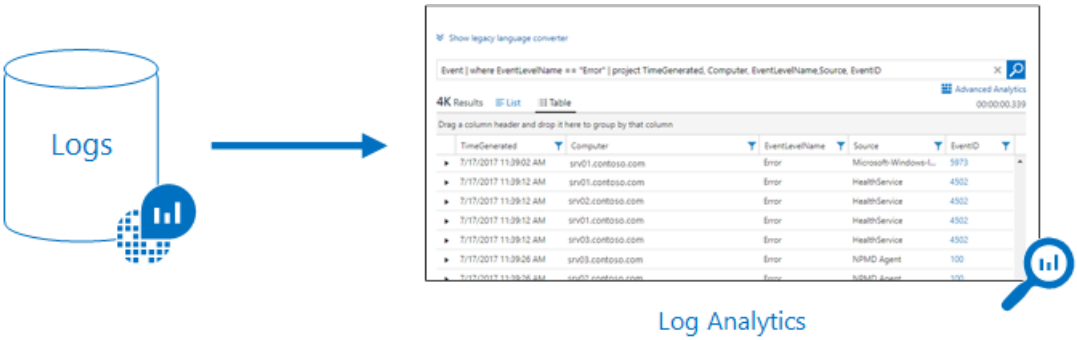
1. Metrics are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. You'll see data collected by Azure Monitor right in their Overview page in the Azure portal.




Metrics Explorer

2. Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis. Log data collected by Azure Monitor can be analyzed with queries to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using Log Analytics in the Azure portal and then either directly analyze the data using these tools or save queries for use with visualizations or alert

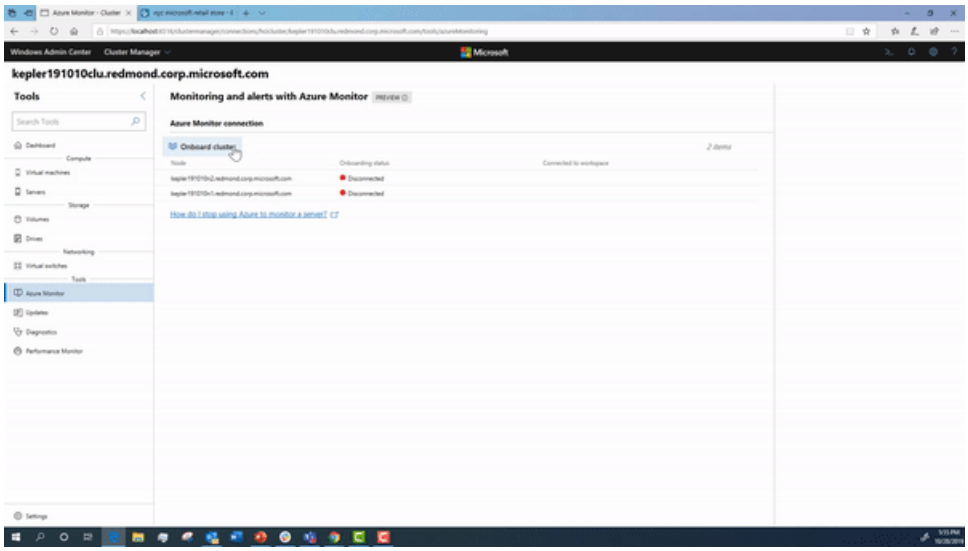
rules.




We will have more details below on how to configure these alerts.

# Onboarding your cluster using Windows Admin Center

Using Windows Admin Center, you can onboard your cluster to Azure Monitor.




During this onboarding flow, the steps below are happening under the hood. We detail how to configure them in detail in case you want to manually setup your cluster.

### Configuring Health Service

The first thing that you need to do is configure your cluster. As you may know, the Health Service improves the day-to-day monitoring and operational experience for clusters running Storage Spaces Direct.

As we saw above, Azure Monitor collects logs from each node that it is running on in your cluster. So, we have to configure the Health Service to write to an event channel, which happens to be:

```
Event Channel: Microsoft-Windows-Health/Operational
Event ID: 8465
```

To configure the Health Service, you run:

```
get-storagesubsystem clus* | Set-StorageHealthSetting -Name "Platform.ETW.MasTypes" -Value
"Microsoft.Health.EntityType.Subsystem,Microsoft.Health.EntityType.Server,Microsoft.Health.EntityType.Physical
Disk,Microsoft.Health.EntityType.StoragePool,Microsoft.Health.EntityType.Volume,Microsoft.Health.EntityType.Cl
uster"
```

When you run the cmdlet above to set the Health Settings, you cause the events we want to begin being written to the *Microsoft-Windows-Health/Operational* event channel.

### Configuring Log Analytics

Now that you have setup the proper logging on your cluster, the next step is to properly configure log analytics.

To give an overview, Azure Log Analytics can collect data directly from your physical or virtual Windows computers in your datacenter or other cloud environment into a single repository for detailed analysis and correlation.

To understand the supported configuration, review supported Windows operating systems and network firewall configuration.

If you don't have an Azure subscription, create a free account before you begin.

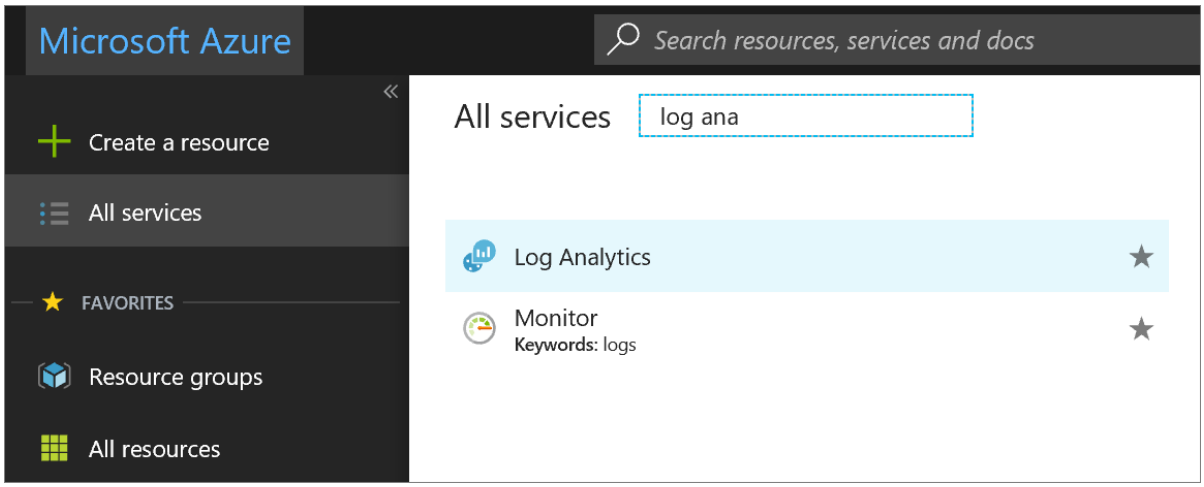
#### Login in to Azure Portal

Log in to the Azure portal at https://portal.azure.com.

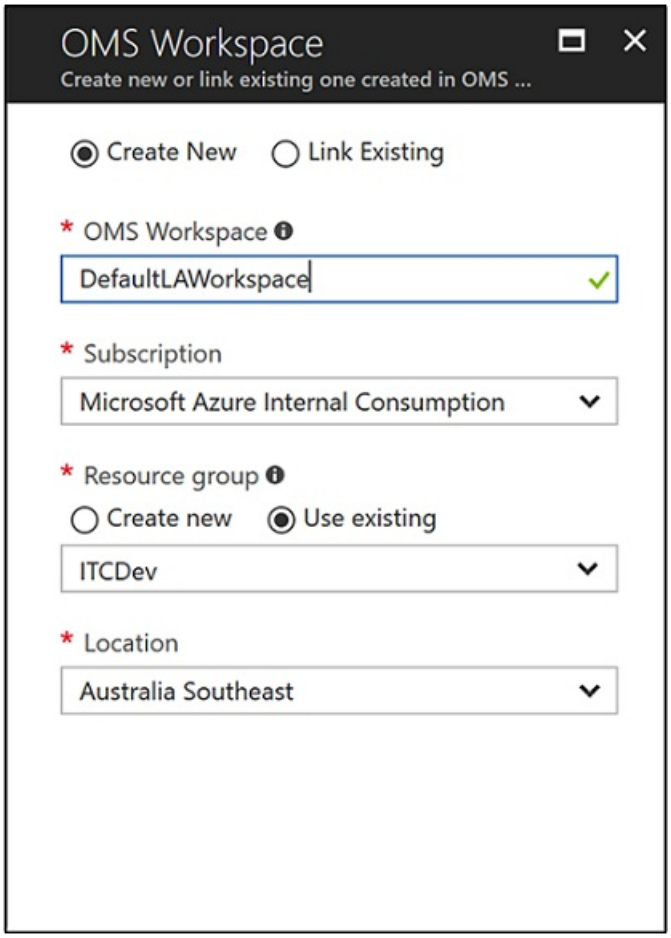
#### Create a workspace

For more details on the steps listed below, see the Azure Monitor documentation.

1. In the Azure portal, click **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.




2. Click **Create**, and then select choices for the following items:
   - Provide a name for the new **Log Analytics Workspace**, such as *DefaultLAWorkspace*.
   - Select a **Subscription** to link to by selecting from the drop-down list if the default selected is not appropriate.
   - For **Resource Group**, select an existing resource group that contains one or more Azure virtual machines.



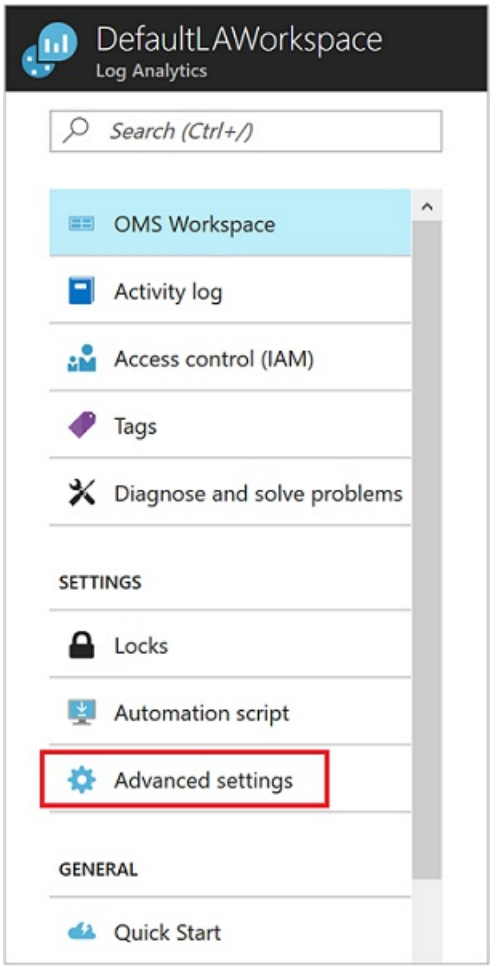

3. After providing the required information on the **Log Analytics Workspace** pane, click **OK**.

While the information is verified and the workspace is created, you can track its progress under **Notifications** from the menu.

#### Obtain workspace ID and key

Before installing the Microsoft Monitoring Agent for Windows, you need the workspace ID and key for your Log Analytics workspace. This information is required by the setup wizard to properly configure the agent and ensure it can successfully communicate with Log Analytics.

1. In the Azure portal, click **All services** found in the upper left-hand corner. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.
2. In your list of Log Analytics workspaces, select *DefaultLAWorkspace* created earlier.
3. Select **Advanced settings**.

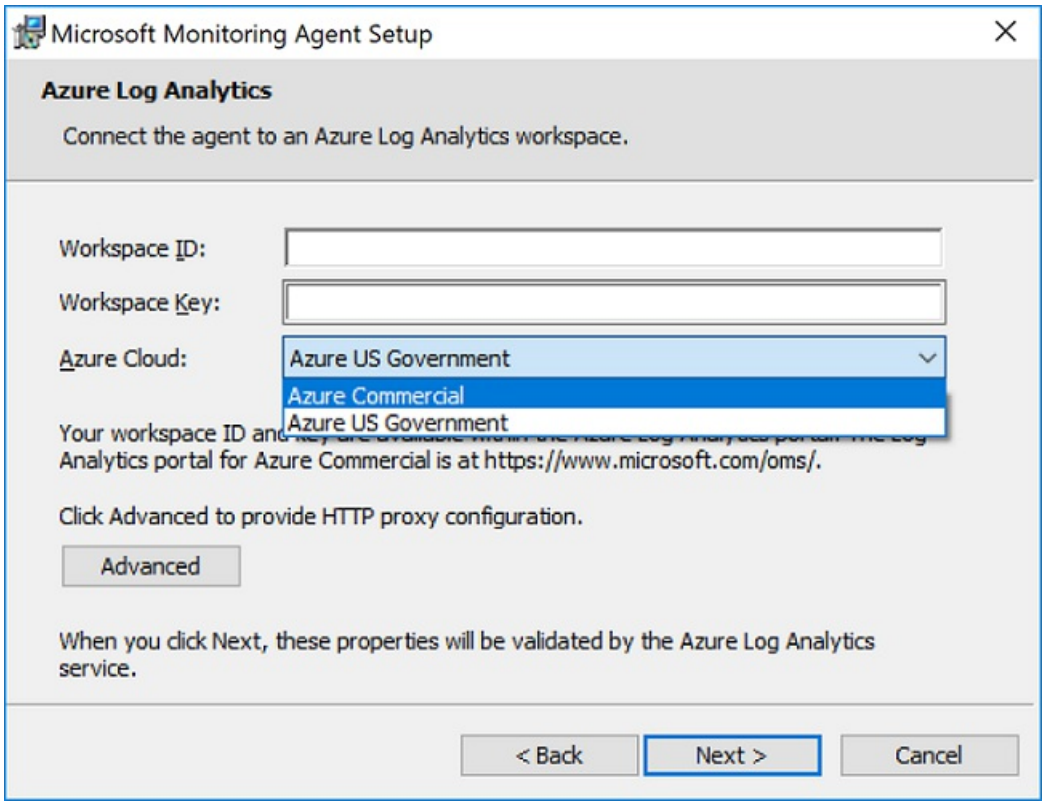



4. Select **Connected Sources**, and then select **Windows Servers**.
5. The value to the right of **Workspace ID** and **Primary Key**. Save both temporarily - copy and paste both into your favorite editor for the time being.

**Installing the agent on Windows**

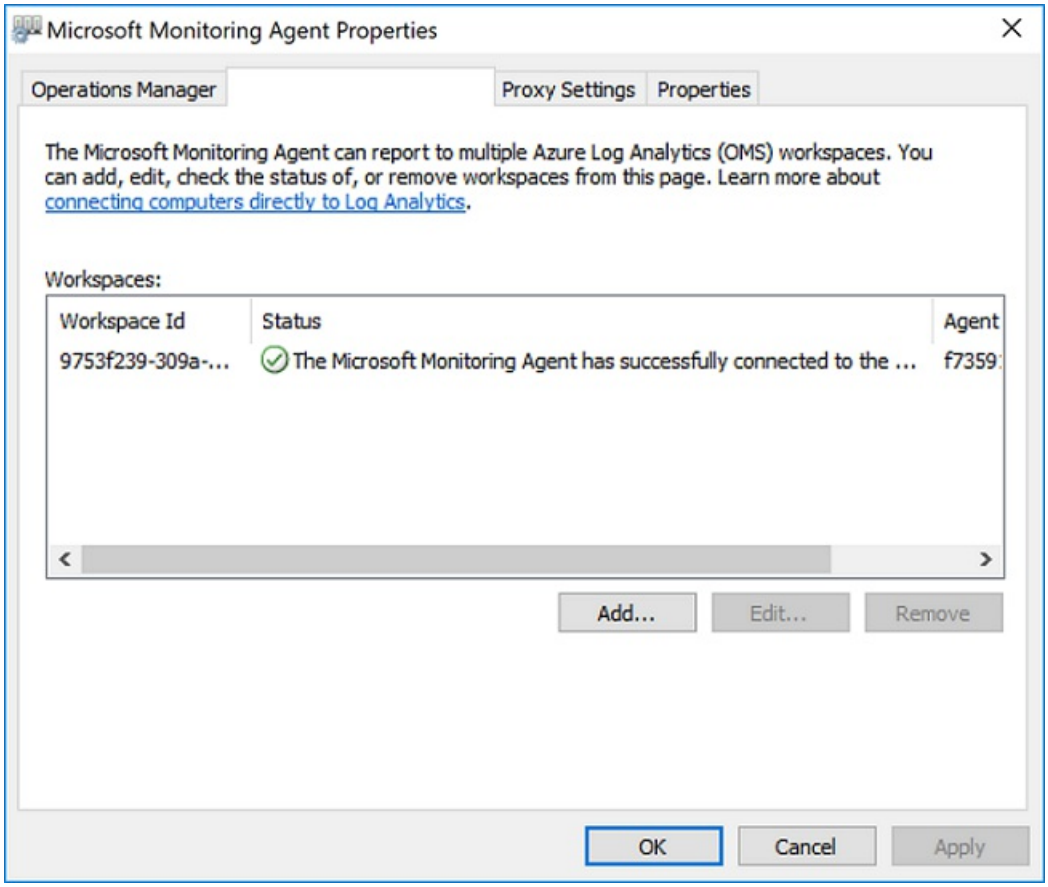
The following steps install and configure the Microsoft Monitoring Agent. **Be sure to install this agent on each server in your cluster and indicate that you want the agent to run at Windows Startup.**

1. On the **Windows Servers** page, select the appropriate **Download Windows Agent** version to download depending on the processor architecture of the Windows operating system.
2. Run Setup to install the agent on your computer.
3. On the **Welcome** page, click **Next**.
4. On the **License Terms** page, read the license and then click **I Agree**.
5. On the **Destination Folder** page, change or keep the default installation folder and then click **Next**.
6. On the **Agent Setup Options** page, choose to connect the agent to Azure Log Analytics and then click **Next**.
7. On the **Azure Log Analytics** page, perform the following:
    a. Paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied earlier. a. If the computer needs to communicate through a proxy server to the Log Analytics service, click **Advanced** and provide the URL and port number of the proxy server. If your proxy server requires authentication, type the username and password to authenticate with the proxy server and then click **Next**.
8. Click **Next** once you have completed providing the necessary configuration settings.




9. On the **Ready to Install** page, review your choices and then click **Install**.
10. On the **Configuration completed successfully** page, click **Finish**.

When complete, the **Microsoft Monitoring Agent** appears in **Control Panel**. You can review your configuration and verify that the agent is connected to Log Analytics. When connected, on the **Azure Log Analytics** tab, the agent displays a message stating: **The Microsoft Monitoring Agent has successfully connected to the Microsoft Log Analytics service.**

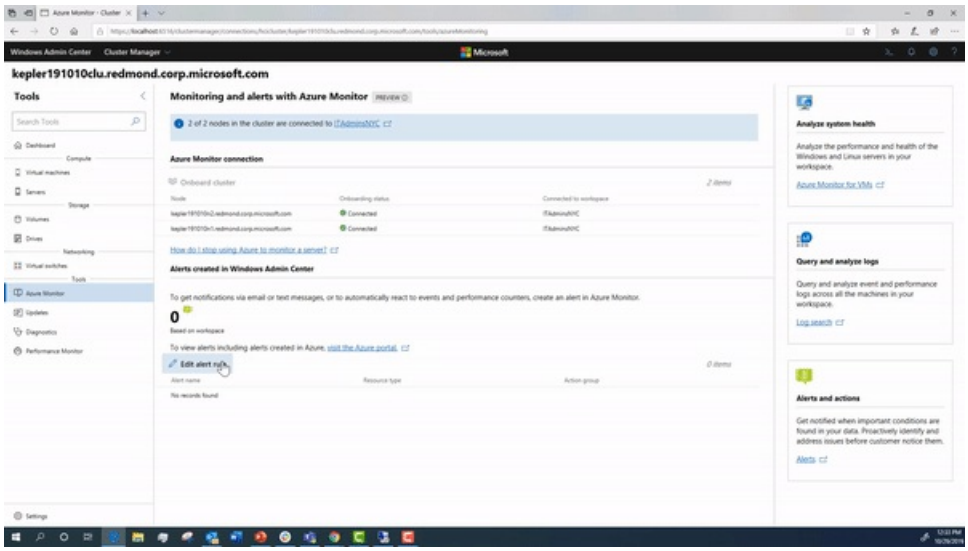



To understand the supported configuration, review supported Windows operating systems and network firewall

configuration.

## Setting up alerts using Windows Admin Center

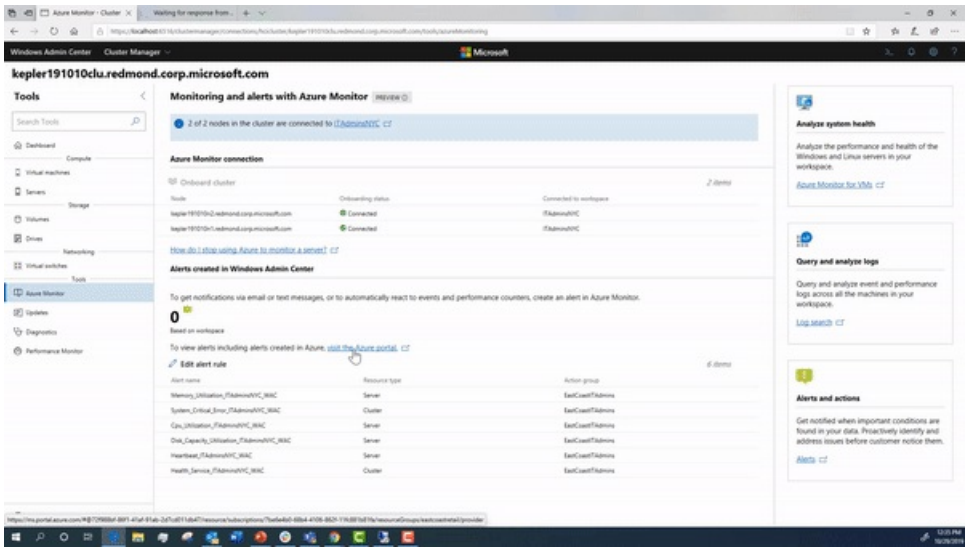
In Windows Admin Center, you can configure default alerts that will apply to all servers in your Log Analytics workspace.




These are the alerts and their default conditions that you can opt into:

| ALERT NAME | DEFAULT CONDITION |
|---|---|
| CPU utilization | Over 85% for 10 minutes |
| Disk capacity utilization | Over 85% for 10 minutes |
| Memory utilization | Available memory less than 100 MB for 10 minutes |
| Heartbeat | Fewer than 2 beats for 5 minutes |
| System critical error | Any critical alert in the cluster system event log |
| Health service alert | Any health service fault on the cluster |

Once you configure the alerts in Windows Admin Center, you can see the alerts in your log analytics workspace in Azure.

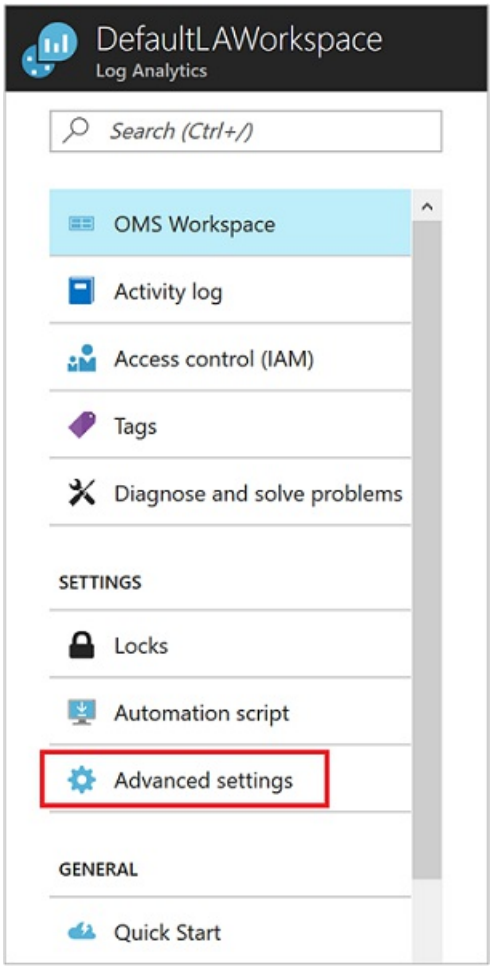



During this onboarding flow, the steps below are happening under the hood. We detail how to configure them in detail in case you want to manually setup your cluster.

**Collecting event and performance data**

Log Analytics can collect events from the Windows event log and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows event log, and several common performance counters to start with.

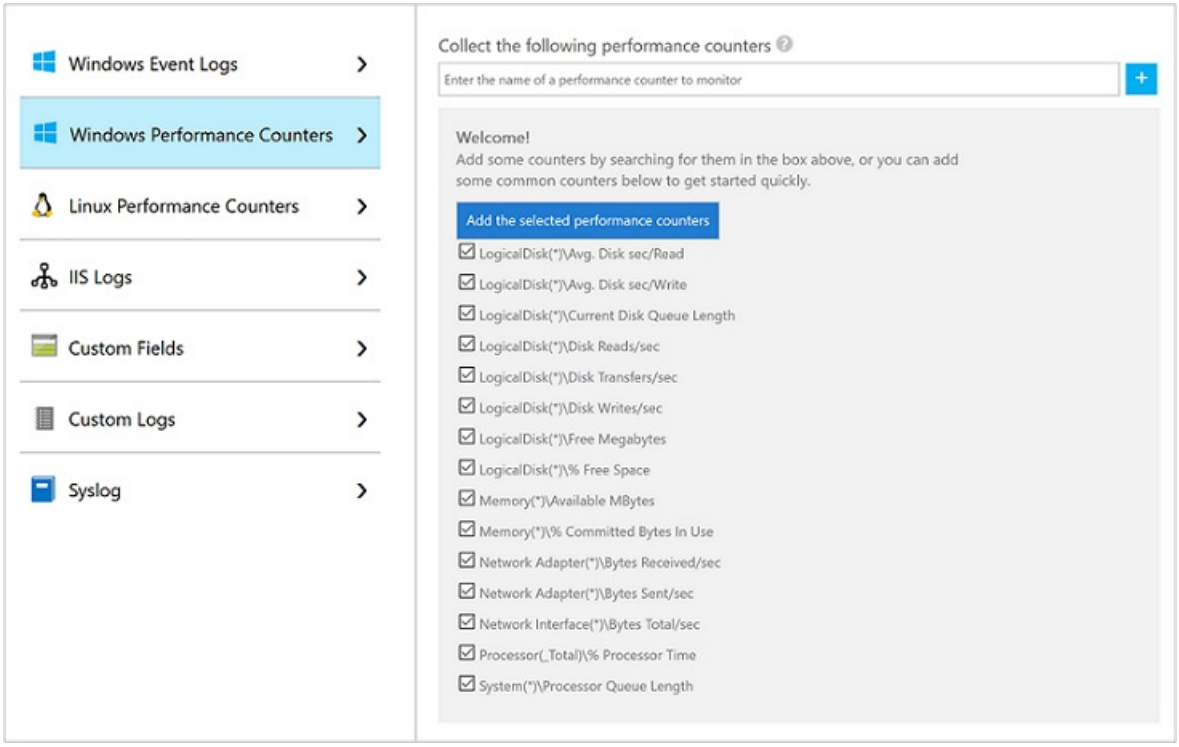
1. In the Azure portal, click **More services** found on the lower left-hand corner. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.
2. Select **Advanced settings**.



3. Select **Data**, and then select **Windows Event Logs**.
4. Here, add the Health Service event channel by typing in the name below and the click the plus sign **+**.

```
Event Channel: Microsoft-Windows-Health/Operational
```

5. In the table, check the severities **Error** and **Warning**.
6. Click **Save** at the top of the page to save the configuration.
7. Select **Windows Performance Counters** to enable collection of performance counters on a Windows computer.
8. When you first configure Windows Performance counters for a new Log Analytics workspace, you are given the option to quickly create several common counters. They are listed with a checkbox next to each.




   Click **Add the selected performance counters**. They are added and preset with a ten second collection sample interval.
9. Click **Save** at the top of the page to save the configuration.

## Creating alerts based on log data

If you've made it this far, your cluster should be sending your logs and performance counters to Log Analytics. The next step is to create alert rules that automatically run log searches at regular intervals. If results of the log search match particular criteria, then an alert is fired that sends you an email or text notification. Let's explore this below.

### Create a query

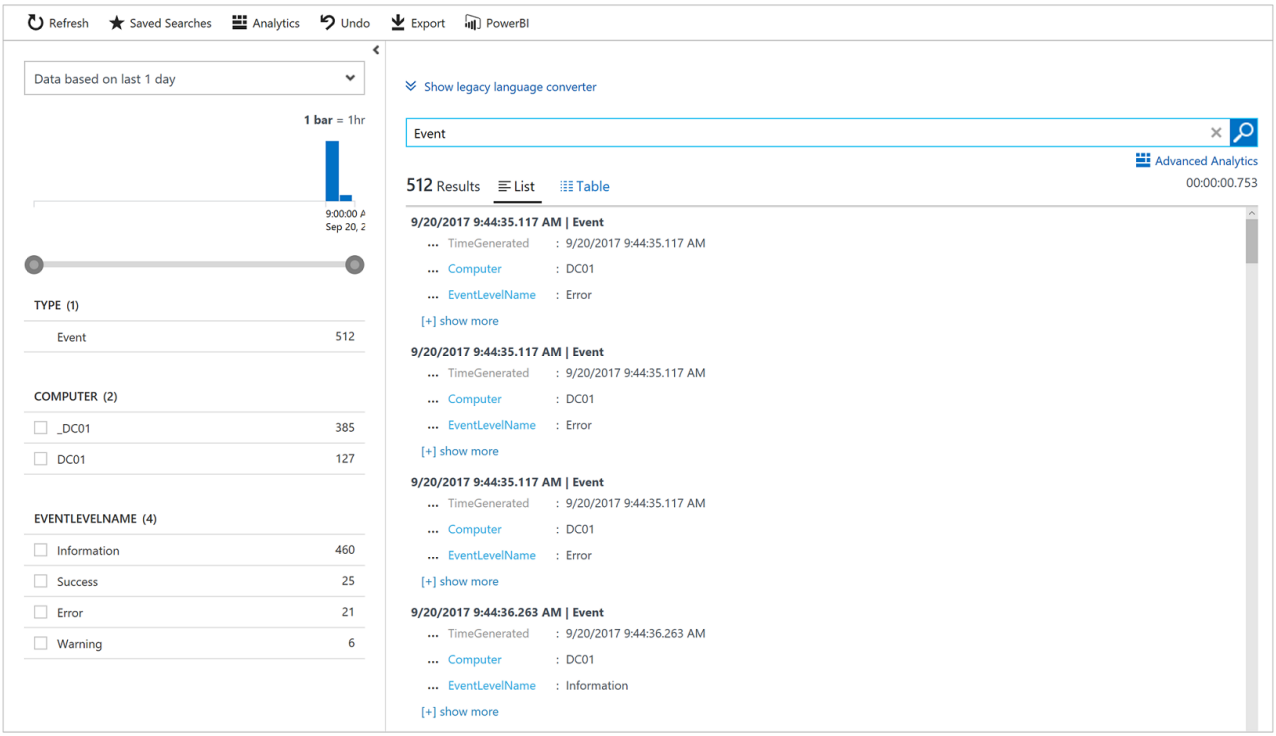
Start by opening the Log Search portal.

1. In the Azure portal, click **All services**. In the list of resources, type **Monitor**. As you begin typing, the list filters based on your input. Select **Monitor**.
2. On the Monitor navigation menu, select **Log Analytics** and then select a workspace.

The quickest way to retrieve some data to work with is a simple query that returns all records in table. Type the following queries in the search box and click the search button.

```
Event
```

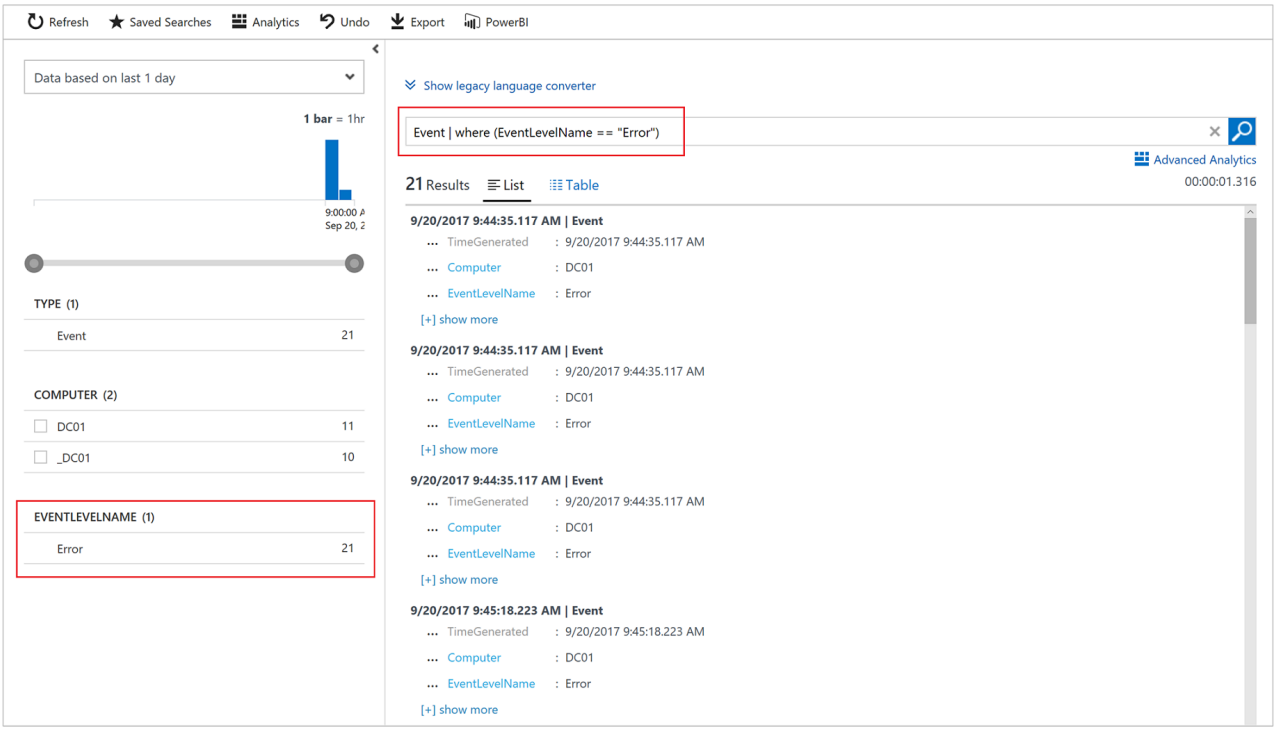
Data is returned in the default list view, and you can see how many total records were returned.




On the left side of the screen is the filter pane which allows you to add filtering to the query without modifying it directly. Several record properties are displayed for that record type, and you can select one or more property values to narrow your search results.

Select the checkbox next to **Error** under **EVENTLEVELNAME** or type the following to limit the results to error events.

```
Event | where (EventLevelName == "Error")
```



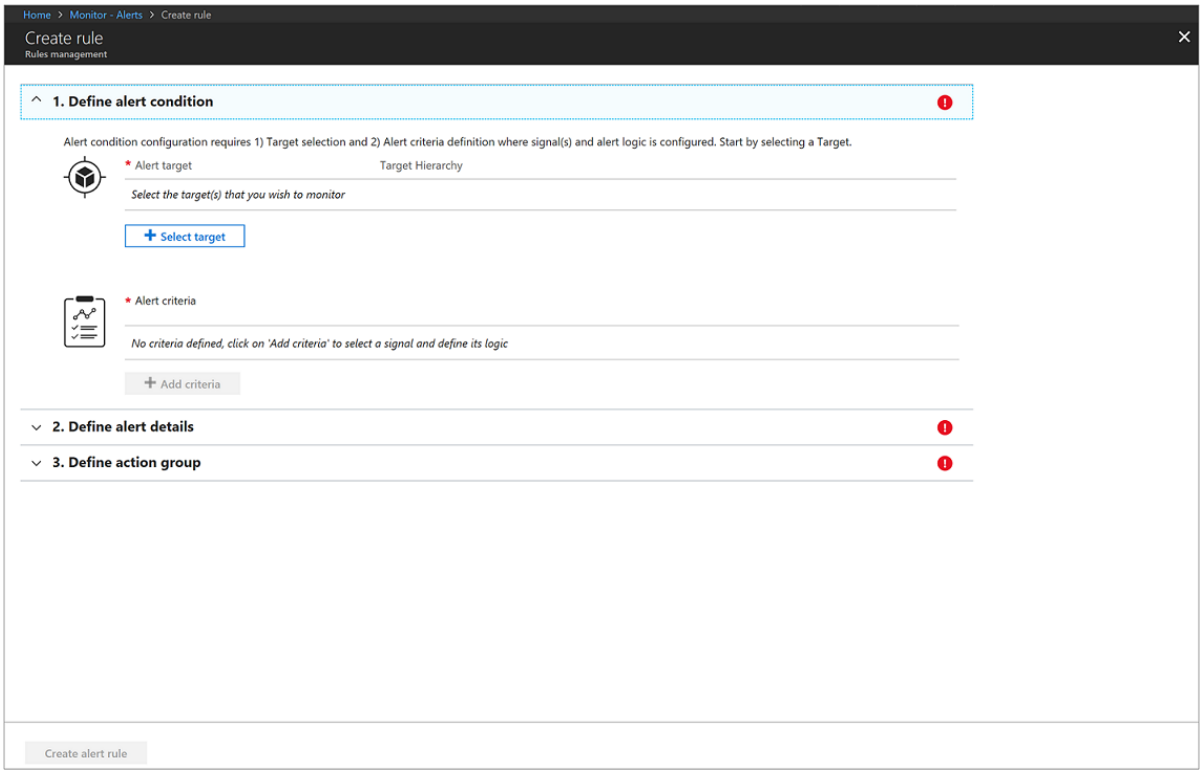

After you have the approriate queries made for events you care about, save them for the next step.

### Create alerts

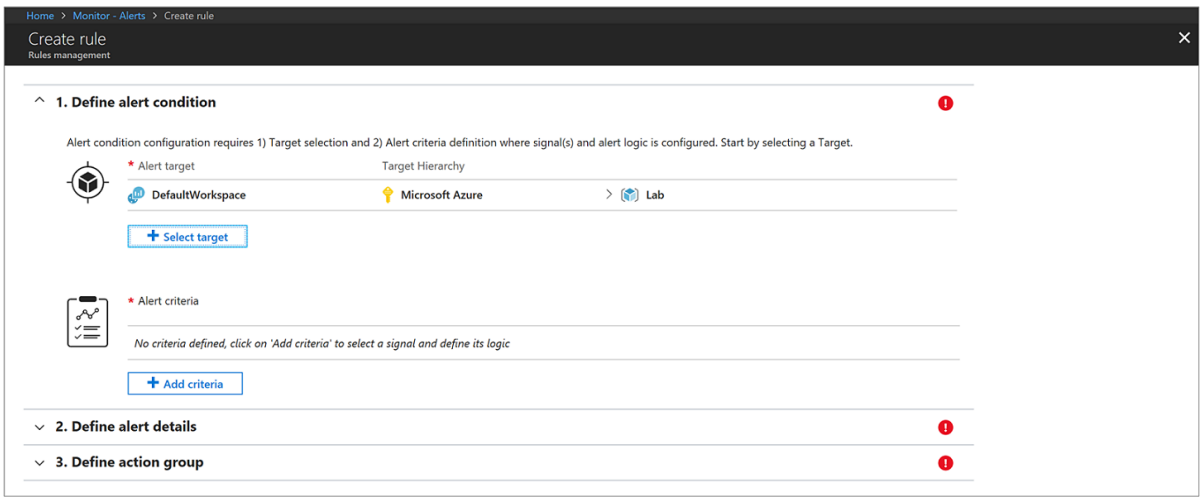
Now, let's walk through an example for creating an alert.

1. In the Azure portal, click **All services**. In the list of resources, type **Log Analytics**. As you begin typing, the list filters based on your input. Select **Log Analytics**.

2. In the left-hand pane, select **Alerts** and then click **New Alert Rule** from the top of the page to create a new alert.




3. For the first step, under the **Create Alert** section, you are going to select your Log Analytics workspace as the resource, since this is a log based alert signal. Filter the results by choosing the specific **Subscription** from the drop-down list if you have more than one, which contains Log Analytics workspace created earlier. Filter the **Resource Type** by selecting **Log Analytics** from the drop-down list. Finally, select the **Resource DefaultLAWorkspace** and then click **Done**.

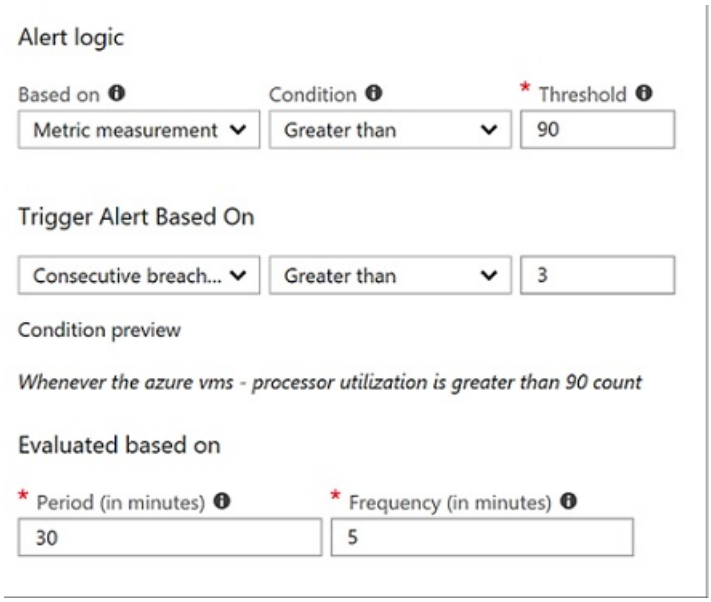



4. Under the section **Alert Criteria**, click **Add Criteria** to select your saved query and then specify logic that the alert rule follows.

5. Configure the alert with the following information: a. From the **Based on** drop-down list, select **Metric measurement**. A metric measurement will create an alert for each object in the query with a value that exceeds our specified threshold. b. For the **Condition**, select **Greater than** and specify a thershold. c. Then define when to trigger the alert. For example you could select **Consecutive breaches** and from the drop-down list select **Greater than** a value of 3. d. Under Evaluation based on section, modify the **Period** value

to **30** minutes and **Frequency** to 5. The rule will run every five minutes and return records that were created within the last thirty minutes from the current time. Setting the time period to a wider window accounts for the potential of data latency, and ensures the query returns data to avoid a false negative where the alert never fires.

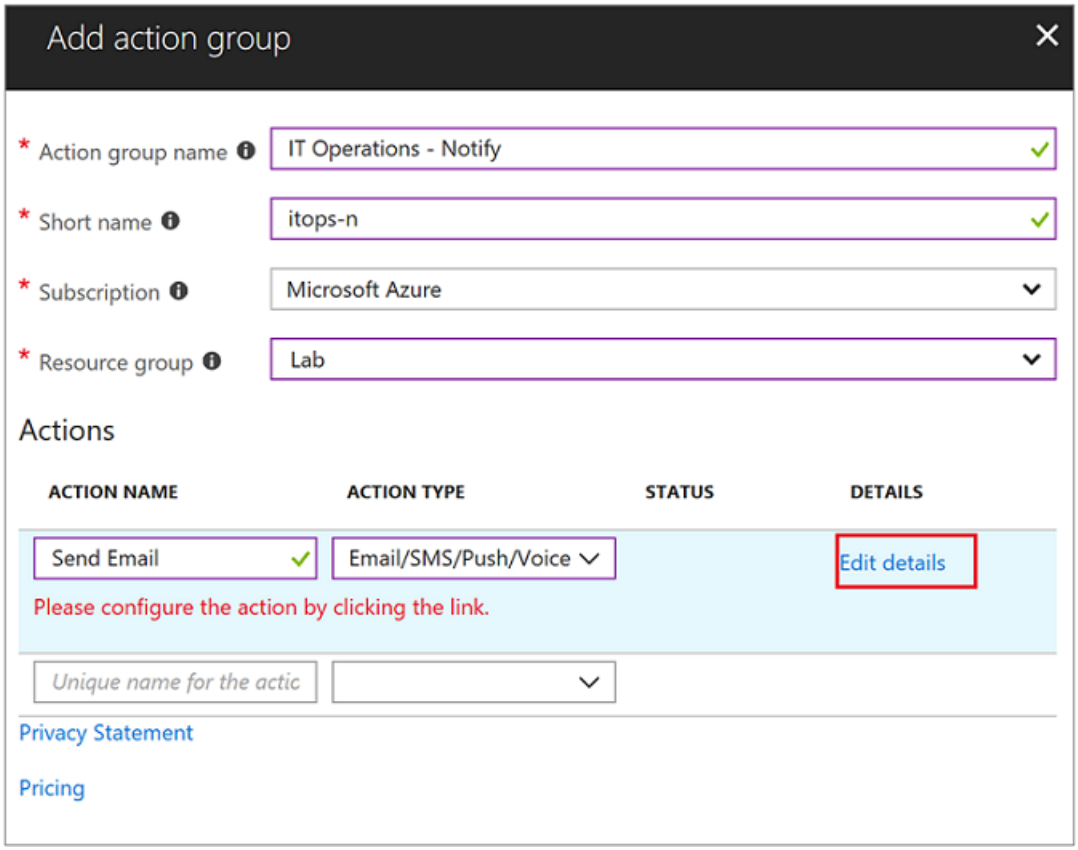
6. Click **Done** to complete the alert rule.




7. Now moving onto the second step, provide a name of your alert in the **Alert rule name** field, such as **Alert on all Error Events**. Specify a **Description** detailing specifics for the alert, and select **Critical(Sev 0)** for the **Severity** value from the options provided.

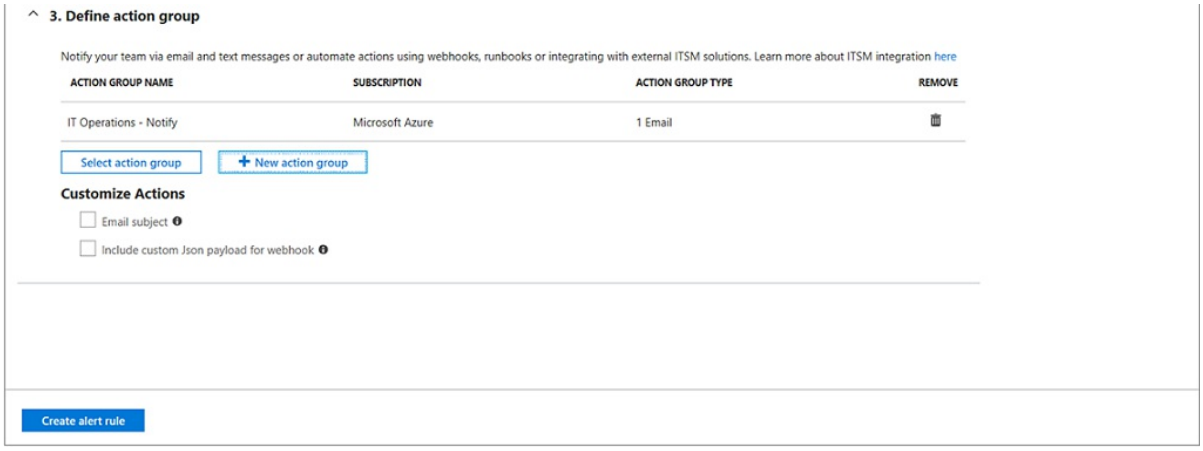
8. To immediately activate the alert rule on creation, accept the default value for **Enable rule upon creation**.

9. For the third and final step, you specify an **Action Group**, which ensures that the same actions are taken each time an alert is triggered and can be used for each rule you define. Configure a new action group with the following information: a. Select **New action group** and the **Add action group** pane appears. b. For **Action group name**, specify a name such as **IT Operations - Notify** and a **Short name** such as **itops-n**. c. Verify the default values for **Subscription** and **Resource group** are correct. If not, select the correct one from the drop-down list. d. Under the Actions section, specify a name for the action, such as **Send Email** and under **Action Type** select **Email/SMS/Push/Voice** from the drop-down list. The **Email/SMS/Push/Voice** properties pane will open to the right in order to provide additional information. e. On the **Email/SMS/Push/Voice** pane, select and setup your preference. For example, enable **Email** and provide a valid email SMTP address to deliver the message to. f. Click **OK** to save your changes.



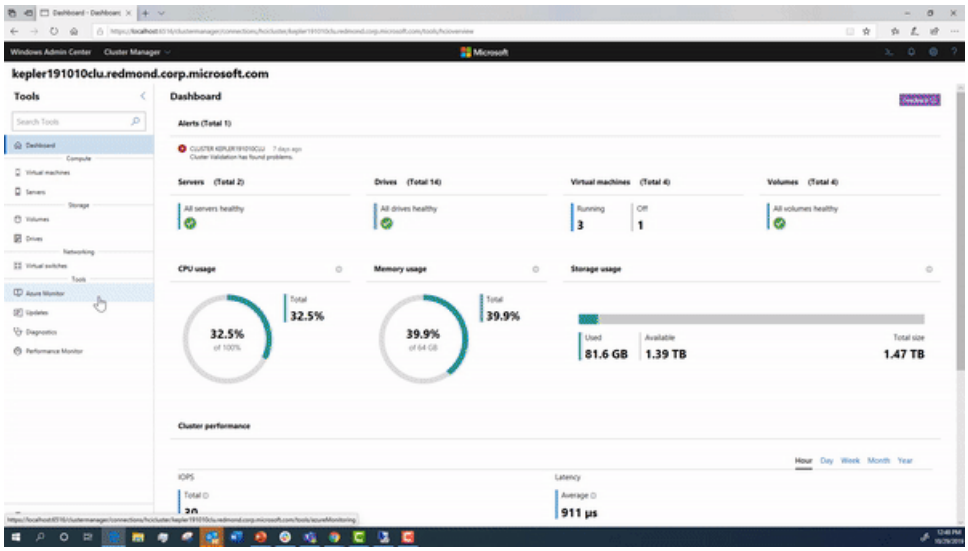

10. Click **OK** to complete the action group.

11. Click **Create alert rule** to complete the alert rule. It starts running immediately.




**Example alert**

For reference, this is what an example alert looks like in Azure.




Below is an example of the email that you will be send by Azure Monitor:

Microsoft

Azure Application Insights

**WARNING**

Average Failed tests is 130 : crossed threshold for 5 minutes

View application in Azure Portal

| | |
|---|---|
| **Time** | 11/08/2018 00:09:24 (UTC) |
| **Application** | VSEng-UnitTestTelemetry |
| **Subscription** | |
| **Performance metric** | Average Failed tests |
| **Configured time period** | 5 minutes |
| **Configured condition** | > |
| **Configured threshold** | 1 |
| **Actual aggregated value** | 130 |

## Additional References

- Storage Spaces Direct overview
- For more detailed information, read the Azure Monitor documentation.
- Read this for an overview on how to connect to other Azure hybrid services.

# Troubleshoot Storage Spaces Direct

12/16/2020 • 20 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

Use the following information to troubleshoot your Storage Spaces Direct deployment.

In general, start with the following steps:

1. Confirm the make/model of SSD is certified for Windows Server 2016 and Windows Server 2019 using the Windows Server Catalog. Confirm with vendor that the drives are supported for Storage Spaces Direct.
2. Inspect the storage for any faulty drives. Use storage management software to check the status of the drives. If any of the drives are faulty, work with your vendor.
3. Update storage and drive firmware if necessary. Ensure the latest Windows Updates are installed on all nodes. You can get the latest updates for Windows Server 2016 from Windows 10 and Windows Server 2016 update history and for Windows Server 2019 from Windows 10 and Windows Server 2019 update history.
4. Update network adapter drivers and firmware.
5. Run cluster validation and review the Storage Space Direct section, ensure the drives that will used for the cache are reported correctly and no errors.

If you're still having issues, review the scenarios below.

## Virtual disk resources are in No Redundancy state

The nodes of a Storage Spaces Direct system restart unexpectedly because of a crash or power failure. Then, one or more of the virtual disks may not come online, and you see the description "Not enough redundancy information."

| FRIENDLYNAME | RESILIENCYSETTINGNAME | OPERATIONALSTATUS | HEALTHSTATUS | ISMANUALATTACH | SIZE | PSCOMPUTERNAME |
|---|---|---|---|---|---|---|
| Disk4 | Mirror | OK | Healthy | True | 10 TB | Node-01.conto... |
| Disk3 | Mirror | OK | Healthy | True | 10 TB | Node-01.conto... |
| Disk2 | Mirror | No Redundancy | Unhealthy | True | 10 TB | Node-01.conto... |
| Disk1 | Mirror | {No Redundancy, InService} | Unhealthy | True | 10 TB | Node-01.conto... |

Additionally, after an attempt to bring the virtual disk online, the following information is logged in the Cluster log (DiskRecoveryAction).

```
[Verbose] 00002904.00001040::YYYY/MM/DD-12:03:44.891 INFO [RES] Physical Disk <DiskName>: OnlineThread:
SuGetSpace returned 0.
[Verbose] 00002904.00001040:: YYYY/MM/DD -12:03:44.891 WARN [RES] Physical Disk < DiskName>: Underlying
virtual disk is in 'no redundancy' state; its volume(s) may fail to mount.
[Verbose] 00002904.00001040:: YYYY/MM/DD -12:03:44.891 ERR [RES] Physical Disk <DiskName>: Failing online due
to virtual disk in 'no redundancy' state. If you would like to attempt to online the disk anyway, first set
this resource's private property 'DiskRecoveryAction' to 1. We will try to bring the disk online for recovery,
but even if successful, its volume(s) or CSV may be unavailable.
```

The **No Redundancy Operational Status** can occur if a disk failed or if the system is unable to access data on the virtual disk. This issue can occur if a reboot occurs on a node during maintenance on the nodes.

To fix this issue, follow these steps:

1. Remove the affected Virtual Disks from CSV. This will put them in the "Available storage" group in the cluster and start showing as a ResourceType of "Physical Disk."

   ```
   Remove-ClusterSharedVolume -name "VdiskName"
   ```

2. On the node that owns the Available Storage group, run the following command on every disk that's in a No Redundancy state. To identify which node the "Available Storage" group is on you can run the following command.

   ```
   Get-ClusterGroup
   ```

3. Set the disk recovery action and then start the disk(s).

   ```
   Get-ClusterResource "VdiskName" | Set-ClusterParameter -Name DiskRecoveryAction -Value 1
   Start-ClusterResource -Name "VdiskName"
   ```

4. A repair should automatically start. Wait for the repair to finish. It may go into a suspended state and start again. To monitor the progress:

   - Run **Get-StorageJob** to monitor the status of the repair and to see when it is completed.
   - Run **Get-VirtualDisk** and verify that the Space returns a HealthStatus of Healthy.

5. After the repair finishes and the Virtual Disks are Healthy, change the Virtual Disk parameters back.

   ```
   Get-ClusterResource "VdiskName" | Set-ClusterParameter -Name DiskRecoveryAction -Value 0
   ```

6. Take the disk(s) offline and then online again to have the DiskRecoveryAction take effect:

   ```
   Stop-ClusterResource "VdiskName"
   Start-ClusterResource "VdiskName"
   ```

7. Add the affected Virtual Disks back to CSV.

   ```
   Add-ClusterSharedVolume -name "VdiskName"
   ```

**DiskRecoveryAction** is an override switch that enables attaching the Space volume in read-write mode without any checks. The property enables you to do diagnostics into why a volume won't come online. It's very similar to Maintenance Mode but you can invoke it on a resource in a Failed state. It also lets you access the data, which can be helpful in situations such as "No Redundancy," where you can get access to whatever data you can and copy it.

The DiskRecoveryAction property was added in the February 22, 2018, update, KB 4077525.

## Detached status in a cluster

When you run the **Get-VirtualDisk** cmdlet, the OperationalStatus for one or more Storage Spaces Direct virtual disks is Detached. However, the HealthStatus reported by the **Get-PhysicalDisk** cmdlet indicates that all the physical disks are in a Healthy state.

The following is an example of the output from the **Get-VirtualDisk** cmdlet.

| FRIENDLYNAME | RESILIENCYSETTINGNAME | OPERATIONAL STATUS | HEALTHSTATUS | ISMANUALATTACH | SIZE | PSCOMPUTERNAME |
|---|---|---|---|---|---|---|
| Disk4 | Mirror | OK | Healthy | True | 10 TB | Node-01.conto... |
| Disk3 | Mirror | OK | Healthy | True | 10 TB | Node-01.conto... |
| Disk2 | Mirror | Detached | Unknown | True | 10 TB | Node-01.conto... |
| Disk1 | Mirror | Detached | Unknown | True | 10 TB | Node-01.conto... |

Additionally, the following events may be logged on the nodes:

```
Log Name: Microsoft-Windows-StorageSpaces-Driver/Operational
Source: Microsoft-Windows-StorageSpaces-Driver
Event ID: 311
Level: Error
User: SYSTEM
Computer: Node#.contoso.local
Description: Virtual disk {GUID} requires a data integrity scan.

Data on the disk is out-of-sync and a data integrity scan is required.

To start the scan, run the following command:
Get-ScheduledTask -TaskName "Data Integrity Scan for Crash Recovery" | Start-ScheduledTask

Once you have resolved the condition listed above, you can online the disk by using the following commands in
PowerShell:

Get-VirtualDisk | ?{ $_.ObjectId -Match "{GUID}" } | Get-Disk | Set-Disk -IsReadOnly $false
Get-VirtualDisk | ?{ $_.ObjectId -Match "{GUID}" } | Get-Disk | Set-Disk -IsOffline  $false
-----------------------------------------------------------

Log Name: System
Source: Microsoft-Windows-ReFS
Event ID: 134
Level: Error
User: SYSTEM
Computer: Node#.contoso.local
Description: The file system was unable to write metadata to the media backing volume <VolumeId>. A write
failed with status "A device which does not exist was specified." ReFS will take the volume offline. It may be
mounted again automatically.
-----------------------------------------------------------
Log Name: Microsoft-Windows-ReFS/Operational
Source: Microsoft-Windows-ReFS
Event ID: 5
Level: Error
User: SYSTEM
Computer: Node#.contoso.local
Description: ReFS failed to mount the volume.
Context: 0xffffbb89f53f4180
Error: A device which does not exist was specified.
Volume GUID:{00000000-0000-0000-0000-000000000000}
DeviceName:
Volume Name:
```

The **Detached Operational Status** can occur if the dirty region tracking (DRT) log is full. Storage Spaces uses dirty region tracking (DRT) for mirrored spaces to make sure that when a power failure occurs, any in-flight updates to metadata are logged to make sure that the storage space can redo or undo operations to bring the storage space back into a flexible and consistent state when power is restored and the system comes back up. If the DRT log is full, the virtual disk can't be brought online until the DRT metadata is synchronized and flushed. This process requires running a full scan, which can take several hours to finish.

To fix this issue, follow these steps:

1. Remove the affected Virtual Disks from CSV.

   ```
   Remove-ClusterSharedVolume -name "VdiskName"
   ```

2. Run the following commands on every disk that's not coming online.

   ```
   Get-ClusterResource -Name "VdiskName" | Set-ClusterParameter DiskRunChkDsk 7
   Start-ClusterResource -Name "VdiskName"
   ```

3. Run the following command on every node in which the detached volume is online.

   ```
   Get-ScheduledTask -TaskName "Data Integrity Scan for Crash Recovery" | Start-ScheduledTask
   ```

   This task should be initiated on all nodes on which the detached volume is online. A repair should automatically start. Wait for the repair to finish. It may go into a suspended state and start again. To monitor the progress:

   - Run **Get-StorageJob** to monitor the status of the repair and to see when it is completed.
   - Run **Get-VirtualDisk** and verify the Space returns a HealthStatus of Healthy.
     - The "Data Integrity Scan for Crash Recovery" is a task that doesn't show as a storage job, and there is no progress indicator. If the task is showing as running, it is running. When it completes, it will show completed.

       Additionally, you can view the status of a running schedule task by using the following cmdlet:

       ```
       Get-ScheduledTask | ? State -eq running
       ```

4. As soon as the "Data Integrity Scan for Crash Recovery" is finished, the repair finishes and the Virtual Disks are Healthy, change the Virtual Disk parameters back.

   ```
   Get-ClusterResource -Name "VdiskName" | Set-ClusterParameter DiskRunChkDsk 0
   ```

5. Take the disk(s) offline and then online again to have the DiskRecoveryAction take effect:

   ```
   Stop-ClusterResource "VdiskName"
   Start-ClusterResource "VdiskName"
   ```

6. Add the affected Virtual Disks back to CSV.

   ```
   Add-ClusterSharedVolume -name "VdiskName"
   ```

   **DiskRunChkdsk value 7** is used to attach the Space volume and have the partition in read-only mode. This enables Spaces to self-discover and self-heal by triggering a repair. Repair will run automatically once mounted. It also allows you to access the data, which can be helpful to get access to whatever data you can to copy. For some fault conditions, such as a full DRT log, you need to run the Data Integrity Scan for Crash Recovery scheduled task.

**Data Integrity Scan for Crash Recovery task** is used to synchronize and clear a full dirty region tracking (DRT) log. This task can take several hours to complete. The "Data Integrity Scan for Crash Recovery" is a task that doesn't show as a storage job, and there is no progress indicator. If the task is showing as running, it is running. When it completes, it will show as completed. If you cancel the task or restart a node while this task is running, the task will need to start over from the beginning.

For more information, see Troubleshooting Storage Spaces Direct health and operational states.

## Event 5120 with STATUS_IO_TIMEOUT c00000b5

> **IMPORTANT**
>
> **For Windows Server 2016:** To reduce the chance of experiencing these symptoms while applying the update with the fix, it is recommended to use the Storage Maintenance Mode procedure below to install the October 18, 2018, cumulative update for Windows Server 2016 or a later version when the nodes currently have installed a Windows Server 2016 cumulative update that was released from May 8, 2018 to October 9, 2018.

You might get event 5120 with STATUS_IO_TIMEOUT c00000b5 after you restart a node on Windows Server 2016 with cumulative update that were released from May 8, 2018 KB 4103723 to October 9, 2018 KB 4462917 installed.

When you restart the node, Event 5120 is logged in the System event log and includes one of the following error codes:

```
Event Source: Microsoft-Windows-FailoverClustering
Event ID: 5120
Description:    Cluster Shared Volume 'CSVName' ('Cluster Virtual Disk (CSVName)') has entered a paused state
because of 'STATUS_IO_TIMEOUT(c00000b5)'. All I/O will temporarily be queued until a path to the volume is
reestablished.

Cluster Shared Volume 'CSVName' ('Cluster Virtual Disk (CSVName)') has entered a paused state because of
'STATUS_CONNECTION_DISCONNECTED(c000020c)'. All I/O will temporarily be queued until a path to the volume is
reestablished.
```

When an Event 5120 is logged, a live dump is generated to collect debugging information that may cause additional symptoms or have a performance effect. Generating the live dump creates a brief pause to enable taking a snapshot of memory to write the dump file. Systems that have lots of memory and are under stress may cause nodes to drop out of cluster membership and also cause the following Event 1135 to be logged.

```
Event source: Microsoft-Windows-FailoverClustering
Event ID: 1135
Description: Cluster node 'NODENAME'was removed from the active failover cluster membership. The Cluster
service on this node may have stopped. This could also be due to the node having lost communication with other
active nodes in the failover cluster. Run the Validate a Configuration wizard to check your network
configuration. If the condition persists, check for hardware or software errors related to the network
adapters on this node. Also check for failures in any other network components to which the node is connected
such as hubs, switches, or bridges.
```

A change introduced in May 8, 2018 to Windows Server 2016, which was a cumulative update to add SMB Resilient Handles for the Storage Spaces Direct intra-cluster SMB network sessions. This was done to improve resiliency to transient network failures and improve how RoCE handles network congestion. These improvements also inadvertently increased time-outs when SMB connections try to reconnect and waits to time-out when a node is restarted. These issues can affect a system that is under stress. During unplanned downtime, IO pauses of up to 60 seconds have also been observed while the system waits for connections to time-out. To fix this issue, install the October 18, 2018, cumulative update for Windows Server 2016 or a later version.

*Note* This update aligns the CSV time-outs with SMB connection time-outs to fix this issue. It does not implement the changes to disable live dump generation mentioned in the Workaround section.

**Shutdown process flow:**

1. Run the Get-VirtualDisk cmdlet, and make sure that the HealthStatus value is Healthy.
2. Drain the node by running the following cmdlet:

```
Suspend-ClusterNode -Drain
```

3. Put the disks on that node in Storage Maintenance Mode by running the following cmdlet:

```
Get-StorageFaultDomain -type StorageScaleUnit | Where-Object {$_.FriendlyName -eq "<NodeName>"} |
Enable-StorageMaintenanceMode
```

4. Run the **Get-PhysicalDisk** cmdlet, and make sure that the OperationalStatus value is In Maintenance Mode.
5. Run the **Restart-Computer** cmdlet to restart the node.
6. After node restarts, remove the disks on that node from Storage Maintenance Mode by running the following cmdlet:

```
Get-StorageFaultDomain -type StorageScaleUnit | Where-Object {$_.FriendlyName -eq "<NodeName>"} |
Disable-StorageMaintenanceMode
```

7. Resume the node by running the following cmdlet:

```
Resume-ClusterNode
```

8. Check the status of the resync jobs by running the following cmdlet:

```
Get-StorageJob
```

### Disabling live dumps

To mitigate the effect of live dump generation on systems that have lots of memory and are under stress, you may additionally want to disable live dump generation. Three options are provided below.

Caution

This procedure can prevent the collection of diagnostic information that Microsoft Support may need to investigate this problem. A Support agent may have to ask you to re-enable live dump generation based on specific troubleshooting scenarios.

There are two methods to disable live dumps, as described below.

#### Method 1 (recommended in this scenario)

To completely disable all dumps, including live dumps system-wide, follow these steps:

1. Create the following registry key:
   HKLM\System\CurrentControlSet\Control\CrashControl\ForceDumpsDisabled
2. Under the new **ForceDumpsDisabled** key, create a REG_DWORD property as GuardedHost, and then set its value to 0x10000000.
3. Apply the new registry key to each cluster node.

> **NOTE**
>
> You have to restart the computer for the nregistry change to take effect.

After this registry key is set, live dump creation will fail and generate a "STATUS_NOT_SUPPORTED" error.

#### Method 2

By default, Windows Error Reporting will allow only one LiveDump per report type per 7 days and only 1 LiveDump per machine per 5 days. You can change that by setting the following registry keys to only allow one LiveDump on the machine forever.

```
reg add "HKLM\Software\Microsoft\Windows\Windows Error Reporting\FullLiveKernelReports" /v
SystemThrottleThreshold /t REG_DWORD /d 0xFFFFFFFF /f
```

```
reg add "HKLM\Software\Microsoft\Windows\Windows Error Reporting\FullLiveKernelReports" /v
ComponentThrottleThreshold /t REG_DWORD /d 0xFFFFFFFF /f
```

*Note* You have to restart the computer for the change to take effect.

**Method 3**

To disable cluster generation of live dumps (such as when an Event 5120 is logged), run the following cmdlet:

```
(Get-Cluster).DumpPolicy = ((Get-Cluster).DumpPolicy -band 0xFFFFFFFFFFFFFFFE)
```

This cmdlet has an immediate effect on all cluster nodes without a computer restart.

# Slow IO performance

If you are seeing slow IO performance, check if cache is enabled in your Storage Spaces Direct configuration.

There are two ways to check:

1. Using the cluster log. Open the cluster log in text editor of choice and search for "[=== SBL Disks ===]." This will be a list of the disk on the node the log was generated on.

   Cache Enabled Disks Example: Note here that the state is CacheDiskStateInitializedAndBound and there is a GUID present here.

   ```
   [=== SBL Disks ===]
    {26e2e40f-a243-1196-49e3-8522f987df76},3,false,true,1,48,{1ff348f1-d10d-7a1a-d781-
   4734f4440481},CacheDiskStateInitializedAndBound,1,8087,54,false,false,HGST    ,HUH721010AL4200 ,
   7PG3N2ER,A21D,{d5e27a3b-42fb-410a-81c6-9d8cc12da20c},[R/M 0 R/U 0 R/T 0 W/M 0 W/U 0 W/T 0],
   ```

   Cache Not Enabled: Here we can see there is no GUID present and the state is CacheDiskStateNonHybrid.

   ```
   [=== SBL Disks ===]
   {426f7f04-e975-fc9d-28fd-72a32f811b7d},12,false,true,1,24,{00000000-0000-0000-0000-
   000000000000},CacheDiskStateNonHybrid,0,0,0,false,false,HGST    ,HUH721010AL4200 ,
   7PGXXG6C,A21D,{d5e27a3b-42fb-410a-81c6-9d8cc12da20c},[R/M 0 R/U 0 R/T 0 W/M 0 W/U 0 W/T 0],
   ```

   Cache Not Enabled: When all disks are of the same type case is not enabled by default. Here we can see there is no GUID present and the state is CacheDiskStateIneligibleDataPartition.

   ```
   {d543f90c-798b-d2fe-7f0a-cb226c77eeed},10,false,false,1,20,{00000000-0000-0000-0000-
   000000000000},CacheDiskStateIneligibleDataPartition,0,0,0,false,false,NVMe    ,INTEL SSDPE7KX02,
   PHLF7330004V2P0LGN,0170,{79b4d631-976f-4c94-a783-df950389fd38},[R/M 0 R/U 0 R/T 0 W/M 0 W/U 0 W/T 0],
   ```

2. Using Get-PhysicalDisk.xml from the SDDCDiagnosticInfo

   a. Open the XML file using "$d = Import-Clixml GetPhysicalDisk.XML"
   b. Run "ipmo storage"
   c. run "$d". Note that Usage is Auto-Select, not Journal You'll see output like this:

| FRIENDLY NAME | SERIALNUMBER | MEDIATYPE | CANPOOL | OPERATIONALSTATUS | HEALTHSTATUS | USAGE | SIZE |
|---|---|---|---|---|---|---|---|
| NVMe INTEL SSDPE7KX02 | PHLF733000372P0LGN | SSD | False | OK | Healthy | Auto-Select 1.82 TB | |
| NVMe INTEL SSDPE7KX02 | PHLF7504008J2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF7504005F2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF7504002A2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF7504004T2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF7504002E2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF733002Z2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF733000272P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF733001J2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF733000302P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |
| NVMe INTEL SSDPE7KX02 | PHLF733004D2P0LGN | SSD | False | OK | Healthy | Auto-Select | 1.82 TB |

# How to destroy an existing cluster so you can use the same disks again

In a Storage Spaces Direct cluster, once you disable Storage Spaces Direct and use the clean-up process described in Clean drives, the clustered storage pool still remains in an Offline state, and the Health Service is removed from cluster.

The next step is to remove the phantom storage pool:

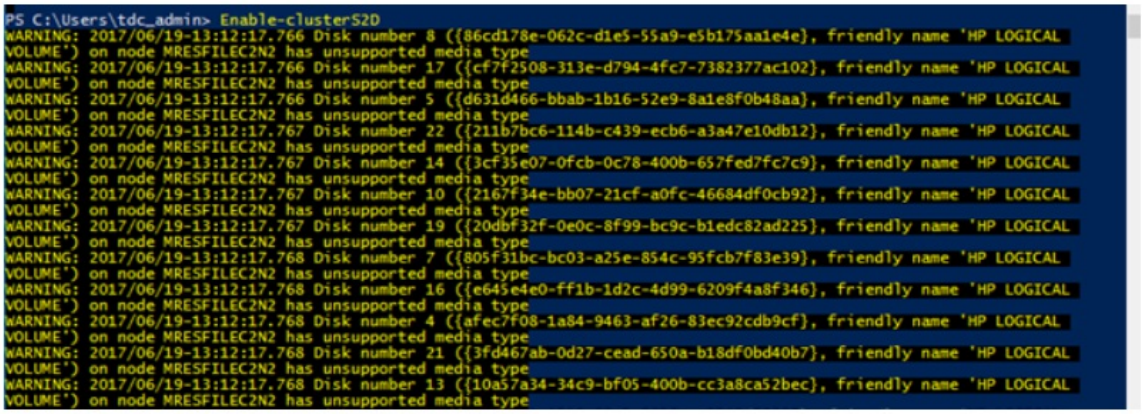
```
Get-ClusterResource -Name "Cluster Pool 1" | Remove-ClusterResource
```

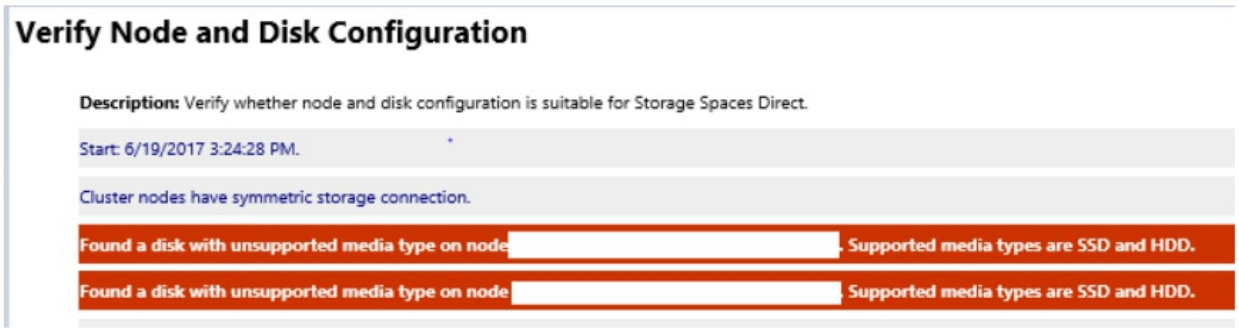
Now, if you run **Get-PhysicalDisk** on any of the nodes, you'll see all the disks that were in the pool. For example, in a lab with a 4-Node cluster with 4 SAS disks, 100GB each presented to each node. In that case, after Storage Space Direct is disabled, which removes the SBL (Storage Bus Layer) but leaves the filter, if you run **Get-PhysicalDisk**, it should report 4 disks excluding the local OS disk. Instead it reported 16 instead. This is the same for all nodes in the cluster. When you run a **Get-Disk** command, you'll see the locally attached disks numbered as 0, 1, 2 and so on, as seen in this sample output:

| NUMBER | FRIENDLY NAME | SERIAL NUMBER | HEALTHSTATUS | OPERATIONAL STATUS | TOTAL SIZE | PARTITION STYLE |
|---|---|---|---|---|---|---|
| 0 | Msft Virtu... | | Healthy | Online | 127 GB | GPT |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| 1 | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| 2 | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| 4 | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| 3 | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |
| | Msft Virtu... | | Healthy | Offline | 100 GB | RAW |

# Error message about "unsupported media type" when you create an Storage Spaces Direct cluster using Enable-ClusterS2D

You might see errors similar to this when you run the **Enable-ClusterS2D** cmdlet:




To fix this issue, ensure the HBA adapter is configured in HBA mode. No HBA should be configured in RAID mode.

# Enable-ClusterStorageSpacesDirect hangs at 'Waiting until SBL disks are surfaced' or at 27%

You will see the following information in the validation report:

Disk `<identifier>` connected to node `<nodename>` returned a SCSI Port Association and the corresponding enclosure device could not be found. The hardware is not compatible with Storage Spaces Direct (S2D), contact the hardware vendor to verify support for SCSI Enclosure Services (SES).

The issue is with the HPE SAS expander card that lies between the disks and the HBA card. The SAS expander creates a duplicate ID between the first drive connected to the expander and the expander itself. This has been resolved in HPE Smart Array Controllers SAS Expander Firmware: 4.02.

# Intel SSD DC P4600 series has a non-unique NGUID

You might see an issue where an Intel SSD DC P4600 series device seems to be reporting similar 16 byte NGUID for multiple namespaces such as 0100000001000000E4D25C000014E214 or 0100000001000000E4D25C0000EEE214 in the example below.

| UNIQUEID | DEVICEID | MEDIATYPE | BUSTYPE | SERIALNUMBER | SIZE | CANPOOL | FRIENDLYNAME | OPERATIONALSTATUS |
|---|---|---|---|---|---|---|---|---|
| 5000CCA251D12E30 | 0 | HDD | SAS | 7PKR197G | 10000831348736 | False | HGST | HUH721010AL4200 |

| UNIQUEID | DEVICEID | MEDIATYPE | BUSTYPE | SERIALNUMBER | SIZE | CANPOOL | FRIENDLYNAME | OPERATIONALSTATUS |
|---|---|---|---|---|---|---|---|---|
| eui.0100000000100000E4D25C000014E214 | 4 | SSD | NVMe | 0100_0000_0100_0000_E4D2_5C00_0014_E214. | 1600321314816 | True | INTEL | SSDPE2KE016T7 |
| eui.0100000000100000E4D25C000014E214 | 5 | SSD | NVMe | 0100_0000_0100_0000_E4D2_5C00_0014_E214. | 1600321314816 | True | INTEL | SSDPE2KE016T7 |
| eui.0100000000100000E4D25C0000EEE214 | 6 | SSD | NVMe | 0100_0000_0100_0000_E4D2_5C00_00EE_E214. | 1600321314816 | True | INTEL | SSDPE2KE016T7 |
| eui.0100000000100000E4D25C0000EEE214 | 7 | SSD | NVMe | 0100_0000_0100_0000_E4D2_5C00_00EE_E214. | 1600321314816 | True | INTEL | SSDPE2KE016T7 |

To fix this issue, update the firmware on the Intel drives to the latest version. Firmware version QDV101B1 from May 2018 is known to resolve this issue.

The May 2018 release of the Intel SSD Data Center Tool includes a firmware update, QDV101B1, for the Intel SSD DC P4600 series.

## Physical Disk "Healthy," and Operational Status is "Removing from Pool"

In a Windows Server 2016 Storage Spaces Direct cluster, you might see the HealthStatus for one ore more physical disks as "Healthy," while the OperationalStatus is "(Removing from Pool, OK)."

"Removing from Pool" is an intent set when **Remove-PhysicalDisk** is called but stored in Health to maintain state and allow recovery if the remove operation fails. You can manually change the OperationalStatus to Healthy with one of the following methods:

- Remove the physical disk from the pool, and then add it back.
- Import-Module Clear-PhysicalDiskHealthData.ps1
- Run the Clear-PhysicalDiskHealthData.ps1 script to clear the intent. (Available for download as a .TXT file. You'll need to save it as a .PS1 file before you can run it.)

Here are some examples showing how to run the script:

- Use the **SerialNumber** parameter to specify the disk you need to set to Healthy. You can get the serial number from **WMI MSFT_PhysicalDisk** or **Get-PhysicalDIsk**. (We're just using 0s for the serial number below.)

  ```
  Clear-PhysicalDiskHealthData -Intent -Policy -SerialNumber 000000000000000 -Verbose -Force
  ```

- Use the **UniqueId** parameter to specify the disk (again from **WMI MSFT_PhysicalDisk** or **Get-**

PhysicalDIsk).

```
Clear-PhysicalDiskHealthData -Intent -Policy -UniqueId 00000000000000000 -Verbose -Force
```

## File copy is slow

You might seen an issue using File Explorer to copy a large VHD to the virtual disk - the file copy is taking longer than expected.

Using File Explorer, Robocopy or Xcopy to copy a large VHD to the virtual disk is not a recommended method to as this will result in slower than expected performance. The copy process does not go through the Storage Spaces Direct stack, which sits lower on the storage stack, and instead acts like a local copy process.

If you want to test Storage Spaces Direct performance, we recommend using VMFleet and Diskspd to load and stress test the servers to get a base line and set expectations of the Storage Spaces Direct performance.

## Expected events that you would see on rest of the nodes during the reboot of a node.

It is safe to ignore these events:

```
Event ID 205: Windows lost communication with physical disk {XXXXXXXXXXXXXXXXXXX }. This can occur if a cable
failed or was disconnected, or if the disk itself failed.

Event ID 203: Windows lost communication with physical disk {xxxxxxxxxxxxxxxxxxxxxxx }. This can occur if a
cable failed or was disconnected, or if the disk itself failed.
```

If you're running Azure VMs, you can ignore this event:

```
Event ID 32: The driver detected that the device \Device\Harddisk5\DR5 has its write cache enabled. Data
corruption may occur.
```

## Slow performance or "Lost Communication," "IO Error," "Detached," or "No Redundancy" errors for deployments that use Intel P3x00 NVMe devices

We've identified a critical issue that affects some Storage Spaces Direct users who are using hardware based on the Intel P3x00 family of NVM Express (NVMe) devices with firmware versions before "Maintenance Release 8."

> **NOTE**
> Individual OEMs may have devices that are based on the Intel P3x00 family of NVMe devices with unique firmware version strings. Contact your OEM for more information of the latest firmware version.

If you are using hardware in your deployment based on the Intel P3x00 family of NVMe devices, we recommend that you immediately apply the latest available firmware (at least Maintenance Release 8). This Microsoft Support article provides additional information about this issue.

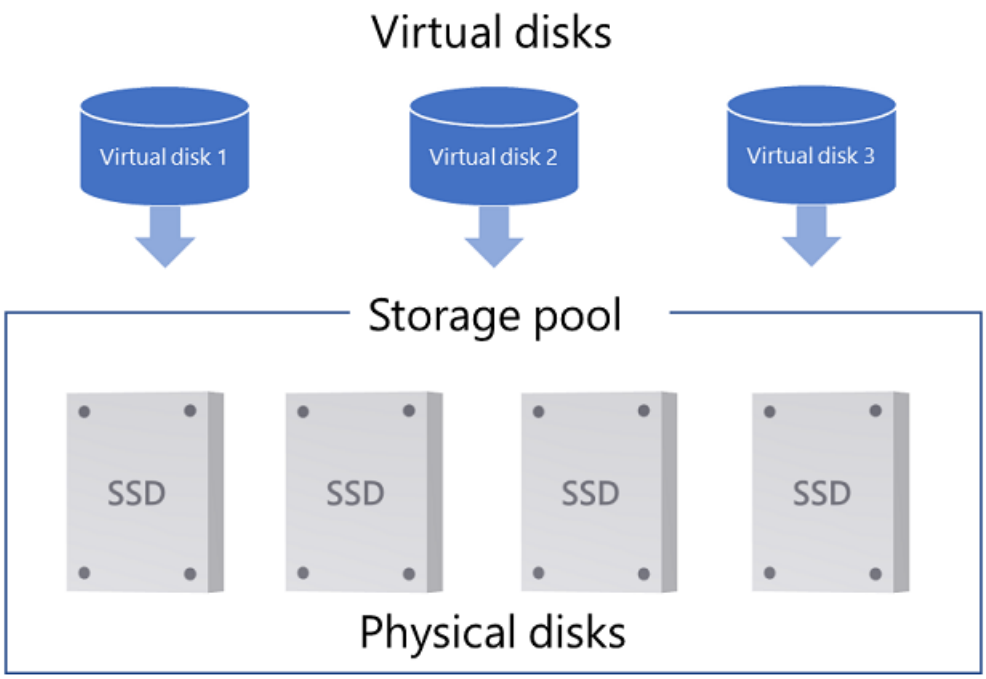
# Troubleshoot Storage Spaces and Storage Spaces Direct health and operational states

12/16/2020 • 14 minutes to read • Edit Online

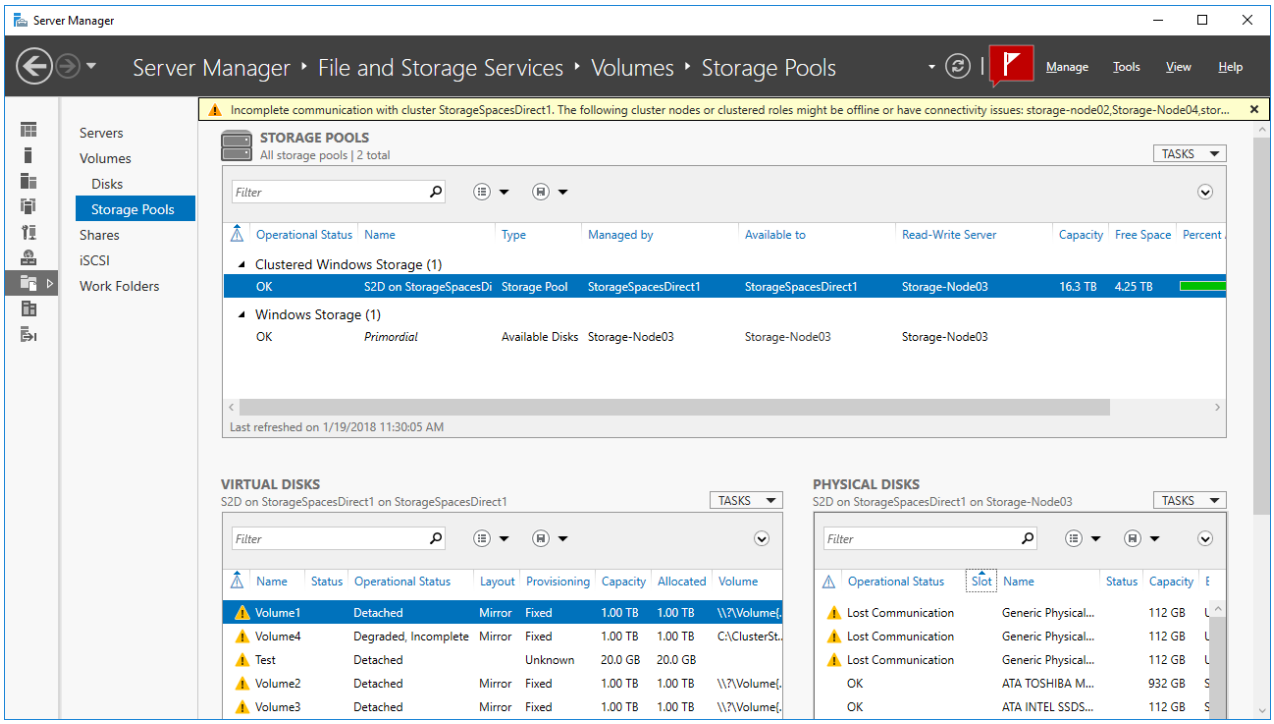
Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server (Semi-Annual Channel), Windows 10, Windows 8.1

This topic describes the health and operational states of storage pools, virtual disks (which sit underneath volumes in Storage Spaces), and drives in Storage Spaces Direct and Storage Spaces. These states can be invaluable when trying to troubleshoot various issues such as why you can't delete a virtual disk because of a read-only configuration. It also discusses why a drive can't be added to a pool (the CannotPoolReason).

Storage Spaces has three primary objects - *physical disks* (hard drives, SSDs, etc.) that are added to a *storage pool*, virtualizing the storage so that you can create *virtual disks* from free space in the pool, as shown here. Pool metadata is written to each drive in the pool. Volumes are created on top of the virtual disks and store your files, but we're not going to talk about volumes here.




You can view health and operational states in Server Manager, or with PowerShell. Here's an example of a variety of (mostly bad) health and operational states on a Storage Spaces Direct cluster that's missing most of its cluster nodes (right-click the column headers to add **Operational Status**). This isn't a happy cluster.




# Storage pool states

Every storage pool has a health status - **Healthy**, **Warning**, or **Unknown/Unhealthy**, as well as one or more operational states.

To find out what state a pool is in, use the following PowerShell commands:

```
Get-StoragePool -IsPrimordial $False | Select-Object HealthStatus, OperationalStatus, ReadOnlyReason
```

Here's an example output showing a storage pool in the Unknown health state with the Read-only operational status:

```
FriendlyName                OperationalStatus HealthStatus IsPrimordial IsReadOnly
------------                ----------------- ------------ ------------ ----------
S2D on StorageSpacesDirect1 Read-only         Unknown      False        True
```

The following sections list the health and operational states.

### Pool health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| OK | The storage pool is healthy. |

### Pool health state: Warning

When the storage pool is in the **Warning** health state, it means that the pool is accessible, but one or more drives failed or are missing. As a result, your storage pool might have reduced resilience.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Degraded | There are failed or missing drives in the storage pool. This condition occurs only with drives hosting pool metadata.<br><br>**Action**: Check the state of your drives and replace any failed drives before there are additional failures. |

**Pool health state: Unknown or Unhealthy**

When a storage pool is in the **Unknown** or **Unhealthy** health state, it means that the storage pool is read-only and can't be modified until the pool is returned to the **Warning** or **OK** health states.

| OPERATIONAL STATE | READ-ONLY REASON | DESCRIPTION |
| --- | --- | --- |
| Read-only | Incomplete | This can occur if the storage pool loses its quorum, which means that most drives in the pool have failed or are offline for some reason. When a pool loses its quorum, Storage Spaces automatically sets the pool configuration to read-only until enough drives become available again.<br><br>**Action:**<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring all servers online.<br>2. Set the pool back to read-write by opening a PowerShell session with administrative permissions and then typing:<br><br>`Get-StoragePool -IsPrimordial $False \| Set-StoragePool -IsReadOnly $false` |
| | Policy | An administrator set the storage pool to read-only.<br><br>**Action:** To set a clustered storage pool to read-write access in Failover Cluster Manager, go to **Pools**, right-click the pool and then select **Bring Online**.<br><br>For other servers and PCs, open a PowerShell session with administrative permissions and then type:<br><br>`Get-StoragePool \| Set-StoragePool -IsReadOnly $false` |

| OPERATIONAL STATE | READ-ONLY REASON | DESCRIPTION |
|---|---|---|
| | Starting | Storage Spaces is starting or waiting for drives to be connected in the pool. This should be a temporary state. Once completely started, the pool should transition to a different operational state.<br><br>**Action:** If the pool stays in the *Starting* state, make sure that all drives in the pool are connected properly. |

See also, the Windows Server storage forum.

## Virtual disk states

In Storage Spaces, volumes are placed on virtual disks (storage spaces) that are carved out of free space in a pool. Every virtual disk has a health status - **Healthy**, **Warning**, **Unhealthy**, or **Unknown** as well as one or more operational states.

To find out what state virtual disks are in, use the following PowerShell commands:

```
Get-VirtualDisk | Select-Object FriendlyName,HealthStatus, OperationalStatus, DetachedReason
```

Here's an example of output showing a detached virtual disk and a degraded/incomplete virtual disk:

```
FriendlyName HealthStatus OperationalStatus      DetachedReason
------------ ------------ -----------------      --------------
Volume1      Unknown      Detached               By Policy
Volume2      Warning      {Degraded, Incomplete} None
```

The following sections list the health and operational states.

#### Virtual disk health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
|---|---|
| OK | The virtual disk is healthy. |
| Suboptimal | Data isn't written evenly across drives.<br><br>**Action**: Optimize drive usage in the storage pool by running the Optimize-StoragePool cmdlet. |

#### Virtual disk health state: Warning

When the virtual disk is in a **Warning** health state, it means that one or more copies of your data are unavailable, but Storage Spaces can still read at least one copy of your data.

| OPERATIONAL STATE | DESCRIPTION |
|---|---|
| In service | Windows is repairing the virtual disk, such as after adding or removing a drive. When the repair is complete, the virtual disk should return to the OK health state. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Incomplete | The resilience of the virtual disk is reduced because one or more drives failed or are missing. However, the missing drives contain up-to-date copies of your data.<br><br>**Action**:<br>1. Reconnect any missing drives, replace any failed drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive. |
| Degraded | The resilience of the virtual disk is reduced because one or more drives failed or are missing, and there are outdated copies of your data on these drives.<br><br>**Action**:<br>1. Reconnect any missing drives, replace any failed drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive. |

### Virtual disk health state: Unhealthy

When a virtual disk is in an **Unhealthy** health state, some or all of the data on the virtual disk is currently inaccessible.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| No redundancy | The virtual disk has lost data because too many drives failed.<br><br>**Action**: Replace failed drives and then restore your data from backup. |

### Virtual disk health state: Information/Unknown

The virtual disk can also be in the **Information** health state (as shown in the Storage Spaces Control Panel item) or **Unknown** health state (as shown in PowerShell) if an administrator took the virtual disk offline or the virtual disk has become detached.

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
| --- | --- | --- |

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
| --- | --- | --- |
| Detached | By Policy | An administrator took the virtual disk offline, or set the virtual disk to require manual attachment, in which case you'll have to manually attach the virtual disk every time Windows restarts.,<br><br>**Action**: Bring the virtual disk back online. To do so when the virtual disk is in a clustered storage pool, in Failover Cluster Manager select **Storage** > **Pools** > **Virtual Disks**, select the virtual disk that shows the **Offline** status and then select **Bring Online**.<br><br>To bring a virtual disk back online when not in a cluster, open a PowerShell session as an Administrator and then try using the following command:<br><br>`Get-VirtualDisk \| Where-Object -Filter { $_.OperationalStatus -eq "Detached" } \| Connect-VirtualDisk`<br><br>To automatically attach all non-clustered virtual disks after Windows restarts, open a PowerShell session as an Administrator and then use the following command:<br><br>`Get-VirtualDisk \| Set-VirtualDisk -ismanualattach $false` |
| | Majority Disks Unhealthy | Too many drives used by this virtual disk failed, are missing, or have stale data.<br><br>**Action**:<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. After all drives and servers are online, replace any failed drives. See Health Service for details.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive.<br>3. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br><br>If more disks failed than you have copies of your data and the virtual disk wasn't repaired in-between failures, all data on the virtual disk is permanently lost. In this unfortunate case, delete the virtual disk, create a new virtual disk, and then restore from a backup. |

| OPERATIONAL STATE | DETACHED REASON | DESCRIPTION |
|---|---|---|
| | Incomplete | Not enough drives are present to read the virtual disk.<br><br>**Action**:<br>1. Reconnect any missing drives, and if you're using Storage Spaces Direct, bring online any servers that are offline.<br>2. After all drives and servers are online, replace any failed drives. See Health Service for details.<br>Storage Spaces Direct automatically starts a repair if needed after reconnecting or replacing a drive.<br>3. If you're not using Storage Spaces Direct, next repair the virtual disk using the Repair-VirtualDisk cmdlet.<br><br>If more disks failed than you have copies of your data and the virtual disk wasn't repaired in-between failures, all data on the virtual disk is permanently lost. In this unfortunate case, delete the virtual disk, create a new virtual disk, and then restore from a backup. |
| | Timeout | Attaching the virtual disk took too long<br><br>**Action:** This shouldn't happen often, so you might try see if the condition passes in time. Or you can try disconnecting the virtual disk with the Disconnect-VirtualDisk cmdlet, then using the Connect-VirtualDisk cmdlet to reconnect it. |

## Drive (physical disk) states

The following sections describe the health states a drive can be in. Drives in a pool are represented in PowerShell as *physical disk* objects.

### Drive health state: Healthy

| OPERATIONAL STATE | DESCRIPTION |
|---|---|
| OK | The drive is healthy. |
| In service | The drive is performing some internal housekeeping operations. When the action is complete, the drive should return to the *OK* health state. |

### Drive health state: Warning

A drive in the Warning state can read and write data successfully but has an issue.

| OPERATIONAL STATE | DESCRIPTION |
|---|---|

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Lost communication | The drive is missing. If you're using Storage Spaces Direct, this could be because a server is down.<br><br>**Action**: If you're using Storage Spaces Direct, bring all servers back online. If that doesn't fix it, reconnect the drive, replace it, or try getting detailed diagnostic info about this drive by following the steps in Troubleshooting using Windows Error Reporting > Physical disk timed out. |
| Removing from pool | Storage Spaces is in the process of removing the drive from its storage pool.<br><br>This is a temporary state. After the removal is complete, if the drive is still attached to the system, the drive transitions to another operational state (usually OK) in a primordial pool. |
| Starting maintenance mode | Storage Spaces is in the process of putting the drive in maintenance mode after an administrator put the drive in maintenance mode. This is a temporary state - the drive should soon be in the *In maintenance mode* state. |
| In maintenance mode | An administrator placed the drive in maintenance mode, halting reads and writes from the drive. This is usually done before updating drive firmware, or when testing failures.<br><br>**Action**: To take the drive out of maintenance mode, use the Disable-StorageMaintenanceMode cmdlet. |
| Stopping maintenance mode | An administrator took the drive out of maintenance mode, and Storage Spaces is in the process of bringing the drive back online. This is a temporary state - the drive should soon be in another state - ideally *Healthy*. |
| Predictive failure | The drive reported that it's close to failing.<br><br>**Action**: Replace the drive. |
| IO error | There was a temporary error accessing the drive.<br><br>**Action**:<br>1. If the drive doesn't transition back to the **OK** state, you can try using the Reset-PhysicalDisk cmdlet to wipe the drive.<br>2. Use Repair-VirtualDisk to restore the resiliency of affected virtual disks.<br>3. If this keeps happening, replace the drive. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Transient error | There was a temporary error with the drive. This usually means the drive was unresponsive, but it could also mean that the Storage Spaces protective partition was inappropriately removed from the drive.<br><br>**Action**:<br>1. If the drive doesn't transition back to the **OK** state, you can try using the Reset-PhysicalDisk cmdlet to wipe the drive.<br>2. Use Repair-VirtualDisk to restore the resiliency of affected virtual disks.<br>3. If this keeps happening, replace the drive, or try getting detailed diagnostic info about this drive by following the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Abnormal latency | The drive is performing slowly, as measured by the Health Service in Storage Spaces Direct.<br><br>**Action**: If this keeps happening, replace the drive so it doesn't reduce the performance of Storage Spaces as a whole. |

### Drive health state: Unhealthy

A drive in the Unhealthy state can't currently be written to or accessed.

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Not usable | This drive can't be used by Storage Spaces. For more info see Storage Spaces Direct hardware requirements; if you're not using Storage Spaces Direct, see Storage Spaces overview. |
| Split | The drive has become separated from the pool.<br><br>**Action**: Reset the drive, erasing all data from the drive and adding it back to the pool as an empty drive. To do so, open a PowerShell session as an administrator, run the Reset-PhysicalDisk cmdlet, and then run Repair-VirtualDisk.<br><br>To get detailed diagnostic info about this drive, follow the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Stale metadata | Storage Spaces found old metadata on the drive.<br><br>**Action**: This should be a temporary state. If the drive doesn't transition back to OK, you can run Repair-VirtualDisk to start a repair operation on affected virtual disks. If that doesn't resolve the issue, you can reset the drive with the Reset-PhysicalDisk cmdlet, wiping all data from the drive, and then run Repair-VirtualDisk. |
| Unrecognized metadata | Storage Spaces found unrecognized metadata on the drive, which usually means that the drive has metadata from a different pool on it.<br><br>**Action**: To wipe the drive and add it to the current pool, reset the drive. To reset the drive, open a PowerShell session as an administrator, run the Reset-PhysicalDisk cmdlet, and then run Repair-VirtualDisk. |

| OPERATIONAL STATE | DESCRIPTION |
| --- | --- |
| Failed media | The drive failed and won't be used by Storage Spaces anymore.<br><br>**Action**: Replace the drive.<br><br>To get detailed diagnostic info about this drive, follow the steps in Troubleshooting using Windows Error Reporting > Physical disk failed to come online. |
| Device hardware failure | There was a hardware failure on this drive.<br><br>**Action**: Replace the drive. |
| Updating firmware | Windows is updating the firmware on the drive. This is a temporary state that usually lasts less than a minute and during which time other drives in the pool handle all reads and writes. For more info, see Update drive firmware. |
| Starting | The drive is getting ready for operation. This should be a temporary state - once complete, the drive should transition to a different operational state. |

## Reasons a drive can't be pooled

Some drives just aren't ready to be in a storage pool. You can find out why a drive isn't eligible for pooling by looking at the `CannotPoolReason` property of a physical disk. Here's an example PowerShell script to display the CannotPoolReason property:

```
Get-PhysicalDisk | Format-Table FriendlyName,MediaType,Size,CanPool,CannotPoolReason
```

Here's an example output:

```
FriendlyName          MediaType          Size CanPool CannotPoolReason
------------          ---------          ---- ------- ----------------
ATA MZ7LM120HCFD00D3  SSD        120034123776   False Insufficient Capacity
Msft Virtual Disk     SSD         10737418240    True
Generic Physical Disk SSD        119990648832   False In a Pool
```

The following table gives a little more detail on each of the reasons.

| REASON | DESCRIPTION |
| --- | --- |

| REASON | DESCRIPTION |
| --- | --- |
| In a pool | The drive already belongs to a storage pool.<br><br>Drives can belong to only a single storage pool at a time. To use this drive in another storage pool, first remove the drive from its existing pool, which tells Storage Spaces to move the data on the drive to other drives on the pool. Or reset the drive if the drive has been disconnected from its pool without notifying Storage Spaces.<br><br>To safely remove a drive from a storage pool, use Remove-PhysicalDisk, or go to Server Manager > **File and Storage Services** > **Storage Pools**, > **Physical Disks**, right-click the drive and then select **Remove Disk**.<br><br>To reset a drive, use Reset-PhysicalDisk. |
| Not healthy | The drive isn't in a healthy state and might need to be replaced. |
| Removable media | The drive is classified as a removable drive.<br><br>Storage Spaces doesn't support media that are recognized by Windows as removable, such as Blu-Ray drives. Although many fixed drives are in removable slots, in general, media that are *classified* by Windows as removable aren't suitable for use with Storage Spaces. |
| In use by cluster | The drive is currently used by a Failover Cluster. |
| Offline | The drive is offline.<br><br>To bring all offline drives online and set to read/write, open a PowerShell session as an administrator and use the following scripts:<br><br>`Get-Disk \| Where-Object -Property OperationalStatus -EQ "Offline" \| Set-Disk -IsOffline $false`<br><br>`Get-Disk \| Where-Object -Property IsReadOnly -EQ $true \| Set-Disk -IsReadOnly $false` |
| Insufficient capacity | This typically occurs when there are partitions taking up the free space on the drive.<br><br>**Action**: Delete any volumes on the drive, erasing all data on the drive. One way to do that is to use the Clear-Disk PowerShell cmdlet. |
| Verification in progress | The Health Service is checking to see if the drive or firmware on the drive is approved for use by the server administrator. |
| Verification failed | The Health Service couldn't check to see if the drive or firmware on the drive is approved for use by the server administrator. |
| Firmware not compliant | The firmware on the physical drive isn't in the list of approved firmware revisions specified by the server administrator by using the Health Service. |

| REASON | DESCRIPTION |
| --- | --- |
| Hardware not compliant | The drive isn't in the list of approved storage models specified by the server administrator by using the Health Service. |

## Additional References

- Storage Spaces Direct
- Storage Spaces Direct hardware requirements
- Understanding cluster and pool quorum

# Collect diagnostic data with Storage Spaces Direct

11/2/2020 • 5 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016

There are various diagnostic tools that can be used to collect the data needed to troubleshoot Storage Spaces Direct and Failover Cluster. In this article, we will focus on **Get-SDDCDiagnosticInfo** - a one touch tool that will gather all relevant information to help you diagnose your cluster.

Given that the logs and other information that **Get-SDDCDiagnosticInfo** are dense, the information on troubleshooting presented below will be helpful for troubleshooting advanced issues that have been escalated and that may require data to be sent to Microsoft for triaging.

## Installing Get-SDDCDiagnosticInfo

The **Get-SDDCDiagnosticInfo** PowerShell cmdlet (a.k.a. **Get-PCStorageDiagnosticInfo**, previously known as **Test-StorageHealth**) can be used to gather logs for and perform health checks for Failover Clustering (Cluster, Resources, Networks, Nodes), Storage Spaces (Physical Disks, Enclosures, Virtual Disks), Cluster Shared Volumes, SMB File Shares, and Deduplication.

There are two methods of installing the script, both of which are outlines below.

### PowerShell Gallery

The PowerShell Gallery is a snapshot of the GitHub Repo. Note that installing items from the PowerShell Gallery requires the latest version of the PowerShellGet module, which is available in Windows 10, in Windows Management Framework (WMF) 5.0, or in the MSI-based installer (for PowerShell 3 and 4).

We install the latest version of the Microsoft Networking Diagnostics tools during this process as well since Get-SDDCDiagnosticInfo relies on this. This manifest module contains network diagnostic and troubleshooting tool, which are maintained by the Microsoft Core Networking Product Group at Microsoft.

You can install the module by running following command in PowerShell with administrator privileges:

```
Install-PackageProvider NuGet -Force
Install-Module PrivateCloud.DiagnosticInfo -Force
Import-Module PrivateCloud.DiagnosticInfo -Force
Install-Module -Name MSFT.Network.Diag
```

To update the module, run the following command in PowerShell:

```
Update-Module PrivateCloud.DiagnosticInfo
```

### GitHub

The GitHub Repo is the most up-to-date version of the module, since we are continually iterating here. To install the module from GitHub, download the latest module from the archive and extract the PrivateCloud.DiagnosticInfo directory to the correct PowerShell modules path pointed by `$env:PSModulePath`

```
# Allowing Tls12 and Tls11 -- e.g. github now requires Tls12
# If this is not set, the Invoke-WebRequest fails with "The request was aborted: Could not create SSL/TLS
secure channel."
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$module = 'PrivateCloud.DiagnosticInfo'
Invoke-WebRequest -Uri https://github.com/PowerShell/$module/archive/master.zip -OutFile $env:TEMP\master.zip
Expand-Archive -Path $env:TEMP\master.zip -DestinationPath $env:TEMP -Force
if (Test-Path $env:SystemRoot\System32\WindowsPowerShell\v1.0\Modules\$module) {
    rm -Recurse $env:SystemRoot\System32\WindowsPowerShell\v1.0\Modules\$module -ErrorAction Stop
    Remove-Module $module -ErrorAction SilentlyContinue
} else {
    Import-Module $module -ErrorAction SilentlyContinue
}
if (-not ($m = Get-Module $module -ErrorAction SilentlyContinue)) {
    $md = "$env:ProgramFiles\WindowsPowerShell\Modules"
} else {
    $md = (gi $m.ModuleBase -ErrorAction SilentlyContinue).PsParentPath
    Remove-Module $module -ErrorAction SilentlyContinue
    rm -Recurse $m.ModuleBase -ErrorAction Stop
}
cp -Recurse $env:TEMP\$module-master\$module $md -Force -ErrorAction Stop
rm -Recurse $env:TEMP\$module-master,$env:TEMP\master.zip
Import-Module $module -Force
```

If you need to get this module on an offline cluster, download the zip, move it to your target server node, and install the module.

## Gathering Logs

After you have enabled event channels and completed the installation process, you can use the Get-SDDCDiagnosticInfo PowerShell cmdlet in the module to get:

- Reports on storage health, plus details on unhealthy components
- Reports of storage capacity by pool, volume and deduplicated volume
- Event logs from all cluster nodes and a summary error report

Assume that your storage cluster has the name *"CLUS01"*.

To execute against a remote storage cluster:

```
Get-SDDCDiagnosticInfo -ClusterName CLUS01
```

To execute locally on clustered storage node:

```
Get-SDDCDiagnosticInfo
```

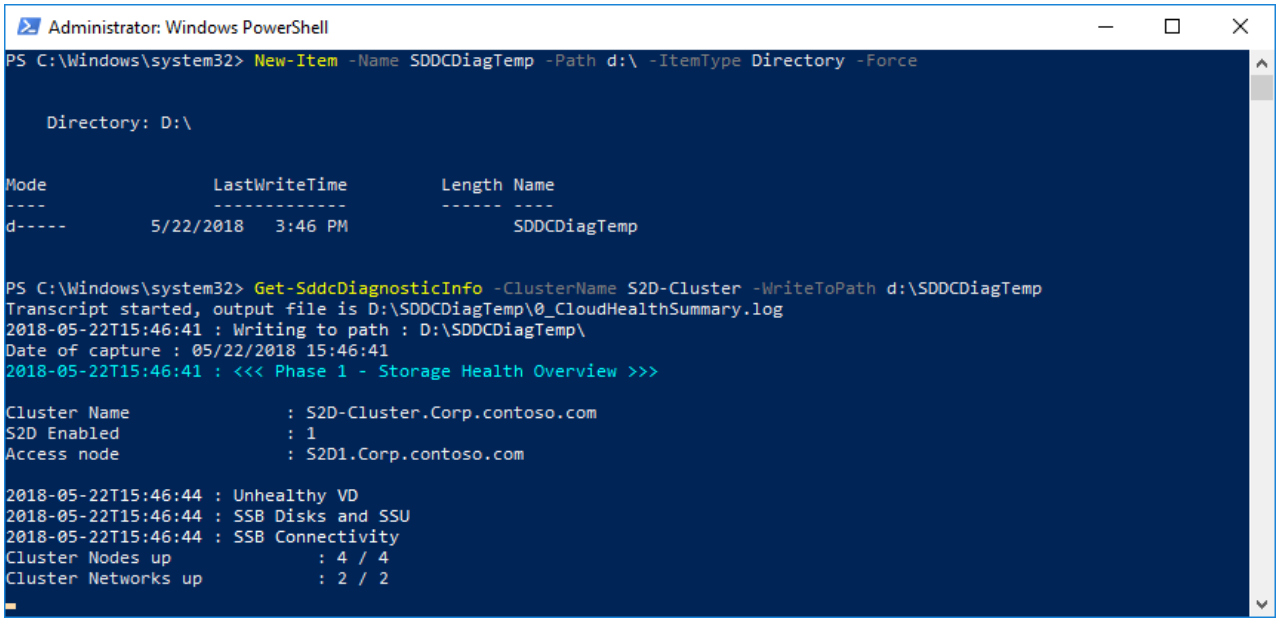
To save results to a specified folder:

```
Get-SDDCDiagnosticInfo -WriteToPath D:\Folder
```

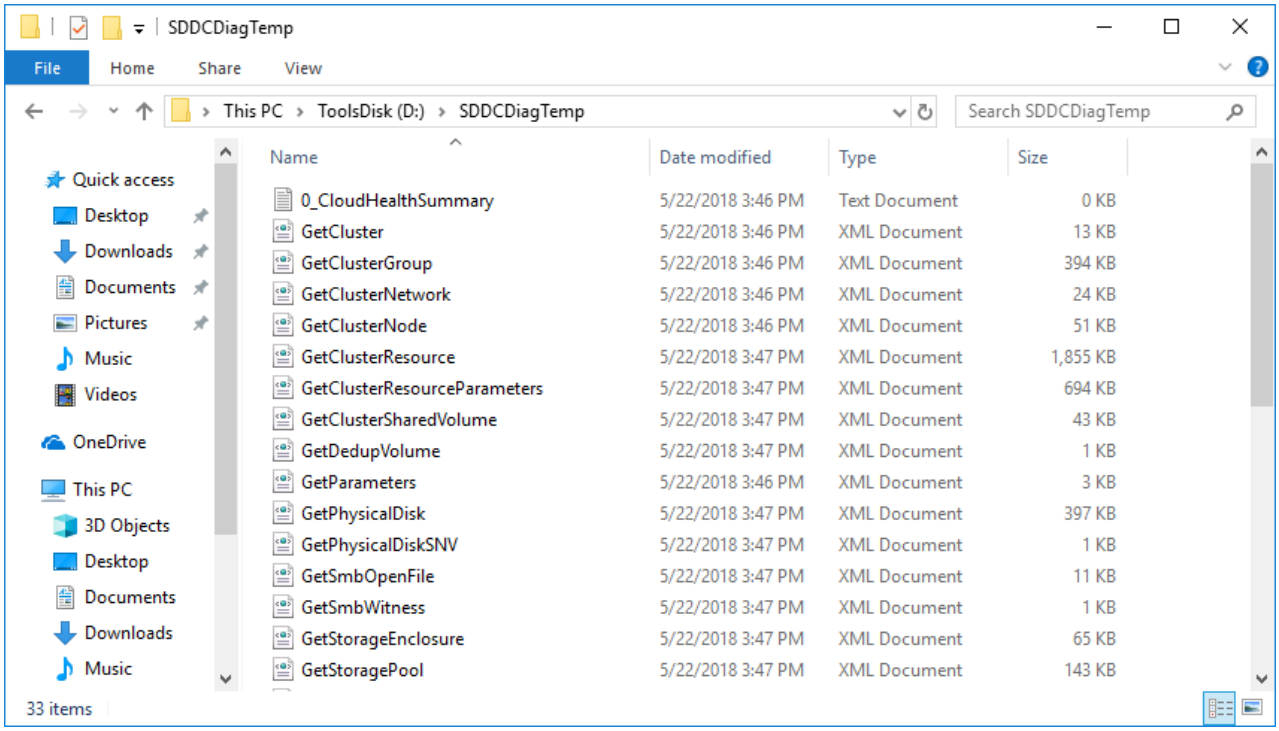
Here is an example of how this looks on a real cluster:

```
New-Item -Name SDDCDiagTemp -Path d:\ -ItemType Directory -Force
Get-SddcDiagnosticInfo -ClusterName S2D-Cluster -WriteToPath d:\SDDCDiagTemp
```

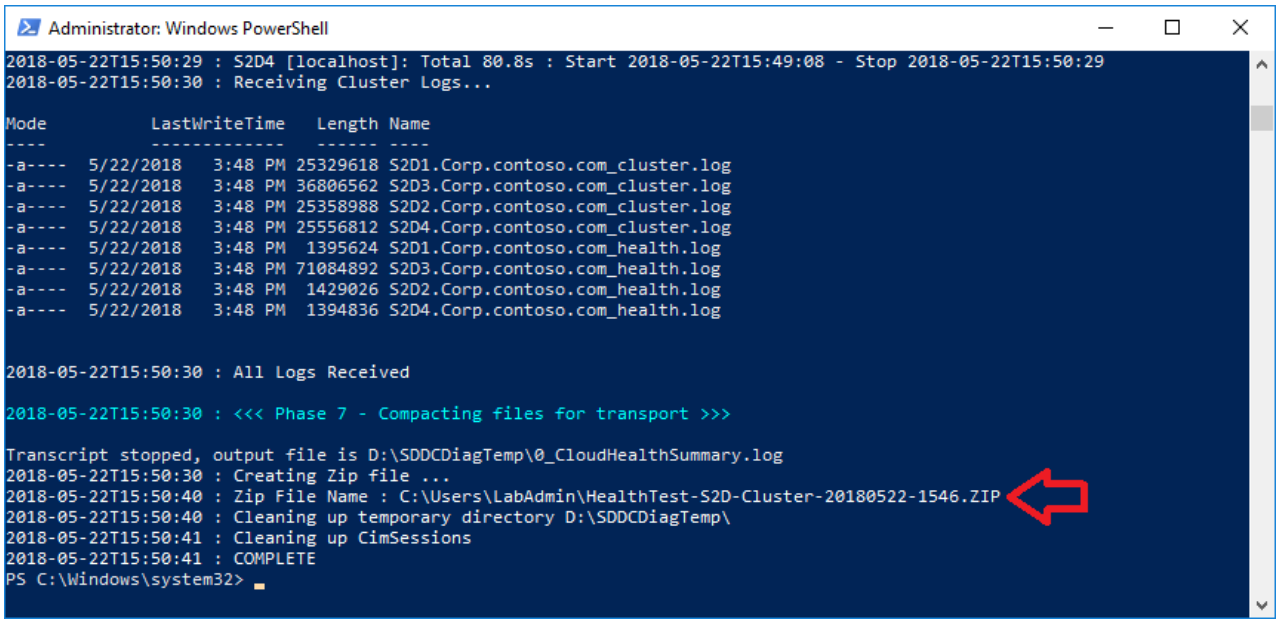
As you can see, script will also do validation of current cluster state




As you can see, all data are being written to SDDCDiagTemp folder




After script will finish, it will create ZIP in your users directory



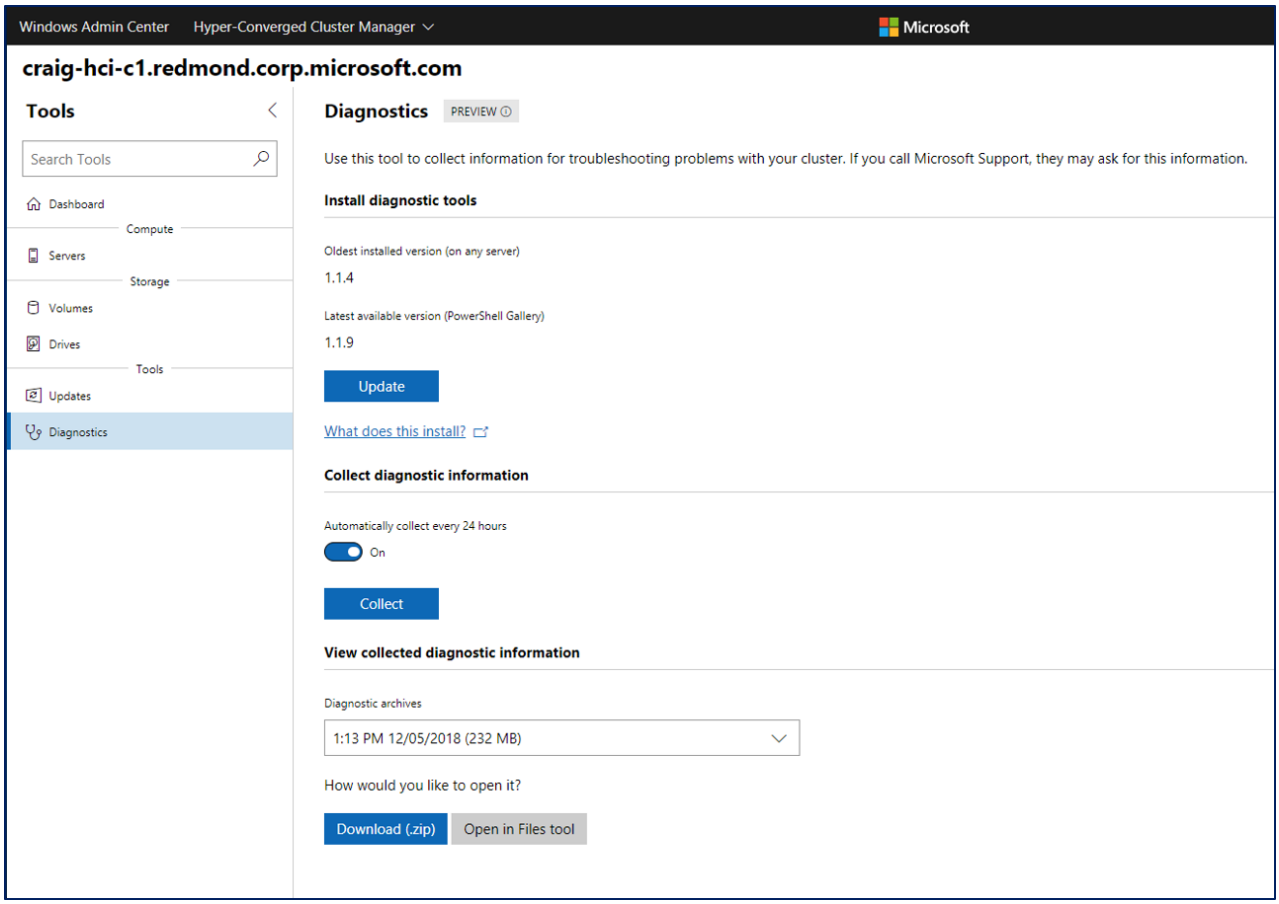

Let's generate a report into a text file

```
#find the latest diagnostic zip in UserProfile
    $DiagZip=(get-childitem $env:USERPROFILE | where Name -like HealthTest*.zip)
    $LatestDiagPath=($DiagZip | sort lastwritetime | select -First 1).FullName
#expand to temp directory
    New-Item -Name SDDCDiagTemp -Path d:\ -ItemType Directory -Force
    Expand-Archive -Path $LatestDiagPath -DestinationPath D:\SDDCDiagTemp -Force
#generate report and save to text file
    $report=Show-SddcDiagnosticReport -Path D:\SDDCDiagTemp
    $report | out-file d:\SDDCReport.txt
```

For reference, here is a link to the sample report and sample zip.

To view this in Windows Admin Center (version 1812 onwards), navigate to the *Diagnostics* tab. As you see in the screenshot below, you can

- Install diagnostic tools
- Update them (if they are out-of-date),
- Schedule daily diagnostic runs (these have a low impact on your system, usually take <5 minutes in the background, and won't take up more than 500mb on your cluster)
- View previously collected diagnostic information if you need to give it to support or analyze it yourself.




# Get-SDDCDiagnosticInfo output

The following are the files included in the zipped output of Get-SDDCDiagnosticInfo.

### Health Summary Report

The health summary report is saved as:

- 0_CloudHealthSummary.log

This file is generated after parsing all the data collected and is meant to provide a quick summary of your system. It contains:

- System information
- Storage health overview (number of nodes up, resources online, cluster shared volumes online, unhealthy components, etc.)
- Details on unhealthy components (cluster resources that are offline, failed, or online pending)
- Firmware and driver information
- Pool, physical disk, and volume details
- Storage Performance (performance counters are collected)

This report is being continually updated to include more useful information. For the latest information, see the GitHub README.

### Logs and XML files

The script runs various log gathering scripts and saves the output as xml files. We collect cluster and health logs, system information (MSInfo32), unfiltered event logs (failover clustering, dis diagnostics, hyper-v, storage spaces, and more), and storage diagnostics information (operational logs). For the latest information on what information is collected, see the GitHub README (what we collect).

# How to consume the XML files from Get-PCStorageDiagnosticInfo

You can consume the data from the XML files provided in data collected by the **Get-PCStorageDiagnosticInfo** cmdlet. These files have information about the virtual disks, physical disks, basic cluster info and other PowerShell related outputs.

To see the results of these outputs, open a PowerShell window and run the following steps.

```
ipmo storage
$d = import-clixml <filename>
$d
```

## What to expect next?

A lot of improvements and new cmdlets to analyze SDDC system health. Provide feedback on what you'd like to see by filing issues here. Also, feel free to contribute helpful changes to the script, by submitting a pull request.

# Storage Spaces Direct - Frequently asked questions (FAQ)

11/2/2020 • 4 minutes to read • Edit Online

This article lists some common and frequently asked questions related to Storage Spaces Direct.

## When you use Storage Spaces Direct with 3 nodes, can you get both performance and capacity tiers?

Yes, you can get both a performance and capacity tier in a 2-node or 3-node Storage Spaces Direct configuration. However, you must make sure that you have 2 capacity devices. That means that you must use all the three types of devices: NVME, SSD, and HDD.

## Refs file system provides real-time tiering with Storage Spaces Direct. Does REFS provide the same functionality with shared storage spaces in 2016?

No, you won't get real-time tiering with shared storage spaces with 2016. This is only for Storage Spaces Direct.

## Can I use an NTFS file system with Storage Spaces Direct?

Yes, you can use the NTFS file system with Storage Spaces Direct. However, REFS is recommended. NTFS does not provide real-time tiering.

## I have configured 2 node Storage Spaces Direct clusters, where the virtual disk is configured as 2-way mirror resiliency. If I add a new fault domain, will the resiliency of the existing virtual disk change?

After you have added the new fault domain, the new virtual disks that you create will jump to a 3-way mirror. However, the existing virtual disk will remain a 2-way mirrored disk. You can copy the data to the new virtual disks from the existing volumes to gain the benefits of the new resiliency.

## The Storage Spaces Direct was created using the autoconfig:0 switch and the pool was created manually. When I try to query the Storage Spaces Direct pool to create a new volume, I get a message saying: "Enable-ClusterS2D again." What should I do?

By default, when you configure Storage Spaces Direct by using the enable-S2D cmdlet, the cmdlet does everything for you. It creates the pool and the tiers. When using autoconfig:0, everything must be done manually. If you created only the pool, the tier is not necessarily created. You will receive an "Enable-ClusterS2D again" error message if you have either not created Tiers at all or not created Tiers in a manner corresponding to the devices attached. We recommend that you do not use the autoconfig switch in a production environment.

## Is it possible to add a spinning disk (HDD) to the Storage Spaces Direct pool after you have created Storage Spaces Direct with SSD devices?

No. By default, if you use the single device type to create the pool, it would not configure cache disks and all disks would be used for capacity. You can add NVME disks to the configuration, and NVME disks would be configured for cache.

## I have configured a 2-rack fault domain: RACK 1 has 2 fault domains, RACK 2 has 1 fault domain. Each server has 4 capacity 100 GB devices. Can I use all 1,200 GB of space from the pool?

No, you can use only 800 GB. In a rack fault domain, you must make sure that you have a 2-way mirror configuration so that each chuck and its duplicate land in a different rack.

## What should the cache size be when I am configuring Storage Spaces Direct?

The cache should be sized to accommodate the working set (the data that's being actively read or written at any given time) of your applications and workloads.

## How can I determine the size of cache that is being used by Storage Spaces Direct?

Use the built-in utility PerfMon to inspect the cache misses. Review the cache miss reads/sec from the Cluster Storage Hybrid Disk counter. Remember that if too many reads are missing the cache, your cache is undersized and you may want to expand it.

## Is there a calculator that shows the exact size of the disks that are being set aside for cache, capacity, and resiliency that would enable me to plan better?

You can use the Storage Spaces Calculator to help with your planning. It is available at https://aka.ms/s2dcalc.

## What is the best configuration that you would recommend when configuring 6 servers and 3 racks?

Use 2 servers on each of the racks to get the virtual disk resiliency of a 3-way mirror. Remember that the rack configuration would work correctly only if you are providing the configuration to the OS in the manner it is placed on the rack.

## Can I enable maintenance mode for a specific disk on a specific server in Storage Spaces Direct cluster?

Yes, you can enable storage maintenance mode on a specific disk and a specific fault domain. The Enable-StorageMaintenanceMode command is automatically invoked when you pause a node. You can enable it for a specific disk by running the following command:

```
Get-PhysicalDisk -SerialNumber <SerialNumber> | Enable-StorageMaintenanceMode
```

## Is Storage Spaces Direct supported on my hardware?

We recommend that you contact your hardware vendor to verify support. Hardware vendors test the solution on their hardware and comment about whether it is supported or not. For example, at the time of this writing, servers

such as R730 / R730xd / R630 that have more than 8 drive slots can support SES and are compatible with Storage Spaces Direct. Dell supports only the HBA330 with Storage Spaces Direct. R620 does not support SES and is not compatible with Storage Spaces Direct.

For more hardware support information, go to the following website: Windows Server Catalog

## How does Storage Spaces Direct make use of SES?

Storage Spaces Direct uses SCSI Enclosure Services (SES) mapping to make sure that slabs of data and the metadata is spread across the fault domains in a resilient fashion. If the hardware does not support SES, there is no mapping of the enclosures, and the data placement is not resilient.

## Which command can you use to check the physical extent for a virtual disk?

This one:

```
get-virtualdisk -friendlyname "xyz" | get-physicalextent
```

# Storage-class Memory (NVDIMM-N) Health Management in Windows

12/16/2020 • 7 minutes to read • Edit Online

> Applies To: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel), Windows 10

This article provides system administrators and IT Pros with information about error handling and health management specific to storage-class memory (NVDIMM-N) devices in Windows, highlighting the differences between storage-class memory and traditional storage devices.

If you aren't familiar with Windows' support for storage-class memory devices, these short videos provide an overview:

- Using Non-volatile Memory (NVDIMM-N) as Block Storage in Windows Server 2016
- Using Non-volatile Memory (NVDIMM-N) as Byte-Addressable Storage in Windows Server 2016
- Accelerating SQL Server 2016 performance with Persistent Memory in Windows Server 2016

Also see Understand and deploy persistent memory in Storage Spaces Direct.

JEDEC-compliant NVDIMM-N storage-class memory devices are supported in Windows with native drivers, starting in Windows Server 2016 and Windows 10 (version 1607). While these devices behave similar to other disks (HDDs and SSDs), there are some differences.

All conditions listed here are expected to be very rare occurrences, but depend on the conditions in which the hardware is used.

The various cases below may refer to Storage Spaces configurations. The particular configuration of interest is one where two NVDIMM-N devices are utilized as a mirrored write-back cache in a storage space. To set up such a configuration, see Configuring Storage Spaces with a NVDIMM-N write-back cache.

In Windows Server 2016, the Storage Spaces GUI shows NVDIMM-N bus type as UNKNOWN. It doesn't have any fuctionality loss or inability in creation of Pool, Storage VD. You can verify the bus type by running the following command:

```
PS C:\>Get-PhysicalDisk | fl
```

The parameter BusType in output of cmdlet will correctly show bus type as "SCM"

## Checking the health of storage-class memory

To query the health of storage-class memory, use the following commands in a Windows PowerShell session.

```
PS C:\> Get-PhysicalDisk | where BusType -eq "SCM" | select SerialNumber, HealthStatus, OperationalStatus,
OperationalDetails
```

Doing so yields this example output:

| SERIALNUMBER | HEALTHSTATUS | OPERATIONALSTATUS | OPERATIONALDETAILS |
|---|---|---|---|
| 802c-01-1602-117cb5fc | Healthy | OK | |
| 802c-01-1602-117cb64f | Warning | Predictive Failure | {Threshold Exceeded,NVDIMM_N Error} |

> **NOTE**
> To find the Physical location of an NVDIMM-N device specified in an event, on the **Details** tab of the event in Event Viewer, go to **EventData** > **Location**. Note that Windows Server 2016 lists the incorrect location NVDIMM-N devices, but this is fixed in Windows Server, version 1709.

For help understanding the various health conditions, see the following sections.

## "Warning" Health Status

This condition is when you check the health of a storage-class memory device and see that it's Health Status is listed as **Warning**, as shown in this example output:

| SERIALNUMBER | HEALTHSTATUS | OPERATIONALSTATUS | OPERATIONALDETAILS |
|---|---|---|---|
| 802c-01-1602-117cb5fc | Healthy | OK | |
| 802c-01-1602-117cb64f | Warning | Predictive Failure | {Threshold Exceeded,NVDIMM_N Error} |

The following table lists some info about this condition.

| HEADING | DESCRIPTION |
|---|---|
| Likely condition | NVDIMM-N Warning Threshold breached |
| Root Cause | NVDIMM-N devices track various thresholds, such as temperature, NVM lifetime, and/or energy source lifetime. When one of those thresholds is exceeded, the operating system is notified. |
| General behavior | Device remains fully operational. This is a warning, not an error. |
| Storage Spaces behavior | Device remains fully operational. This is a warning, not an error. |
| More info | OperationalStatus field of the PhysicalDisk object. EventLog – Microsoft-Windows-ScmDisk0101/Operational |
| What to do | Depending on the warning threshold breached, it may be prudent to consider replacing the entire, or certain parts of the NVDIMM-N. For example, if the NVM lifetime threshold is breached, replacing the NVDIMM-N may make sense. |

## Writes to an NVDIMM-N fail

This condition is when you check the health of a storage-class memory device and see the Health Status listed as **Unhealthy**, and Operational Status mentions an **IO Error**, as shown in this example output:

| SERIALNUMBER | HEALTHSTATUS | OPERATIONALSTATUS | OPERATIONALDETAILS |
|---|---|---|---|
| 802c-01-1602-117cb5fc | Healthy | OK | |
| 802c-01-1602-117cb64f | Unhealthy | {Stale Metadata, IO Error, Transient Error} | {Lost Data Persistence, Lost Data, NV...} |

The following table lists some info about this condition.

| HEADING | DESCRIPTION |
|---|---|
| Likely condition | Loss of Persistence / Backup Power |
| Root Cause | NVDIMM-N devices rely on a back-up power source for their persistence – usually a battery or super-cap. If this back-up power source is unavailable or the device cannot perform a backup for any reason (Controller/Flash Error), data is at risk and Windows will prevent any further writes to the affected devices. Reads are still possible to evacuate data. |
| General behavior | The NTFS volume will be dismounted.<br>The PhysicalDisk Health Status field will show "Unhealthy" for all affected NVDIMM-N devices. |
| Storage Spaces behavior | Storage Space will remain operational as long as only one NVDIMM-N is affected. If multiple devices are affected, writes to the Storage Space will fail.<br>The PhysicalDisk Health Status field will show "Unhealthy" for all affected NVDIMM-N devices. |
| More info | OperationalStatus field of the PhysicalDisk object.<br>EventLog – Microsoft-Windows-ScmDisk0101/Operational |
| What to do | We recommended backing-up the affected NVDIMM-N's data. To gain read access, you can manually bring the disk online (it will surface as a read-only NTFS volume).<br><br>To fully clear this condition, the root cause must be resolved (i.e. service power supply or replace NVDIMM-N, depending on issue) and the volume on the NVDIMM-N must either be taken offline and brought online again, or the system must be restarted.<br><br>To make the NVDIMM-N usable in Storage Spaces again, use the **Reset-PhysicalDisk** cmdlet, which re-integrates the device and starts the repair process. |

## NVDIMM-N is shown with a capacity of '0' Bytes or as a "Generic Physical Disk"

This condition is when a storage-class memory device is shown with a capacity of 0 bytes and cannot be initialized, or is exposed as a "Generic Physical Disk" object with an Operational Status of **Lost Communication**, as shown in this example output:

| SERIALNUMBER | HEALTHSTATUS | OPERATIONALSTATUS | OPERATIONALDETAILS |
|---|---|---|---|
| 802c-01-1602-117cb5fc | Healthy | OK | |
| | Warning | Lost Communication | |

The following table lists some info about this condition.

| HEADING | DESCRIPTION |
|---|---|
| Likely condition | BIOS Did Not Expose NVDIMM-N to OS |
| Root Cause | NVDIMM-N devices are DRAM based. When a corrupt DRAM address is referenced, most CPUs will initiate a machine check and restart the server. Some server platforms then un-map the NVDIMM, preventing the OS from accessing it and potentially causing another machine check. This may also occur if the BIOS detects that the NVDIMM-N has failed and needs to be replaced. |
| General behavior | NVDIMM-N is shown as uninitialized, with a capacity of 0 bytes and cannot be read or written. |
| Storage Spaces behavior | Storage Space remains operational (provided only 1 NVDIMM-N is affected).<br>NVDIMM-N PhysicalDisk object is shown with a Health Status of Warning and as a "General Physical Disk" |
| More info | OperationalStatus field of the PhysicalDisk object.<br>EventLog – Microsoft-Windows-ScmDisk0101/Operational |
| What to do | The NVDIMM-N device must be replaced or sanitized, such that the server platform exposes it to the host OS again. Replacement of the device is recommended, as additional uncorrectable errors could occur. Adding a replacement device to a storage spaces configuration can be achieved with the **Add-Physicaldisk** cmdlet. |

## NVDIMM-N is shown as a RAW or empty disk after a reboot

This condition is when you check the health of a storage-class memory device and see a Health Status of **Unhealthy** and Operational Status of **Unrecognized Metadata**, as shown in this example output:

| SERIALNUMBER | HEALTHSTATUS | OPERATIONALSTATUS | OPERATIONALDETAILS |
|---|---|---|---|
| 802c-01-1602-117cb5fc | Healthy | OK | {Unknown} |
| 802c-01-1602-117cb64f | Unhealthy | {Unrecognized Metadata, Stale Metadata} | {Unknown} |

The following table lists some info about this condition.

| HEADING | DESCRIPTION |
|---|---|
| Likely condition | Backup/Restore Failure |

| HEADING | DESCRIPTION |
| --- | --- |
| Root Cause | A failure in the backup or restore procedure will likely result in all data on the NVDIMM-N to be lost. When the operating system loads, it will appear as a brand new NVDIMM-N without a partition or file system and surface as RAW, meaning it doesn't have a file system. |
| General behavior | NVDIMM-N will be in read-only mode. Explicit user action is needed to begin using it again. |
| Storage Spaces behavior | Storage Spaces remains operational if only one NVDIMM is affected).<br>NVDIMM-N physical disk object will be shown with the Health Status "Unhealthy" and is not used by Storage Spaces. |
| More info | OperationalStatus field of the PhysicalDisk object.<br>EventLog – Microsoft-Windows-ScmDisk0101/Operational |
| What to do | If the user doesn't want to replace the affected device, they can use the **Reset-PhysicalDisk** cmdlet to clear the read-only condition on the affected NVDIMM-N. In Storage Spaces environments this will also attempt to re-integrate the NVDIMM-N into Storage Space and start the repair process. |

## Interleaved Sets

Interleaved sets can often be created in a platform's BIOS to make multiple NVDIMM-N devices appear as a single device to the host operating system.

Windows Server 2016 and Windows 10 Anniversary Edition do not support interleaved sets of NVDIMM-Ns.

At the time of this writing, there is no mechanism for the host operating system to correctly identify individual NVDIMM-Ns in such a set and clearly communicate to the user which particular device may have caused an error or needs to be serviced.

# Work Folders overview

12/16/2020 • 10 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1, Windows 7

This topic discusses Work Folders, a role service for file servers running Windows Server that provides a consistent way for users to access their work files from their PCs and devices.

If you're looking to download or use Work Folders on Windows 10, Windows 7, or an Android or iOS device, see the following:

- Work Folders for Windows 10
- Work Folders for Windows 7 (64 bit download)
- Work Folders for Windows 7 (32 bit download)
- Work Folders for iOS
- Work Folders for Android

## Role description

With Work Folders users can store and access work files on personal computers and devices, often referred to as bring-your-own device (BYOD), in addition to corporate PCs. Users gain a convenient location to store work files, and they can access them from anywhere. Organizations maintain control over corporate data by storing the files on centrally managed file servers, and optionally specifying user device policies such as encryption and lock-screen passwords.

Work Folders can be deployed with existing deployments of Folder Redirection, Offline Files, and home folders. Work Folders stores user files in a folder on the server called a *sync share*. You can specify a folder that already contains user data, which enables you to adopt Work Folders without migrating servers and data or immediately phasing out your existing solution.

## Practical applications

Administrators can use Work Folders to provide users with access to their work files while keeping centralized storage and control over the organization's data. Some specific applications for Work Folders include:

- Provide a single point of access to work files from a user's work and personal computers and devices
- Access work files while offline, and then sync with the central file server when the PC or device next has Internet or intranet connectivity
- Deploy with existing deployments of Folder Redirection, Offline Files, and home folders
- Use existing file server management technologies, such as file classification and folder quotas, to manage user data
- Specify security policies to instruct user's PCs and devices to encrypt Work Folders and use a lock screen password
- Use Failover Clustering with Work Folders to provide a high-availability solution

## Important functionality

Work Folders includes the following functionality.

| FUNCTIONALITY | AVAILABILITY | DESCRIPTION |
| --- | --- | --- |
| Work Folders role service in Server Manager | Windows Server 2019, Windows Server 2016, or Windows Server 2012 R2 | File and Storage Services provides a way to set up sync shares (folders that store user's work files), monitors Work Folders, and manages sync shares and user access |
| Work Folders cmdlets | Windows Server 2019, Windows Server 2016, or Windows Server 2012 R2 | A Windows PowerShell module that contains comprehensive cmdlets for managing Work Folders servers |
| Work Folders integration with Windows | Windows 10<br>Windows 8.1<br>Windows RT 8.1<br>Windows 7 (download required) | Work Folders provides the following functionality in Windows computers:<br>- A Control Panel item that sets up and monitors Work Folders<br>- File Explorer integration that enables easy access to files in Work Folders<br>- A sync engine that transfers files to and from a central file server while maximizing battery life and system performance |
| Work Folders app for devices | Android<br>Apple iPhone and iPad® | An app that allows popular devices to access files in Work Folders |

# New and changed functionality

The following table describes some of the major changes in Work Folders.

| FEATURE/FUNCTIONALITY | NEW OR UPDATED? | DESCRIPTION |
| --- | --- | --- |
| Improved logging | New in Windows Server 2019 | Event logs on the Work Folders server can be used to monitor sync activity and identify users that are failing sync sessions. Use Event ID 4020 in the Microsoft-Windows-SyncShare/Operational event log to identify which users are failing sync sessions. Use Event ID 7000 and Event ID 7001 in the Microsoft-Windows-SyncShare/Reporting event log to monitor users that are successfully completing upload and download sync sessions. |
| Performance counters | New in Windows Server 2019 | The following performance counters were added: Bytes downloaded/sec, Bytes uploaded/sec, Connected Users, Files downloaded/sec, Files uploaded/sec, Users with change detection, Incoming requests/sec and Outstanding requests. |

| FEATURE/FUNCTIONALITY | NEW OR UPDATED? | DESCRIPTION |
| --- | --- | --- |
| Improved server performance | Updated in Windows Server 2019 | Performance improvements were made to handle more users per server. The limit per server varies and is based on the number of files and file churn. To determine the limit per server, users should be added to the server in phases. |
| On-demand file access | Added to Windows 10 version 1803 | Enables you to see and access all of your files. You control which files are stored on your PC and available offline. The rest of your files are always visible and don't take up any space on your PC, but you need connectivity to the Work Folders file server to access them. |
| Azure AD Application Proxy support | Added to Windows 10 version 1703, Android, iOS | Remote users can securely access their files on the Work Folders server using Azure AD Application Proxy. |
| Faster change replication | Updated in Windows 10 and Windows Server 2016 | For Windows Server 2012 R2, when file changes are synced to the Work Folders server, clients are not notified of the change and wait up to 10 minutes to get the update. When using Windows Server 2016, the Work Folders server immediately notifies Windows 10 clients and the file changes are synced immediately. This capability is new in Windows Server 2016 and requires a Windows 10 client. If you're using an older client or the Work Folders server is Windows Server 2012 R2, the client will continue to poll every 10 minutes for changes. |
| Integrated with Windows Information Protection (WIP) | Added to Windows 10 version 1607 | If an administrator deploys WIP, Work Folders can enforce data protection by encrypting the data on the PC. The encryption is using a key associated with the Enterprise ID, which can be remotely wiped by using a supported mobile device management package such as Microsoft Intune. |

## Software requirements

Work Folders has the following software requirements for file servers and your network infrastructure:

- A server running Windows Server 2019, Windows Server 2016, or Windows Server 2012 R2 for hosting sync shares with user files
- A volume formatted with the NTFS file system for storing user files
- To enforce password policies on Windows 7 PCs, you must use Group Policy password policies. You also have to exclude the Windows 7 PCs from Work Folders password policies (if you use them).
- A server certificate for each file server that will host Work Folders. These certificates should be from a

certification authority (CA) that is trusted by your users—ideally a public CA.

- (Optional) An Active Directory Domain Services forest with the schema extensions in Windows Server 2012 R2 to support automatically referring PCs and devices to the correct file server when using multiple file servers.

To enable users to sync across the Internet, there are additional requirements:

- The ability to make a server accessible from the Internet by creating publishing rules in your organization's reverse proxy or network gateway
- (Optional) A publicly registered domain name and the ability to create additional public DNS records for the domain
- (Optional) Active Directory Federation Services (AD FS) infrastructure when using AD FS authentication

Work Folders has the following software requirements for client computers:

- PCs and devices must be running one of the following operating systems:
  - Windows 10
  - Windows 8.1
  - Windows RT 8.1
  - Windows 7
  - Android 4.4 KitKat and later
  - iOS 10.2 and later
- Windows 7 PCs must be running one of the following editions of Windows:
  - Windows 7 Professional
  - Windows 7 Ultimate
  - Windows 7 Enterprise
- Windows 7 PCs must be joined to your organization's domain (they can't be joined to a workgroup).
- Enough free space on a local, NTFS-formatted drive to store all the user's files in Work Folders, plus an additional 6 GB of free space if Work Folders is located on the system drive, as it is by default. Work Folders uses the following location by default: **%USERPROFILE%\Work Folders**

  However, users can change the location during setup (microSD cards and USB drives formatted with the NTFS file system are supported locations, though sync will stop if the drives are removed).

  The maximum size for individual files is 10 GB by default. There is no per-user storage limit, although administrators can use the quotas functionality of File Server Resource Manager to implement quotas.
- Work Folders doesn't support rolling back the virtual machine state of client virtual machines. Instead perform backup and restore operations from inside the client virtual machine by using System Image Backup or another backup app.

## Work Folders compared to other sync technologies

The following table discusses how various Microsoft sync technologies are positioned and when to use each.

| | WORK FOLDERS | OFFLINE FILES | ONEDRIVE FOR BUSINESS | ONEDRIVE |
|---|---|---|---|---|
| **Technology summary** | Syncs files that are stored on a file server with PCs and devices | Syncs files that are stored on a file server with PCs that have access to the corporate network (can be replaced by Work Folders) | Syncs files that are stored in Microsoft 365 or in SharePoint with PCs and devices inside or outside a corporate network, and provides document collaboration functionality | Syncs personal files that are stored in OneDrive with PCs, Mac computers, and devices |
| **Intended to provide user access to work files** | Yes | Yes | Yes | No |
| **Cloud service** | None | None | Microsoft 365 | Microsoft OneDrive |
| **Internal network servers** | File servers running Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 | File servers | SharePoint server (optional) | None |
| **Supported clients** | PCs, iOS, Android | PCs in a corporate network or connected through DirectAccess, VPNs, or other remote access technologies | PCs, iOS, Android, Windows Phone | PCs, Mac computers, Windows Phone, iOS, Android |

**NOTE**

In addition to the sync technologies listed in the previous table, Microsoft offers other replication technologies, including DFS Replication, which is designed for server-to-server replication, and BranchCache, which is designed as a branch office WAN acceleration technology. For more information, see DFS Namespaces and DFS Replication and BranchCache Overview

## Server Manager information

Work Folders is part of the File and Storage Services role. You can install Work Folders by using the Add Roles and Features Wizard or the `Install-WindowsFeature` cmdlet. Both methods accomplish the following:

- Adds the **Work Folders** page to **File and Storage Services** in Server Manager
- Installs the Windows Sync Shares service, which is used by Windows Server to host sync shares
- Installs the SyncShare Windows PowerShell module to manage Work Folders on the server

## Interoperability with Windows Azure virtual machines

You can run this Windows Server role service on a virtual machine in Windows Azure. This scenario has been tested with Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

To learn about how to get started with Windows Azure virtual machines, visit the Windows Azure web site.

# See also

| CONTENT TYPE | REFERENCES |
| --- | --- |
| **Product evaluation** | - Work Folders for Android – Released (blog post)<br>- Work Folders for iOS – iPad App Release (blog post)<br>- Introducing Work Folders on Windows Server 2012 R2 (blog post)<br>- Introduction to Work Folders (Channel 9 Video)<br>- Work Folders Test Lab Deployment (blog post)<br>- Work Folders for Windows 7 (blog post) |
| **Deployment** | - Designing a Work Folders Implementation<br>- Deploying Work Folders<br>- Deploying Work Folders with AD FS and Web Application Proxy (WAP)<br>- Deploying Work Folders with Azure AD Application Proxy<br>- Offline Files (CSC) to Work Folders Migration Guide<br>- Performance Considerations for Work Folders Deployments<br>- Work Folders for Windows 7 (64 bit download)<br>- Work Folders for Windows 7 (32 bit download) |
| **Operations** | - Work Folders iPad app: FAQ (for users)<br>- Work Folders Certificate Management (blog post)<br>- Monitoring Windows Server 2012 R2 Work Folders Deployments (blog post)<br>- SyncShare (Work Folders) Cmdlets in Windows PowerShell<br>- Storage and File Services PowerShell Cmdlets Quick Reference Card For Windows Server 2012 R2 Preview Edition |
| **Troubleshooting** | - Windows Server 2012 R2 – Resolving Port Conflict with IIS Websites and Work Folders (blog post)<br>- Common Errors in Work Folders |
| **Community resources** | - File Services and Storage Forum<br>- The Storage Team at Microsoft - File Cabinet Blog<br>- Ask the Directory Services Team Blog |
| **Related technologies** | - Storage in Windows Server 2016<br>- File and Storage Services<br>- File Server Resource Manager<br>- Folder Redirection, Offline Files, and Roaming User Profiles<br>- BranchCache<br>- DFS Namespaces and DFS Replication |

# Planning a Work Folders deployment

11/2/2020 • 13 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1, Windows 7

This topic explains the design process for a Work Folders implementation, and assumes that you have the following background:

- Have a basic understanding of Work Folders (as described in Work Folders)
- Have a basic understanding of Active Directory Domain Services (AD DS) concepts
- Have a basic understanding of Windows file sharing and related technologies
- Have a basic understanding of SSL certificate usage
- Have a basic understanding of enabling web access to internal resources via a web reverse proxy

  The following sections will help you design your Work Folders implementation. Deploying Work Folders is discussed in the next topic, Deploying Work Folders.

## Software requirements

Work Folders has the following software requirements for file servers and your network infrastructure:

- A server running Windows Server 2012 R2 or Windows Server 2016 for hosting sync shares with user files
- A volume formatted with the NTFS file system for storing user files
- To enforce password policies on Windows 7 PCs, you must use Group Policy password policies. You also have to exclude the Windows 7 PCs from Work Folders password policies (if you use them).
- A server certificate for each file server that will host Work Folders. These certificates should be from a certification authority (CA) that is trusted by your users—ideally a public CA.
- (Optional) An Active Directory Domain Services forest with schema extensions in Windows Server 2012 R2 to support automatically referring PCs and devices to the correct file server when using multiple file servers.

To enable users to sync across the Internet, there are additional requirements:

- The ability to make a server accessible from the Internet by creating publishing rules in your organization's reverse proxy or network gateway
- (Optional) A publicly registered domain name and the ability to create additional public DNS records for the domain
- (Optional) Active Directory Federation Services (AD FS) infrastructure when using AD FS authentication

Work Folders has the following software requirements for client computers:

- Computers must be running one of the following operating systems:
  - Windows 10
  - Windows 8.1

    - Windows RT 8.1
    - Windows 7
    - Android 4.4 KitKat and later
    - iOS 10.2 and later
- Windows 7 PCs must be running one of the following editions of Windows:
    - Windows 7 Professional
    - Windows 7 Ultimate
    - Windows 7 Enterprise
- Windows 7 PCs must be joined to your organization's domain (they can't be joined to a workgroup).
- Enough free space on a local, NTFS-formatted drive to store all the user's files in Work Folders, plus an additional 6 GB of free space if Work Folders is located on the system drive, as it is by default. Work Folders uses the following location by default: **%USERPROFILE%\Work Folders**

  However, users can change the location during setup (microSD cards and USB drives formatted with the NTFS file system are supported locations, though sync will stop if the drives are removed).

  The maximum size for individual files is 10 GB by default. There is no per-user storage limit, although administrators can use the quotas functionality of File Server Resource Manager to implement quotas.
- Work Folders doesn't support rolling back the virtual machine state of client virtual machines. Instead perform backup and restore operations from inside the client virtual machine by using System Image Backup or another backup app.

> **NOTE**
> Make sure to install the Windows 8.1 and Windows Server 2012 R2 General Availability update rollup on all Work Folders servers and any client computers running Windows 8.1 or Windows Server 2012 R2. For more information, see article 2883200 in the Microsoft Knowledge Base.

## Deployment scenarios

Work Folders can be implemented on any number of file servers within a customer environment. This allows Work Folders implementations to scale based on customer needs and can result in highly individualized deployments. However, most deployments will fall into one of the following three basic scenarios.

**Single-Site Deployment**

In a single-site deployment, file servers are hosted within a central site in the customer infrastructure. This deployment type is seen most often in customers with a highly centralized infrastructure or with smaller branch offices that do not maintain local file servers. This deployment model can be easier for IT staff to administer, since all server assets are local, and internet ingress/egress is likely centralized at this location as well. However, this deployment model also relies on good WAN connectivity between the central site and any branch offices, and users in branch offices are vulnerable to an interruption of service due to network conditions.

**Multiple-Site Deployment**

In a multiple-site deployment, file servers are hosted in multiple locations within the customer's infrastructure. This could mean multiple datacenters or it could mean that branch offices maintain individual file servers. This deployment type is seen most often in larger customer environments or in customers that have several larger branch offices that maintain local server assets. This deployment model is more complex for IT personnel to

administer, and relies on careful coordination of data storage and maintenance of Active Directory Domain Services (AD DS) to ensure that users are using the correct sync server for Work Folders.

**Hosted Deployment**

In a hosted deployment, sync servers are deployed in an IAAS (Infrastructure-as-a-Service) solution such as Windows Azure VM. This deployment method has the advantage of making the availability of file servers less dependent on WAN connectivity within a customer's business. If a device is able to connect to the Internet, it can get to its sync server. However, the servers deployed in the hosted environment still need to be able to reach the organization's Active Directory domain to authenticate users, and the customer trades infrastructure requirements on-premises for additional complexity in maintaining that connection.

# Deployment technologies

Work Folders deployments consist of a number of technologies that work together to provide service to devices on both the internal and external networks. Before designing a Work Folders deployment, customers should be familiar with the requirements of each of the following technologies.

**Active Directory Domain Services**

AD DS provides two important services in a Work Folders deployment. First, as the back-end for Windows authentication, AD DS provides the security and authentication services that are used to grant access to user data. If a domain controller cannot be reached, a file server will be unable to authenticate an incoming request and the device will not be able to access any data stored in that file server's sync share.

Second, AD DS (with the Windows Server 2012 R2 schema update) maintains the msDS-SyncServerURL attribute on each user, which is used to automatically direct users to the appropriate sync server.

**File Servers**

File servers running Windows Server 2012 R2 or Windows Server 2016 host the Work Folders role service, and host the sync shares that store users' Work Folders data. File servers can also host data stored by other technologies operating on the internal network (such as file shares), and can be clustered to provide fault tolerance for user data.

**Group Policy**

If you have Windows 7 PCs in your environment, we recommend the following:

- Use Group Policy to control password policies for all domain-joined PCs that use Work Folders.
- Use the Work Folders **Automatically lock screen, and require a password** policy on PCs that aren't joined to your domain.

  You can also use Group Policy to specify a Work Folders server to domain-joined PCs. This simplifies Work Folders setup a little bit– users would otherwise need to enter their work email address to lookup the settings (assuming that Work Folders is set up properly), or enter the Work Folders URL that you explicitly provided them via email or another means of communication.

  You can also use Group Policy to forcibly set up Work Folders on a per-user or per-computer basis, though doing so causes Work Folders to sync on every PC a user signs in to (when using the per-user policy setting), and prevents users from specifying an alternate location for Work Folders on their PC (such as on a microSD card to conserve space on the primary drive). We suggest carefully evaluating your user's needs before forcing automatic setup.

**Windows Intune**

Windows Intune also provides a layer of security and manageability for non-domain-joined devices that would not otherwise be present. You can use Windows Intune to configure and manage users' personal devices such as tablets that connect to Work Folders from across the Internet. Windows Intune can provide devices with the sync server URL to use – otherwise users must enter their work email address to lookup the settings (if you publish a

public Work Folders URL in the form of https://workfolders.*contoso.com*), or enter the sync server URL directly.

Without a Windows Intune deployment, users must configure external devices manually, which can result in increased demands on a customer's help desk staff.

You can also use Windows Intune to selectively wipe the data from Work Folders on a user's device without affecting the rest of their data – handy for if a user leaves your organization or has their device stolen.

**Web Application Proxy/Azure AD Application Proxy**

Work Folders is built around the concept of allowing Internet-connected devices to retrieve business data securely from the internal network, which allows users to "take their data with them" on their tablets and devices that would not normally be able to access work files. To do this, a reverse proxy must be used to publish sync server URLs and make them available to Internet clients.

Work Folders supports using Web Application Proxy, Azure AD Application Proxy or 3rd party reverse proxy solutions:

- Web Application Proxy is an on-premises reverse proxy solution. To learn more, see Web Application Proxy in Windows Server 2016.
- Azure AD Application Proxy is a cloud reverse proxy solution. To learn more, see How to provide secure remote access to on-premises applications

## Additional design considerations

In addition to understanding each of the components noted above, customers need to spend time in their design thinking about the number of sync servers and shares to operate, and whether or not to leverage failover clustering to provide fault tolerance on those sync servers

**Number of Sync Servers**

It is possible for a customer to operate multiple sync servers in an environment. This can be a desirable configuration for several reasons:

- Geographic distribution of users – for example, branch office files servers or regional datacenters
- Data storage requirements – certain business departments might have specific data storage or handling requirements that are easier with a dedicated server
- Load balancing – in large environments, storing user data on multiple servers can increase server performance and uptime.

  For information on Work Folders server scaling and performance, see Performance Considerations for Work Folders Deployments.

> **NOTE**
> When using multiple sync servers, we recommend setting up automatic server discovery for users. This process relies upon the configuration of an attribute on each user account in AD DS. The attribute is named **msDS-SyncServerURL** and becomes available on user accounts after a Windows Server 2012 R2 domain controller is added to the domain or the Active Directory schema updates are applied. This attribute should be set for each user to ensure that users connect to the appropriate sync server. By using automatic server discovery, organizations can publish Work Folders behind a "friendly" URL such as *https://workfolders.contoso.com*, regardless of the number of sync servers in operation.

**Number of Sync Shares**

Individual sync servers can maintain multiple sync shares. This can be useful for the following reasons:

- Auditing and security requirements – If data used by a certain department must be more heavily audited or

retained for a longer period of time, separate sync shares can help administrators keep user folders with differing audit levels separated.

- Differing quotas or file screens – If you want to set different storage quotas or limits on which file types are allowed in Work Folders (file screens) for different groups of users, separate sync shares can help.
- Departmental control – If administrative duties are distributed by department, utilizing separate shares for different departments can aid administrators in enforcing quotas or other policies.
- Differing device policies –If an organization needs to maintain multiple device policies (such as encrypting Work Folders) for different groups of users, using multiple shares enables this.
- Storage capacity –If a file server has multiple volumes, additional shares can be used to take advantage of these additional volumes. An individual share has access to only the volume that it is hosted on, and is unable to take advantage of additional volumes on a file server.

#### Access to Sync Shares

While the sync server that a user accesses is determined by the URL entered at their client (or the URL published for that user in AD DS when using server automatic discovery), access to individual sync shares is determined by the permissions present on the share.

As a result, if a customer is hosting multiple sync shares on the same server, care must be taken to ensure that individual users have permissions to access only one of those shares. Otherwise, when users connect to the server, their client may connect to the wrong share. This can be accomplished by creating a separate security group for each sync share.

Further, access to an individual user's folder inside a sync share is determined by ownership rights on the folder. When creating a sync share, Work Folders by default grants users exclusive access to their files (disabling inheritance and making them the owner of their individual folders).

## Design checklist

The following set of design questions is intended to aid customers in designing a Work Folders implementation that best serves their environment. Customers should work through this checklist prior to attempting to deploy servers.

- Intended Users
  - Which users will use Work Folders?
  - How are users organized? (Geographically, by office, by department, etc)
  - Do any users have special requirements for data storage, security, or retention?
  - Do any users have specific device policy requirements, such as encryption?
  - Which client computers and devices do you need to support? (Windows 8.1, Windows RT 8.1, Windows 7)

    If you're supporting Windows 7 PCs and want to use password policies, exclude the domain storing their computer accounts from the Work Folders password policy, and instead use Group Policy password policies for domain-joined PCs in that domain.
  - Do you need to interoperate with or migrate from other user data management solutions such as Folder Redirection?
  - Do users from multiple domains need to sync across the Internet with a single server?
  - Do you need to support users who aren't members of the Local Administrators group on their domain-joined PCs? (If so, you'll need to exclude the relevant domains from Work Folders device

policies such as encryption and password policies)

- Infrastructure and Capacity Planning
  - In what sites should sync servers be located on the network?
  - Will any sync servers be hosted by an Infrastructure as a Service (IaaS) provider such as in an Azure VM?
  - Will dedicated servers be needed for any specific user groups, and if so, how many users for each dedicated server?
  - Where are the Internet ingress/egress points on the network?
  - Will sync servers be clustered for fault-tolerance?
  - Will sync servers need to maintain multiple data volumes to host user data?
- Data Security
  - Will multiple sync shares need to be created on any sync servers?
  - What groups will be used to provide access to sync shares?
  - If you're using multiple sync servers, what security group will you create for the delegated ability to modify the msDS-SyncServerURL property of user objects?
  - Are there any special security or auditing requirements for individual sync shares?
  - Is multi-factor authentication (MFA) required?
  - Do you need the ability to remotely wipe Work Folders data from PCs and devices?
- Device Access
  - What URL will be used to provide access for Internet-based devices (*the default URL that is required for email-based automatic server discovery is workfolders.domainname*)?
  - How will the URL be published to the Internet?
  - Will automatic server discovery be used?
  - Will Group Policy be used to configure domain-joined PCs?
  - Will Windows Intune be used to configure external devices?
  - Will Device Registration be required for devices to connect?

## Next steps

After designing your Work Folders implementation, it's time to deploy Work Folders. For more information, see Deploying Work Folders.

## Additional References

For additional related information, see the following resources.

| CONTENT TYPE | REFERENCES |
| --- | --- |
| **Product evaluation** | - Work Folders<br>- Work Folders for Windows 7 (blog post) |

| CONTENT TYPE | REFERENCES |
| --- | --- |
| **Deployment** | - Designing a Work Folders Implementation<br>- Deploying Work Folders<br>- Deploying Work Folders with AD FS and Web Application Proxy (WAP)<br>- Deploying Work Folders with Azure AD Application Proxy<br>- Performance Considerations for Work Folders Deployments<br>- Work Folders for Windows 7 (64 bit download)<br>- Work Folders for Windows 7 (32 bit download)<br>- Work Folders Test Lab Deployment (blog post) |

# Deploying Work Folders

11/2/2020 • 16 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows Server 2012 R2, Windows 10, Windows 8.1, Windows 7

This topic discusses the steps needed to deploy Work Folders. It assumes that you've already read Planning a Work Folders deployment.

To deploy Work Folders, a process that can involve multiple servers and technologies, use the following steps.

**TIP**

The simplest Work Folders deployment is a single file server (often called a sync server) without support for syncing over the Internet, which can be a useful deployment for a test lab or as a sync solution for domain-joined client computers. To create a simple deployment, these are minimum steps to follow:

- Step 1: Obtain SSL certificates
- Step 2: Create DNS records
- Step 3: Install Work Folders on file servers
- Step 4: Binding the SSL certificate on the sync servers
- Step 5: Create security groups for Work Folders
- Step 7: Create sync shares for user data

## Step 1: Obtain SSL certificates

Work Folders uses HTTPS to securely synchronize files between the Work Folders clients and the Work Folders server. The requirements for SSL certificates used by Work Folders are as follows:

- The certificate must be issued by a trusted certification authority. For most Work Folders implementations, a publicly trusted CA is recommended, since certificates will be used by non-domain-joined, Internet-based devices.
- The certificate must be valid.
- The private key of the certificate must be exportable (as you will need to install the certificate on multiple servers).
- The subject name of the certificate must contain the public Work Folders URL used for discovering the Work Folders service from across the Internet – this must be in the format of `workfolders.` *<domain_name>*.
- Subject alternative names (SANs) must be present on the certificate listing the server name for each sync server in use.

  The Work Folders Certificate Management blog provides additional information on using certificates with Work Folders.

## Step 2: Create DNS records

To allow users to sync across the Internet, you must create a Host (A) record in public DNS to allow Internet clients to resolve your Work Folders URL. This DNS record should resolve to the external interface of the reverse proxy

server.

On your internal network, create a CNAME record in DNS named workfolders which resolves to the FDQN of a Work Folders server. When Work Folders clients use auto discovery, the URL used to discover the Work Folders server is https://workfolders.domain.com. If you plan to use auto discovery, the workfolders CNAME record must exist in DNS.

## Step 3: Install Work Folders on file servers

You can install Work Folders on a domain-joined server by using Server Manager or by using Windows PowerShell, locally or remotely across a network. This is useful if you are configuring multiple sync servers across your network.

To deploy the role in Server Manager, do the following:

1. Start the **Add Roles and Features Wizard**.
2. On the **Select installation type** page, choose **Role-based or feature-based deployment**.
3. On the **Select destination server** page, select the server on which you want to install Work Folders.
4. On the **Select server roles** page, expand **File and Storage Services**, expand **File and iSCSI Services**, and then select **Work Folders**.
5. When asked if you want to install **IIS Hostable Web Core**, click **Ok** to install the minimal version of Internet Information Services (IIS) required by Work Folders.
6. Click **Next** until you have completed the wizard.

To deploy the role by using Windows PowerShell, use the following cmdlet:

```
Add-WindowsFeature FS-SyncShareService
```

## Step 4: Binding the SSL certificate on the sync servers

Work Folders installs the IIS Hostable Web Core, which is an IIS component designed to enable web services without requiring a full installation of IIS. After installing the IIS Hostable Web Core, you should bind the SSL certificate for the server to the Default Web Site on the file server. However, the IIS Hostable Web Core does not install the IIS Management console.

There are two options for binding the certificate to the Default Web Interface. To use either option you must have installed the private key for the certificate into the computer's personal store.

- Utilize the IIS management console on a server that has it installed. From within the console, connect to the file server you want to manage, and then select the Default Web Site for that server. The Default Web Site will appear disabled, but you can still edit the bindings for the site and select the certificate to bind it to that web site.
- Use the netsh command to bind the certificate to the Default Web Site https interface. The command is as follows:

  ```
  netsh http add sslcert ipport=<IP address>:443 certhash=<Cert thumbprint> appid={CE66697B-3AA0-49D1-
  BDBD-A25C8359FD5D} certstorename=MY
  ```

## Step 5: Create security groups for Work Folders

Before creating sync shares, a member of the Domain Admins or Enterprise Admins groups needs to create some security groups in Active Directory Domain Services (AD DS) for Work Folders (they might also want to delegate some control as described in Step 6). Here are the groups you need:

- One group per sync share to specify which users are allowed to sync with the sync share
- One group for all Work Folders administrators so that they can edit an attribute on each user object that links the user to the correct sync server (if you're going to use multiple sync servers)

  Groups should follow a standard naming convention and should be used only for Work Folders to avoid potential conflicts with other security requirements.

  To create the appropriate security groups, use the following procedure multiple times – once for each sync share, and once to optionally create a group for file server administrators.

**To create security groups for Work Folders**

1. Open Server Manager on a Windows Server 2012 R2 or Windows Server 2016 computer with Active Directory Administration Center installed.
2. On the **Tools** menu, click **Active Directory Administration Center**. Active Directory Administration Center appears.
3. Right-click the container where you want to create the new group (for example, the Users container of the appropriate domain or OU), click **New**, and then click **Group**.
4. In the **Create Group** window, in the **Group** section, specify the following settings:
   - In **Group name**, type the name of the security group, for example: **HR Sync Share Users**, or **Work Folders Administrators**.
   - In **Group scope**, click **Security**, and then click **Global**.
5. In the **Members** section, click **Add**. The Select Users, Contacts, Computers, Service Accounts or Groups dialog box appears.
6. Type the names of the users or groups to which you grant access to a particular sync share (if you're creating a group to control access to a sync share), or type the names of the Work Folders administrators (if you're going to configure user accounts to automatically discover the appropriate sync server), click **OK**, and then click **OK** again.

To create a security group by using Windows PowerShell, use the following cmdlets:

```
$GroupName = "Work Folders Administrators"
$DC = "DC1.contoso.com"
$ADGroupPath = "CN=Users,DC=contoso,DC=com"
$Members = "CN=Maya Bender,CN=Users,DC=contoso,DC=com","CN=Irwin Hume,CN=Users,DC=contoso,DC=com"

New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:$GroupName -Path:$ADGroupPath -
SamAccountName:$GroupName -Server:$DC
Set-ADGroup -Add:@{'Member'=$Members} -Identity:$GroupName -Server:$DC
```

## Step 6: Optionally delegate user attribute control to Work Folders administrators

If you are deploying multiple sync servers and want to automatically direct users to the correct sync server, you'll need to update an attribute on each user account in AD DS. However, this normally requires getting a member of the Domain Admins or Enterprise Admins groups to update the attributes, which can quickly become tiresome if you need to frequently add users or move them between sync servers.

For this reason, a member of the Domain Admins or Enterprise Admins groups might want to delegate the ability to modify the msDS-SyncServerURL property of user objects to the Work Folders Administrators group you created in Step 5, as described in the following procedure.

**Delegate the ability to edit the msDS-SyncServerURL property on user objects in AD DS**

1. Open Server Manager on a Windows Server 2012 R2 or Windows Server 2016 computer with Active Directory Users and Computers installed.
2. On the **Tools** menu, click **Active Directory Users and Computers**. Active Directory Users and Computers appears.
3. Right-click the OU under which all user objects exist for Work Folders (if users are stored in multiple OUs or domains, right-click the container that is common to all of the users), and then click **Delegate Control...**. The Delegation of Control Wizard appears.
4. On the **Users or Groups** page, click **Add...** and then specify the group you created for Work Folders administrators (for example, **Work Folders Administrators**).
5. On the **Tasks to Delegate** page, click **Create a custom task to delegate**.
6. On the **Active Directory Object Type** page, click **Only the following objects in the folder**, and then select the **User objects** checkbox.
7. On the **Permissions** page, clear the **General** checkbox, select the **Property-specific** checkbox, and then select the **Read msDS-SyncServerUrl**, and **Write msDS-SyncServerUrl** checkboxes.

To delegate the ability to edit the msDS-SyncServerURL property on user objects by using Windows PowerShell, use the following example script that makes use of the DsAcls command.

```
$GroupName = "Contoso\Work Folders Administrators"
$ADGroupPath = "CN=Users,dc=contoso,dc=com"

DsAcls $ADGroupPath /I:S /G ""$GroupName":RPWP;msDS-SyncServerUrl;user"
```

> **NOTE**
> The delegation operation might take a while to run in domains with a large number of users.

## Step 7: Create sync shares for user data

At this point, you're ready to designate a folder on the sync server to store your user's files. This folder is called a sync share, and you can use the following procedure to create one.

1. If you don't already have an NTFS volume with free space for the sync share and the user files it will contain, create a new volume and format it with the NTFS file system.
2. In Server Manager, click **File and Storage Services**, and then click **Work Folders**.
3. A list of any existing sync shares is visible at the top of the details pane. To create a new sync share, from the **Tasks** menu choose **New Sync Share...**. The New Sync Share Wizard appears.
4. On the **Select the server and path** page, specify where to store the sync share. If you already have a file share created for this user data, you can choose that share. Alternatively you can create a new folder.

> **NOTE**
>
> By default, sync shares aren't directly accessible via a file share (unless you pick an existing file share). If you want to make a sync share accessible via a file share, use the **Shares** tile of Server Manager or the New-SmbShare cmdlet to create a file share, preferably with access-based enumeration enabled.

5. On the **Specify the structure for user folders** page, choose a naming convention for user folders within the sync share. There are two options available:

   - **User alias** creates user folders that don't include a domain name. If you are using a file share that is already in use with Folder Redirection or another user data solution, select this naming convention. You can optionally select the **Sync only the following subfolder** checkbox to sync only a specific subfolder, such as the Documents folder.
   - **User alias@domain** creates user folders that include a domain name. If you aren't using a file share already in use with Folder Redirection or another user data solution, select this naming convention to eliminate folder naming conflicts when multiple users of the share have identical aliases (which can happen if the users belong to different domains).

6. On the **Enter the sync share name** page, specify a name and a description for the sync share. This is not advertised on the network but is visible in Server Manager and Windows Powershell to help distinguish sync shares from each other.

7. On the **Grant sync access to groups** page, specify the group that you created that lists the users allowed to use this sync share.

   > **IMPORTANT**
   >
   > To improve performance and security, grant access to groups instead of individual users and be as specific as possible, avoiding generic groups such as Authenticated Users and Domain Users. Granting access to groups with large numbers of users increases the time it takes Work Folders to query AD DS. If you have a large number of users, create multiple sync shares to help disperse the load.

8. On the **Specify device policies** page, specify whether to request any security restrictions on client PCs and devices. There are two device policies that can be individually selected:

   - **Encrypt Work Folders** Requests that Work Folders be encrypted on client PCs and devices
   - **Automatically lock screen, and require a password** Requests that client PCs and devices automatically lock their screens after 15 minutes, require a six-character or longer password to unlock the screen, and activate a device lockout mode after 10 failed retries

     > **IMPORTANT**
     >
     > To enforce password policies for Windows 7 PCs and for non-administrators on domain-joined PCs, use Group Policy password policies for the computer domains and exclude these domains from the Work Folders password policies. You can exclude domains by using the Set-Syncshare -PasswordAutoExcludeDomain cmdlet after creating the sync share. For information about setting Group Policy password policies, see Password Policy.

9. Review your selections and complete the wizard to create the sync share.

You can create sync shares using Windows PowerShell by using the New-SyncShare cmdlet. Below is an example of this method:

```
New-SyncShare "HR Sync Share" K:\Share-1 –User "HR Sync Share Users"
```

The example above creates a new sync share named *Share01* with the path *K:\Share-1*, and access granted to the group named *HR Sync Share Users*

> **TIP**
> After you create sync shares you can use File Server Resource Manager functionality to manage the data in the shares. For example, you can use the **Quota** tile inside the Work Folders page in Server Manager to set quotas on the user folders. You can also use File Screening Management to control the types of files that Work Folders will sync, or you can use the scenarios described in Dynamic Access Control for more sophisticated file classification tasks.

## Step 8: Optionally specify a tech support email address

After installing Work Folders on a file server, you probably want to specify an administrative contact email address for the server. To add an email address, use the following procedure:

**Specifying an administrative contact email**

1. In Server Manager, click **File and Storage Services**, and then click **Servers**.
2. Right-click the sync server, and then click **Work Folders Settings**. The Work Folders Settings window appears.
3. In the navigation pane, click **Support Email** and then type the email address or addresses that users should use when emailing for help with Work Folders. Click **OK** when you're finished.

   Work Folders users can click a link in the Work Folders Control Panel item that sends an email containing diagnostic information about the client PC to the address(es) you specify here.

## Step 9: Optionally set up server automatic discovery

If you are hosting multiple sync servers in your environment, you should configure server automatic discovery by populating the **msDS-SyncServerURL** property on user accounts in AD DS.

> **NOTE**
> The msDS-SyncServerURL property in Active Directory should not be defined for remote users that are accessing Work Folders through a reverse proxy solution such as Web Application Proxy or Azure AD Application Proxy. If the msDS-SyncServerURL property is defined, the Work Folders client will try to access an internal URL that's not accessible through the reverse proxy solution. When using Web Application Proxy or Azure AD Application Proxy, you need to create unique proxy applications for each Work Folders server. For more details, see Deploying Work Folders with AD FS and Web Application Proxy: Overview or Deploying Work Folders with Azure AD Application Proxy.

Before you can do so, you must install a Windows Server 2012 R2 domain controller or update the forest and domain schemas by using the `Adprep /forestprep` and `Adprep /domainprep` commands. For information on how to safely run these commands, see Running Adprep.

You probably also want to create a security group for file server administrators and give them delegated permissions to modify this particular user attribute, as described in Step 5 and Step 6. Without these steps you would need to get a member of the Domain Admins or Enterprise Admins group to configure automatic discovery for each user.

**To specify the sync server for users**

1. Open Server Manager on a computer with Active Directory Administration Tools installed.

2. On the **Tools** menu, click **Active Directory Administration Center**. Active Directory Administration Center appears.
3. Navigate to the **Users** container in the appropriate domain, right-click the user you want to assign to a sync share, and then click **Properties**.
4. In the Navigation pane, click **Extensions**.
5. Click the **Attribute Editor** tab, select **msDS-SyncServerUrl** and then click **Edit**. The Multi-valued String Editor dialog box appears.
6. In the **Value to add** box, type the URL of the sync server with which you want this user to sync, click **Add**, click **OK**, and then click **OK** again.

> **NOTE**
> The sync server URL is simply `https://` or `http://` (depending on whether you want to require a secure connection) followed by the fully qualified domain name of the sync server. For example, **https://sync1.contoso.com**.

To populate the attribute for multiple users, use Active Directory PowerShell. Below is an example that populates the attribute for all members of the *HR Sync Share Users* group, discussed in Step 5.

```
$SyncServerURL = "https://sync1.contoso.com"
$GroupName = "HR Sync Share Users"

Get-ADGroupMember -Identity $GroupName |
Set-ADUser –Add @{"msDS-SyncServerURL"=$SyncServerURL}
```

## Step 10: Optionally configure Web Application Proxy, Azure AD Application Proxy, or another reverse proxy

To enable remote users to access their files, you need to publish the Work Folders server through a reverse proxy, making Work Folders available externally on the Internet. You can use Web Application Proxy, Azure Active Directory Application Proxy, or another reverse proxy solution.

To configure Work Folders access using AD FS and Web Application Proxy, see Deploying Work Folders with AD FS and Web Application Proxy (WAP). For background information about Web Application Proxy, see Web Application Proxy in Windows Server 2016. For details on publishing applications such as Work Folders on the Internet using Web Application Proxy, see Publishing Applications using AD FS Preauthentication.

To configure Work Folders access using Azure Active Directory Application Proxy, see Enable remote access to Work Folders using Azure Active Directory Application Proxy

## Step 11: Optionally use Group Policy to configure domain-joined PCs

If you have a large number of domain-joined PCs to which you want to deploy Work Folders, you can use Group Policy to do the following client PC configuration tasks:

- Specify which sync server users should sync with
- Force Work Folders to be set up automatically, using default settings (review the Group Policy discussion in Designing a Work Folders Implementation before doing this)

  To control these settings, create a new Group Policy object (GPO) for Work Folders and then configure the

following Group Policy settings as appropriate:

- "Specify Work Folders settings" policy setting in User Configuration\Policies\Administrative Templates\Windows Components\WorkFolders
- "Force automatic setup for all users" policy setting in Computer Configuration\Policies\Administrative Templates\Windows Components\WorkFolders

> **NOTE**
> These policy settings are available only when editing Group Policy from a computer running Group Policy Management on Windows 8.1, Windows Server 2012 R2 or later. Versions of Group Policy Management from earlier operating systems do not have this setting available. These policy settings do apply to Windows 7 PCs on which the Work Folders for Windows 7 app has been installed.

## See also

For additional related information, see the following resources.

| CONTENT TYPE | REFERENCES |
| --- | --- |
| **Understanding** | - Work Folders |
| **Planning** | - Designing a Work Folders Implementation |
| **Deployment** | - Deploying Work Folders with AD FS and Web Application Proxy (WAP)<br>- Work Folders Test Lab Deployment (blog post)<br>- A new user attribute for Work Folders server Url (blog post) |
| **Technical Reference** | - Interactive logon: Machine account lockout threshold<br>- Sync Share Cmdlets |

# Deploy Work Folders with AD FS and Web Application Proxy: Overview

12/16/2020 • 3 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

The topics in this section provide instructions for deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. The instructions are designed to help you create a complete functioning Work Folders setup with client machines that are ready to start using Work Folders either on-premises or over the Internet.

Work Folders is a component introduced in Windows Server 2012 R2 that allows information workers to sync work files between their devices. For more information about Work Folders, see Work Folders Overview.

To enable users to sync their Work Folders across the Internet, you need to publish Work Folders through a reverse proxy, making Work Folders available externally on the Internet. Web Application Proxy, which is included in AD FS, is one option that you can use to provide reverse proxy functionality. Web Application Proxy pre-authenticates access to the Work Folders web application by using AD FS, so that users on any device can access Work Folders from outside the corporate network.

> **NOTE**
> The instructions covered in this section are for a Windows Server 2016 environment. If you're using Windows Server 2012 R2, follow the Windows Server 2012 R2 instructions.

These topics provide the following:

- Step-by-step instructions for setting up and deploying Work Folders with AD FS and Web Application Proxy via the Windows Server user interface. The instructions describe how to set up a simple test environment with self-signed certificates. You can then use the test example as a guide to help you create a production environment that uses publicly trusted certificates.

## Prerequisites

To follow the procedures and examples in these topics, you need to have the following components ready:

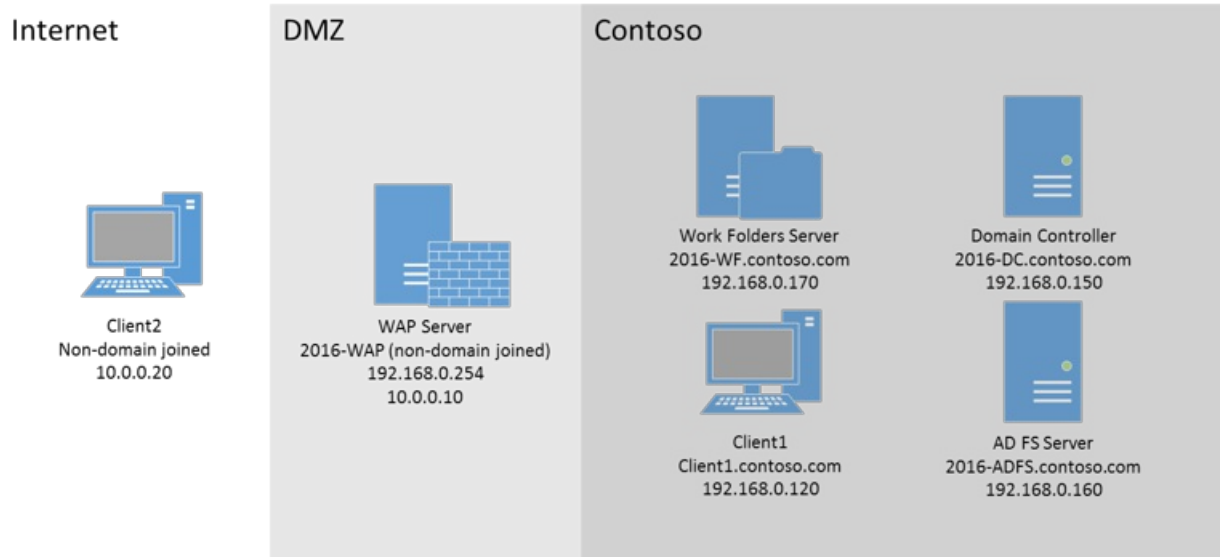
- An Active Directory® Domain Services forest with schema extensions in Windows Server 2012 R2 to support automatic referral of PCs and devices to the correct file server when you are using multiple file servers. It is preferable that DNS be enabled in the forest, but this is not required.
- A domain controller: A server that has the AD DS role enabled, and is configured with a domain (for the test example, contoso.com).

  A domain controller running at least Windows Server 2012 R2 is needed in order to support device registration for Workplace Join. If you don't want to use Workplace Join, you can run Windows Server 2012 on the domain controller.
- Two servers that are joined to the domain (e.g., contoso.com) and that are running Windows Server 2016. One server will be for used for AD FS, and the other will be used for Work Folders.
- One server that is not domain joined and that is running Windows Server 2016. This server will run Web

Application Proxy, and it must have one network card for the network domain (e.g., contoso.com) and another network card for the external network.

- One domain-joined client computer that is running Windows 7 or later.
- One non-domain-joined client computer that is running Windows 7 or later.

For the test environment that we're covering in this guide, you should have the topology that is shown in the following diagram. The computers can be physical machines or virtual machines (VMs).




## Deployment overview

In this group of topics, you'll walk through a step-by-step example of setting up AD FS, Web Application Proxy, and Work Folders in a test environment. The components will be set up in this order:

1. AD FS
2. Work Folders
3. Web Application Proxy
4. The domain-joined workstation and non-domain-joined workstation

You will also use a Windows PowerShell Script to create self-signed certificates.

## Deployment steps

To perform the deployment by using the Windows Server user interface, follow the steps in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set Up AD FS
- Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work
- Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders
- Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy
- Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

## See Also

Work Folders Overview Designing a Work Folders Implementation Deploying Work Folders

# Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set-up AD FS

12/16/2020 • 6 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

This topic describes the first step in deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. You can find the other steps in this process in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Overview
- Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work
- Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders
- Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy
- Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

> **NOTE**
> The instructions covered in this section are for a Windows Server 2019 or Windows Server 2016 environment. If you're using Windows Server 2012 R2, follow the Windows Server 2012 R2 instructions.

To set up AD FS for use with Work Folders, use the following procedures.

## Pre-installment work

If you intend to convert the test environment that you're setting up with these instructions to production, there are two things that you might want to do before you start:

- Set up an Active Directory domain administrator account to use to run the AD FS service.
- Obtain a Secure Sockets Layer (SSL) subject alternative name (SAN) certificate for server authentication. For the test example, you will use a self-signed certificate but for production you should use a publicly trusted certificate.

Obtaining these items can take some time, depending on your company's policies, so it can be beneficial to start the request process for the items before you begin to create the test environment.

There are many commercial certificate authorities (CAs) from which you can purchase the certificate. You can find a list of the CAs that are trusted by Microsoft in KB article 931125. Another alternative is to get a certificate from your company's enterprise CA.

For the test environment, you will use a self-signed certificate that is created by one of the provided scripts.

> **NOTE**
> AD FS does not support Cryptography Next Generation (CNG) certificates, which means that you cannot create the self-signed certificate by using the Windows PowerShell cmdlet New-SelfSignedCertificate. You can, however, use the makecert.ps1 script included in the Deploying Work Folders with AD FS and Web Application Proxy blog post. This script creates a self-signed certificated that works with AD FS and prompts for the SAN names that will be needed to create the certificate.

Next, do the additional pre-installment work described in the following sections.

**Create an AD FS self-signed certificate**

To create an AD FS self-signed certificate, follow these steps:

1. Download the scripts provided in the Deploying Work Folders with AD FS and Web Application Proxy blog post and then copy the file makecert.ps1 to the AD FS machine.
2. Open a Windows PowerShell window with admin privileges.
3. Set the execution policy to unrestricted:

   ```
   Set-ExecutionPolicy –ExecutionPolicy Unrestricted
   ```

4. Change to the directory where you copied the script.
5. Execute the makecert script:

   ```
   .\makecert.ps1
   ```

6. When you are prompted to change the subject certificate, enter the new value for the subject. In this example, the value is **blueadfs.contoso.com**.
7. When you are prompted to enter SAN names, press Y and then enter the SAN names, one at a time.

   For this example, type **blueadfs.contoso.com** and press Enter, then type **2016-adfs.contoso.com** and press Enter, then type **enterpriseregistration.contoso.com** and press Enter.

   When all of the SAN names have been entered, press Enter on an empty line.
8. When you are prompted to install the certificates to the Trusted Root Certification Authority store, press Y.

The AD FS certificate must be a SAN certificate with the following values:

- AD FS service name.domain
- enterpriseregistration.domain
- AD FS server name.domain

In the test example, the values are:

- **blueadfs.contoso.com**
- **enterpriseregistration.contoso.com**
- **2016-adfs.contoso.com**

The enterpriseregistration SAN is needed for Workplace Join.

**Set the server IP address**

Change your server IP address to a static IP address. For the test example, use IP class A, which is 192.168.0.160 / subnet mask: 255.255.0.0 / Default Gateway: 192.168.0.1 / Preferred DNS: 192.168.0.150 (the IP address of your domain controller).

## Install the AD FS role service

To install AD FS, follow these steps:

1. Log on to the physical or virtual machine on which you plan to install AD FS, open **Server Manager**, and start the Add Roles and Features Wizard.
2. On the **Server Roles** page, select the **Active Directory Federation Services** role, and then click **Next**.
3. On the **Active Directory Federation Services (AD FS)** page, you will see a message that states that the Web Application Proxy role cannot be installed on the same computer as AD FS. Click **Next**.
4. Click **Install** on the confirmation page.

To accomplish the equivalent installation of AD FS via Windows PowerShell, use these commands:

```
Add-WindowsFeature RSAT-AD-Tools
Add-WindowsFeature ADFS-Federation –IncludeManagementTools
```

## Configure AD FS

Next, configure AD FS by using either Server Manager or Windows PowerShell.

### Configure AD FS by using Server Manager

To configure AD FS by using Server Manager, follow these steps:

1. Open Server Manager.
2. Click the **Notifications** flag at the top of the Server Manager window, and then click **Configure the federation service on this server**.
3. The Active Directory Federation Services Configuration Wizard launches. On the **Connect to AD DS** page, enter the domain administrator account that you want to use as the AD FS account, and click **Next**.
4. On the **Specify Service Properties** page, enter the subject name of the SSL certificate to use for AD FS communication. In the test example, this is **blueadfs.contoso.com**.
5. Enter the Federation Service name. In the test example, this is **blueadfs.contoso.com**. Click **Next**.

   > **NOTE**
   > The Federation Service name must not use the name of an existing server in the environment. If you do use the name of an existing server, the AD FS installation will fail and must be restarted.

6. On the **Specify Service Account** page, enter the name that you would like to use for the managed service account. For the test example, select **Create a Group Managed Service Account**, and in **Account Name**, enter **ADFSService**. Click **Next**.
7. On the **Specify Configuration Database** page, select **Create a database on this server using Windows Internal Database**, and click **Next**.
8. The **Review Options** page shows you an overview of the options you have selected. Click **Next**.

9. The **Pre-requisite Checks** page indicates whether all the prerequisite checks passed successfully. If there are no issues, click **Configure**.

> **NOTE**
> If you used the name of the AD FS server or any other existing machine for the Federation Service Name, an error message is displayed. You must start the installation over and choose a name other than the name of an existing machine.

10. When the configuration completes successfully, the **Results** page confirms that AD FS was successfully configured.

### Configure AD FS by using PowerShell

To accomplish the equivalent configuration of AD FS via Windows PowerShell, use the following commands.

To install AD FS:

```
Add-WindowsFeature RSAT-AD-Tools
Add-WindowsFeature ADFS-Federation -IncludeManagementTools
```

To create the managed service account:

```
New-ADServiceAccount "ADFSService"-Server 2016-DC.contoso.com -Path "CN=Managed Service
Accounts,DC=Contoso,DC=COM" -DNSHostName 2016-ADFS.contoso.com -ServicePrincipalNames HTTP/2016-
ADFS,HTTP/2016-ADFS.contoso.com
```

After you configure AD FS, you must set up an AD FS farm by using the managed service account that you created in the previous step and the certificate you created in the pre-configuration steps.

To set up an AD FS farm:

```
$cert = Get-ChildItem CERT:\LocalMachine\My |where {$_.Subject -match blueadfs.contoso.com} | sort $_.NotAfter
-Descending | select -first 1
$thumbprint = $cert.Thumbprint
Install-ADFSFarm -CertificateThumbprint $thumbprint -FederationServiceDisplayName "Contoso Corporation" –
FederationServiceName blueadfs.contoso.com -GroupServiceAccountIdentifier contoso\ADFSService$ -
OverwriteConfiguration -ErrorAction Stop
```

Next step: Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work

## See Also

Work Folders Overview

# Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work

12/16/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

This topic describes the second step in deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. You can find the other steps in this process in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Overview
- Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set Up AD FS
- Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders
- Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy
- Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

> **NOTE**
> The instructions covered in this section are for a Windows Server 2019 or Windows Server 2016 environment. If you're using Windows Server 2012 R2, follow the Windows Server 2012 R2 instructions.

In step 1, you installed and configured AD FS. Now, you need to perform the following post-configuration steps for AD FS.

## Configure DNS entries

You must create two DNS entries for AD FS. These are the same two entries that were used in the pre-installation steps when you created the subject alternative name (SAN) certificate.

The DNS entries are in the form:

- AD FS service name.domain
- enterpriseregistration.domain
- AD FS server name.domain (DNS entry should already exist. e.g., 2016-ADFS.contoso.com)

In the test example, the values are:

- **blueadfs.contoso.com**
- **enterpriseregistration.contoso.com**

## Create the A and CNAME records for AD FS

To create A and CNAME records for AD FS, follow these steps:

1. On your domain controller, open DNS Manager.

2. Expand the Forward Lookup Zones folder, right-click on your domain, and select **New Host (A)**.
3. The **New Host** window opens. In the **Name** field, enter the alias for the AD FS service name. In the test example, this is **blueadfs**.

   The alias must be the same as the subject in the certificate that was used for AD FS. For example, if the subject was adfs.contoso.com, then the alias entered here would be **adfs**.

   > **IMPORTANT**
   > When you set up AD FS by using the Windows Server user interface (UI) instead of Windows PowerShell, you must create an A record instead of a CNAME record for AD FS. The reason is that the service principal name (SPN) that is created via the UI contains only the alias that is used to set up the AD FS service as the host.

4. In **IP address**, enter the IP address for the AD FS server. In the test example, this is **192.168.0.160**. Click **Add Host**.
5. In the Forward Lookup Zones folder, right-click on your domain again, and select **New Alias (CNAME)**.
6. In the **New Resource Record** window, add the alias name **enterpriseregistration** and enter the FQDN for the AD FS server. This alias is used for Device Join and must be called **enterpriseregistration**.
7. Click **OK**.

To accomplish the equivalent steps via Windows PowerShell, use the following command. The command must be executed on the domain controller.

```
Add-DnsServerResourceRecord  -ZoneName "contoso.com" -Name blueadfs -A -IPv4Address 192.168.0.160
Add-DnsServerResourceRecord  -ZoneName "contoso.com" -Name enterpriseregistration -CName  -HostNameAlias
2016-ADFS.contoso.com
```

## Set up the AD FS relying party trust for Work Folders

You can set up and configure the relying party trust for Work Folders, even though Work Folders hasn't been set up yet. The relying party trust must be set up to enable Work Folders to use AD FS. Because you're in the process of setting up AD FS, now is a good time to do this step.

To set up the relying party trust:

1. Open **Server Manager**, on the **Tools** menu, select **AD FS Management**.
2. In the right-hand pane, under **Actions**, click **Add Relying Party Trust**.
3. On the **Welcome** page, select **Claims aware** and click **Start**.
4. On the **Select Data Source** page, select **Enter data about the relying party manually**, and then click **Next**.
5. In the **Display name** field, enter **WorkFolders**, and then click **Next**.
6. On the **Configure Certificate** page, click **Next**. The token encryption certificates are optional, and are not needed for the test configuration.
7. On the **Configure URL** page, click **Next**.
8. On the **Configure Identifiers** page, add the following identifier: `https://windows-server-work-folders/V1`. This identifier is a hard-coded value used by Work Folders, and is sent by the Work Folders service when it is communicating with AD FS. Click **Next**.

9. On the Choose Access Control Policy page, select **Permit Everyone**, and then click **Next**.
10. On the **Ready to Add Trust** page, click **Next**.
11. After the configuration is finished, the last page of the wizard indicates that the configuration was successful. Select the checkbox for editing the claims rules, and click **Close**.
12. In the AD FS snap-in, select the **WorkFolders** relying party trust and click **Edit Claim Issuance Policy** under Actions.
13. The **Edit Claim Issuance Policy for WorkFolders** window opens. Click **Add rule**.
14. In the **Claim rule template** drop-down list, select **Send LDAP Attributes as Claims**, and click **Next**.
15. On the **Configure Claim Rule** page, in the **Claim rule name** field, enter **WorkFolders**.
16. In the **Attribute store** drop-down list, select **Active Directory**.
17. In the mapping table, enter these values:
    - User-Principal-Name: UPN
    - Display Name: Name
    - Surname: Surname
    - Given-Name: Given Name
18. Click **Finish**. You'll see the WorkFolders rule listed on the Issuance Transform Rules tab and click **OK**.

**Set relying part trust options**

After the relying party trust has been set up for AD FS, you must finish the configuration by running five commands in Windows PowerShell. These commands set options that are needed for Work Folders to communicate successfully with AD FS, and can't be set through the UI. These options are:

- Enable the use of JSON web tokens (JWTs)
- Disable encrypted claims
- Enable auto-update
- Set the issuing of Oauth refresh tokens to All Devices.
- Grant clients access to the relying party trust

To set these options, use the following commands:

```
Set-ADFSRelyingPartyTrust -TargetIdentifier "https://windows-server-work-folders/V1" -EnableJWT $true
Set-ADFSRelyingPartyTrust -TargetIdentifier "https://windows-server-work-folders/V1" -Encryptclaims $false
Set-ADFSRelyingPartyTrust -TargetIdentifier "https://windows-server-work-folders/V1" -AutoupdateEnabled $true
Set-ADFSRelyingPartyTrust -TargetIdentifier "https://windows-server-work-folders/V1" -
IssueOAuthRefreshTokensTo AllDevices
Grant-AdfsApplicationPermission -ServerRoleIdentifier "https://windows-server-work-folders/V1" -
AllowAllRegisteredClients -ScopeNames openid,profile
```

## Enable Workplace Join

Enabling Workplace Join is optional, but can be useful when you want users to be able to use their personal devices to access workplace resources.

To enable device registration for Workplace Join, you must run the following Windows PowerShell commands, which will configure device registration and set the global authentication policy:

```
Initialize-ADDeviceRegistration -ServiceAccountName <your AD FS service account>
    Example: Initialize-ADDeviceRegistration -ServiceAccountName contoso\adfsservice$
Set-ADFSGlobalAuthenticationPolicy -DeviceAuthenticationEnabled $true
```

## Export the AD FS certificate

Next, export the self-signed AD FS certificate so that it can be installed on the following machines in the test environment:

- The server that is used for Work Folders
- The server that is used for Web Application Proxy
- The domain-joined Windows client
- The non-domain-joined Windows client

To export the certificate, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type **MMC**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Certificates**, and then click **Add**. The Certificates Snap-in Wizard starts.
5. Select **Computer account**, and then click **Next**.
6. Select **Local computer: (the computer this console is running on)**, and then click **Finish**.
7. Click **OK**.
8. Expand the folder **Console Root\Certificates(Local Computer)\Personal\Certificates**.
9. Right-click the **AD FS certificate**, click **All Tasks**, and then click **Export...**.
10. The Certificate Export Wizard opens. Select **Yes, export the private key**.
11. On the **Export File Format** page, leave the default options selected, and click **Next**.
12. Create a password for the certificate. This is the password that you'll use later when you import the certificate to other devices. Click **Next**.
13. Enter a location and name for the certificate, and then click **Finish**.

Installation of the certificate is covered later in the deployment procedure.

## Manage the private key setting

You must give the AD FS service account permission to access the private key of the new certificate. You will need to grant this permission again when you replace the communication certificate after it expires. To grant permission, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type **MMC**.
3. On the **File** menu, click **Add/Remove Snap-in**.

4. In the **Available snap-ins** list, select **Certificates**, and then click **Add**. The Certificates Snap-in Wizard starts.
5. Select **Computer account**, and then click **Next**.
6. Select **Local computer: (the computer this console is running on)**, and then click **Finish**.
7. Click **OK**.
8. Expand the folder **Console Root\Certificates(Local Computer)\Personal\Certificates**.
9. Right-click the **AD FS certificate**, click **All Tasks**, and then click **Manage Private Keys**.
10. In the **Permissions** window, click **Add**.
11. In the **Object Types** window, select **Service Accounts**, and then click **OK**.
12. Type the name of the account that is running AD FS. In the test example, this is ADFSService. Click **OK**.
13. In the **Permissions** window, give the account at least read permissions, and click **OK**.

If you don't have the option to manage private keys, you might need to run the following command:
`certutil -repairstore my *`

## Verify that AD FS is operational

To verify that AD FS is operational, open a browser window and go to `https://blueadfs.contoso.com/federationmetadata/2007-06/federationmetadata.xml`, changing the URL to match your environment.

The browser window will display the federation server metadata without any formatting. If you can see the data without any SSL errors or warnings, your federation server is operational.

Next step: Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders

## See Also

Work Folders Overview

# Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set-up Work Folders

12/16/2020 • 8 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

This topic describes the third step in deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. You can find the other steps in this process in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Overview
- Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set Up AD FS
- Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work
- Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy
- Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

> **NOTE**
> The instructions covered in this section are for a Windows Server 2019 or Windows Server 2016 environment. If you're using Windows Server 2012 R2, follow the Windows Server 2012 R2 instructions.

To set up Work Folders, use the following procedures.

## Pre-installment work

In order to install Work Folders, you must have a server that is joined to the domain and running Windows Server 2016. The server must have a valid network configuration.

For the test example, join the machine that will run Work Folders to the Contoso domain and set up the network interface as described in the following sections.

### Set the server IP address

Change your server IP address to a static IP address. For the test example, use IP class A, which is 192.168.0.170 / subnet mask: 255.255.0.0 / Default Gateway: 192.168.0.1 / Preferred DNS: 192.168.0.150 (the IP address of your domain controller).

### Create the CNAME record for Work Folders

To create the CNAME record for Work Folders, follow these steps:

1. On your domain controller, open **DNS Manager**.
2. Expand the Forward Lookup Zones folder, right-click on your domain, and click **New Alias (CNAME)**.
3. In the **New Resource Record** window, in the **Alias name** field, enter the alias for Work Folders. In the test example, this is **workfolders**.
4. In the **Fully qualified domain name** field, the value should be **workfolders.contoso.com**.
5. In the **Fully qualified domain name for target host** field, enter the FQDN for the Work Folders server. In the test example, this is **2016-WF.contoso.com**.

6. Click **OK**.

To accomplish the equivalent steps via Windows PowerShell, use the following command. The command must be executed on the domain controller.

```
Add-DnsServerResourceRecord  -ZoneName "contoso.com" -Name workfolders -CName  -HostNameAlias 2016-wf.contoso.com
```

**Install the AD FS certificate**

Install the AD FS certificate that was created during AD FS setup into the local computer certificate store, using these steps:

1. Click **Start**, and then click **Run**.
2. Type **MMC**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Certificates**, and then click **Add**. The Certificates Snap-in Wizard starts.
5. Select **Computer account**, and then click **Next**.
6. Select **Local computer: (the computer this console is running on)**, and then click **Finish**.
7. Click **OK**.
8. Expand the folder **Console Root\Certificates(Local Computer)\Personal\Certificates**.
9. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
10. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the certificate store.
11. Expand the folder **Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates**.
12. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
13. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the Trusted Root Certification Authorities store.

**Create the Work Folders self-signed certificate**

To create the Work Folders self-signed certificate, follow these steps:

1. Download the scripts provided in the Deploying Work Folders with AD FS and Web Application Proxy blog post and then copy the file makecert.ps1 to the Work Folders machine.
2. Open a Windows PowerShell window with admin privileges.
3. Set the execution policy to unrestricted:

   ```
   PS C:\temp\scripts> Set-ExecutionPolicy -ExecutionPolicy Unrestricted
   ```

4. Change to the directory where you copied the script.
5. Execute the makeCert script:

```
PS C:\temp\scripts> .\makecert.ps1
```

6. When you are prompted to change the subject certificate, enter the new value for the subject. In this example, the value is **workfolders.contoso.com**.
7. When you are prompted to enter subject alternative name (SAN) names, press Y and then enter the SAN names, one at a time.

   For this example, type **workfolders.contoso.com**, and press Enter. Then type **2016-WF.contoso.com** and press Enter.

   When all of the SAN names have been entered, press Enter on an empty line.
8. When you are prompted to install the certificates to the Trusted Root Certification Authority store, press Y.

The Work Folders certificate must be a SAN certificate with the following values:

- **workfolders.domain**
- **machine name.domain**

In the test example, the values are:

- **workfolders.contoso.com**
- **2016-WF.contoso.com**

## Install Work Folders

To install the Work Folders role, follow these steps:

1. Open **Server Manager**, click **Add roles and features**, and click **Next**.
2. On the **Installation Type** page, select **Role-based or feature-based installation**, and click **Next**.
3. On the **Server Selection** page, select the current server, and click **Next**.
4. On the **Server Roles** page, expand **File and Storage Services**, expand **File and iSCSI Services**, and then select **Work Folders**.
5. On the **Add Roles and Feature Wizard** page, click **Add Features**, and click **Next**.
6. On the **Features** page, click **Next**.
7. On the **Confirmation** page, click **Install**.

## Configure Work Folders

To configure Work Folders, follow these steps:

1. Open **Server Manager**.
2. Select **File and Storage Services**, and then select **Work Folders**.
3. On the **Work Folders** page, start the **New Sync Share Wizard**, and click **Next**.
4. On the **Server and Path** page, select the server where the sync share will be created, enter a local path where the Work Folders data will be stored, and click **Next**.

   If the path doesn't exist, you'll be prompted to create it. Click **OK**.

5. On the **User Folder Structure** page, select **User alias**, and then click **Next**.
6. On the **Sync Share Name** page, enter the name for the sync share. For the test example, this is **WorkFolders**. Click **Next**.
7. On the **Sync Access** page, add the users or groups that will have access to the new sync share. For the test example, grant access to all domain users. Click **Next**.
8. On the **PC Security Policies** page, select **Encrypt work folders** and **Automatically lock page and require a password**. Click **Next**.
9. On the **Confirmation** page, click **Create** to finish the configuration process.

# Work Folders post-configuration work

To finish setting up Work Folders, complete these additional steps:

- Bind the Work Folders certificate to the SSL port
- Configure Work Folders to use AD FS authentication
- Export the Work Folders certificate (if you are using a self-signed certificate)

### Bind the certificate

Work Folders communicates only over SSL and must have the self-signed certificate that you created earlier (or that your certificate authority issued) bound to the port.

There are two methods that you can use to bind the certificate to the port via Windows PowerShell: IIS cmdlets and netsh.

#### Bind the certificate by using netsh

To use the netsh command-line scripting utility in Windows PowerShell, you must pipe the command to netsh. The following example script finds the certificate with the subject **workfolders.contoso.com** and binds it to port 443 by using netsh:

```
$subject = "workfolders.contoso.com"
Try
{
#In case there are multiple certificates with the same subject, get the latest version
$cert = Get-ChildItem CERT:\LocalMachine\My |where {$_.Subject -match $subject} | sort $_.NotAfter -
Descending | select -first 1
$thumbprint = $cert.Thumbprint
$Command = "http add sslcert ipport=0.0.0.0:443 certhash=$thumbprint appid={CE66697B-3AA0-49D1-BDBD-
A25C8359FD5D} certstorename=MY"
$Command | netsh
}
Catch
{
"     Error: unable to locate certificate for $($subject)"
Exit
}
```

#### Bind the certificate by using IIS cmdlets

You can also bind the certificate to the port by using IIS management cmdlets, which are available if you installed the IIS management tools and scripts.

> **NOTE**
>
> Installation of the IIS management tools doesn't enable the full version of Internet Information Services (IIS) on the Work Folders machine; it only enables the management cmdlets. There are some possible benefits to this setup. For example, if you're looking for cmdlets to provide the functionality that you get from netsh. When the certificate is bound to the port via the New-WebBinding cmdlet, the binding is not dependent on IIS in any way. After you do the binding, you can even remove the Web-Mgmt-Console feature, and the certificate will still be bound to the port. You can verify the binding via netsh by typing **netsh http show sslcert**.

The following example uses the New-WebBinding cmdlet to find the certificate with the subject **workfolders.contoso.com** and bind it to port 443:

```
$subject = "workfolders.contoso.com"
Try
{
#In case there are multiple certificates with the same subject, get the latest version
$cert =Get-ChildItem CERT:\LocalMachine\My |where {$_.Subject -match $subject } | sort $_.NotAfter -
Descending | select -first 1
$thumbprint = $cert.Thumbprint
New-WebBinding -Name "Default Web Site" -IP * -Port 443 -Protocol https
#The default IIS website name must be used for the binding. Because Work Folders uses Hostable Web Core and
its own configuration file, its website name, 'ECSsite', will not work with the cmdlet. The workaround is to
use the default IIS website name, even though IIS is not enabled, because the NewWebBinding cmdlet looks for
a site in the default IIS configuration file.
Push-Location IIS:\SslBindings
Get-Item cert:\LocalMachine\MY\$thumbprint | new-item *!443
Pop-Location
}
Catch
{
"     Error: unable to locate certificate for $($subject)"
Exit
}
```

**Set up AD FS authentication**

To configure Work Folders to use AD FS for authentication, follow these steps:

1. Open **Server Manager**.
2. Click **Servers**, and then select your Work Folders server in the list.
3. Right-click the server name, and click **Work Folders Settings**.
4. In the **Work Folder Settings** window, select **Active Directory Federation Services**, and type in the Federation Service URL. Click **Apply**.

   In the test example, the URL is **https://blueadfs.contoso.com**.

The cmdlet to accomplish the same task via Windows PowerShell is:

```
Set-SyncServerSetting -ADFSUrl "https://blueadfs.contoso.com"
```

If you're setting up AD FS with self-signed certificates, you might receive an error message that says the Federation Service URL is incorrect, unreachable, or a relying party trust has not been set up.

This error can also happen if the AD FS certificate was not installed on the Work Folders server or if the CNAME for AD FS was not set up correctly. You must correct these issues before proceeding.

**Export the Work Folders certificate**

The self-signed Work Folders certificate must be exported so that you can later install it on the following machines in the test environment:

- The server that is used for Web Application Proxy
- The domain-joined Windows client
- The non-domain-joined Windows client

To export the certificate, follow the same steps you used to export the AD FS certificate earlier, as described in Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work, Export the AD FS certificate.

Next step: Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy

## See Also

Work Folders Overview

# Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set-up Web Application Proxy

12/16/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

This topic describes the fourth step in deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. You can find the other steps in this process in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Overview
- Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set Up AD FS
- Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work
- Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders
- Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

> **NOTE**
> The instructions covered in this section are for a Windows Server 2019 or Windows Server 2016 environment. If you're using Windows Server 2012 R2, follow the Windows Server 2012 R2 instructions.

To set up Web Application Proxy for use with Work Folders, use the following procedures.

## Install the AD FS and Work Folder certificates

You must install the AD FS and Work Folders certificates that you created earlier (in step 1, Set up AD FS, and step 3, Set up Work Folders) into the local computer certificate store on the machine where the Web Application Proxy role will be installed.

Because you're installing self-signed certificates that can't be traced back to a publisher in the Trusted Root Certification Authorities certificate store, you must also copy the certificates to that store.

To install the certificates, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type **MMC**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Certificates**, and then click **Add**. The Certificates Snap-in Wizard starts.
5. Select **Computer account**, and then click **Next**.
6. Select **Local computer: (the computer this console is running on)**, and then click **Finish**.
7. Click **OK**.

8. Expand the folder **Console Root\Certificates(Local Computer)\Personal\Certificates**.
9. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
10. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the certificate store.
11. Repeat steps 9 and 10, this time browsing to the Work Folders certificate and importing it.
12. Expand the folder **Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates**.
13. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
14. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the Trusted Root Certification Authorities store.
15. Repeat steps 13 and 14, this time browsing to the Work Folders certificate and importing it.

## Install Web Application Proxy

To install Web Application Proxy, follow these steps:

1. On the server where you plan to install the Web Application Proxy, open **Server Manager** and start the **Add Roles and Features** Wizard.
2. Click **Next** on the first and second pages of the wizard.
3. On the **Server Selection** page, select your server, and then click **Next**.
4. On the **Server Role** page, select the **Remote Access** role, and then click **Next**.
5. On the Features page and Remote Access page, click **Next**.
6. On the **Role Services** page, select **Web Application Proxy**, click **Add Features**, and then click **Next**.
7. On the **Confirm installation selections** page, click **Install**.

## Configure Web Application Proxy

To configure Web Application Proxy, follow these steps:

1. Click the warning flag at the top of Server Manager, and then click the link to open the Web Application Proxy Configuration Wizard.
2. On the Welcome page, press **Next**.
3. On the **Federation Server** page, enter the Federation Service name. In the test example, this is **blueadfs.contoso.com**.
4. Enter the credentials of a local administrator account on the federation servers. Do not enter in domain credentials (for example, contoso\administrator), but local credentials (for example, administrator).
5. On the **AD FS Proxy Certificate** page, select the AD FS certificate that you imported earlier. In the test case, this is **blueadfs.contoso.com**. Click **Next**.
6. The confirmation page shows the Windows PowerShell command that will execute to configure the service. Click **Configure**.

## Publish the Work Folders web application

The next step is to publish a web application that will make Work Folders available to clients. To publish the Work Folders web application, follow these steps:

1. Open **Server Manager**, and on the **Tools** menu, click **Remote Access Management** to open the Remote Access Management Console.
2. Under **Configuration**, click **Web Application Proxy**.
3. Under **Tasks**, click **Publish**. The Publish New Application Wizard opens.
4. On the Welcome page, click **Next**.
5. On the **Preauthentication** page, select **Active Directory Federation Services (AD FS)**, and click **Next**.
6. On the **Support Clients** page, select **OAuth2**, and click **Next**.
7. On the **Relying Party** page, select **Work Folders**, and then click **Next**. This list is published to the Web Application Proxy from AD FS.
8. On the **Publishing Settings** page, enter the following and then click **Next**:
   - The name you want to use for the web application
   - The external URL for Work Folders
   - The name of the Work Folders certificate
   - The back-end URL for Work Folders

   By default, the wizard makes the back-end URL the same as the external URL.

   For the test example, use these values:

   Name: **WorkFolders**

   External URL: **https://workfolders.contoso.com**

   External certificate: **The Work Folders certificate that you installed earlier**

   Backend server URL: **https://workfolders.contoso.com**
9. The confirmation page shows the Windows PowerShell command that will execute to publish the application. Click **Publish**.
10. On the **Results** page, you should see the application was published successfully.

> **NOTE**
> If you have multiple Work Folders servers, you need to publish a Work Folders web application for each Work Folders server (repeat steps 1-10).

Next step: Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set Up Clients

## See Also

Work Folders Overview

# Deploy Work Folders with AD FS and Web Application Proxy: Step 5, Set-up Clients

12/16/2020 • 4 minutes to read • Edit Online

Applies to: Windows Server (Semi-Annual Channel), Windows Server 2016

This topic describes the fifth step in deploying Work Folders with Active Directory Federation Services (AD FS) and Web Application Proxy. You can find the other steps in this process in these topics:

- Deploy Work Folders with AD FS and Web Application Proxy: Overview
- Deploy Work Folders with AD FS and Web Application Proxy: Step 1, Set Up AD FS
- Deploy Work Folders with AD FS and Web Application Proxy: Step 2, AD FS Post-Configuration Work
- Deploy Work Folders with AD FS and Web Application Proxy: Step 3, Set Up Work Folders
- Deploy Work Folders with AD FS and Web Application Proxy: Step 4, Set Up Web Application Proxy

Use the following procedures to set up the domain-joined and non-domain joined Windows clients. You can use these clients to test whether files are syncing correctly between the clients' Work Folders.

## Set up a domain-joined client

**Install the AD FS and Work Folder certificates**

You must install the AD FS and Work Folders certificates that you created earlier into the local computer certificate store on the domain-joined client machine.

Because you are installing self-signed certificates that can't be traced back to a publisher in the Trusted Root Certification Authorities certificate store, you must also copy the certificates to that store.

To install the certificates, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type **MMC**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Available snap-ins** list, select **Certificates**, and then click **Add**. The Certificates Snap-in Wizard starts.
5. Select **Computer account**, and then click **Next**.
6. Select **Local computer: (the computer this console is running on)**, and then click **Finish**.
7. Click **OK**.
8. Expand the folder Console Root\Certificates(Local Computer)\Personal\Certificates.
9. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
10. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the certificate store.
11. Repeat steps 9 and 10, this time browsing to the Work Folders certificate and importing it.

12. Expand the folder Console Root\Certificates(Local Computer)\Trusted Root Certification Authorities\Certificates.
13. Right-click **Certificates**, click **All Tasks**, and then click **Import**.
14. Browse to the folder that contains the AD FS certificate, and follow the instructions in the wizard to import the file and place it in the Trusted Root Certification Authorities store.
15. Repeat steps 13 and 14, this time browsing to the Work Folders certificate and importing it.

**Configure Work Folders on the client**

To configure Work Folders on the client machine, follow these steps:

1. On the client machine, open **Control Panel** and click **Work Folders**.
2. Click **Set up Work Folders**.
3. On the **Enter your work email address** page, enter either the user's email address (for example, user@contoso.com) or the Work Folders URL (in the test example, https://workfolders.contoso.com), and then click **Next**.
4. If the user is connected to the corporate network, the authentication is performed by Windows Integrated Authentication. If the user is not connected to the corporate network, the authentication is performed by ADFS (OAuth) and the user will be prompted for credentials. Enter your credentials and click **OK**.
5. After you have authenticated, the **Introducing Work Folders** page is displayed, where you can optionally change the Work Folders directory location. Click **Next**.
6. The **Security Policies** page lists the security policies that you set up for Work Folders. Click **Next**.
7. A message is displayed stating that Work Folders has started syncing with your PC. Click **Close**.
8. The **Manage Work Folders** page shows the amount of space available on the server, sync status, and so on. If necessary, you can re-enter your credentials here. Close the window.
9. Your Work Folders folder opens automatically. You can add content to this folder to sync between your devices.

   For the purpose of the test example, add a test file to this Work Folders folder. After you set up Work Folders on the non-domain-joined machine, you will be able to sync files between the Work Folders on each machine.

## Set up a non-domain-joined client

**Install the AD FS and Work Folder certificates**

Install the AD FS and Work Folders certificates on the non-domain-joined machine, using the same procedure that you used for the domain-joined machine.

**Update the hosts file**

The hosts file on the non-domain-joined client must be updated for the test environment, because no public DNS records were created for Work Folders. Add these entries to the hosts file:

- workfolders.domain
- AD FS service name.domain
- enterpriseregistration.domain

For the test example, use these values:

- 10.0.0.10 workfolders.contoso.com
- 10.0.0.10 blueadfs.contoso.com
- 10.0.0.10 enterpriseregistration.contoso.com

**Configure Work Folders on the client**

Configure Work Folders on the non-domain-joined machine by using the same procedure that you used for the domain-joined machine.

When the new Work Folders folder opens on this client, you can see that the file from the domain-joined machine has already synced to the non-domain-joined machine. You can start adding content to the folder to sync between your devices.

This concludes the procedure for deploying Work Folders, AD FS and Web Application Proxy via the Windows Server UI.

## See Also

Work Folders Overview

# Storage Quality of Service

12/16/2020 • 29 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

Storage Quality of Service (QoS) in Windows Server 2016 provides a way to centrally monitor and manage storage performance for virtual machines using Hyper-V and the Scale-Out File Server roles. The feature automatically improves storage resource fairness between multiple virtual machines using the same file server cluster and allows policy-based minimum and maximum performance goals to be configured in units of normalized IOPs.

You can use Storage QoS in Windows Server 2016 to accomplish the following:

- **Mitigate noisy neighbor issues.** By default, Storage QoS ensures that a single virtual machine cannot consume all storage resources and starve other virtual machines of storage bandwidth.
- **Monitor end to end storage performance.** As soon as virtual machines stored on a Scale-Out File Server are started, their performance is monitored. Performance details of all running virtual machines and the configuration of the Scale-Out File Server cluster can be viewed from a single location
- **Manage Storage I/O per workload business needs** Storage QoS policies define performance minimums and maximums for virtual machines and ensures that they are met. This provides consistent performance to virtual machines, even in dense and overprovisioned environments. If policies cannot be met, alerts are available to track when VMs are out of policy or have invalid policies assigned.

This document outlines how your business can benefit from the new Storage QoS functionality. It assumes that you have a previous working knowledge of Windows Server, Windows Server Failover Clustering, Scale-Out File Server, Hyper-V, and Windows PowerShell.

## Overview

This section describes the requirements for using Storage QoS, an overview of a software-defined solution using Storage QoS, and a list of Storage QoS related terminologies.

### Storage QoS Requirements

Storage QoS supports two deployment scenarios:

- **Hyper-V using a Scale-Out File Server** This scenario requires both of the following:
  - Storage cluster that is a Scale-Out File Server cluster
  - Compute cluster that has least one server with the Hyper-V role enabled

  For Storage QoS, the Failover Cluster is required on Storage servers, but the compute servers are not required to be in a failover cluster. All servers (used for both Storage and Compute) must be running Windows Server 2016.

  If you do not have a Scale-Out File Server cluster deployed for evaluation purposes, for step by step instructions to build one using either existing servers or virtual machines, see Windows Server 2012 R2 Storage: Step-by-step with Storage Spaces, SMB Scale-Out and Shared VHDX (Physical).
- **Hyper-V using Cluster Shared Volumes.** This scenario requires both of the following:
  - Compute cluster with the Hyper-V role enabled

- Hyper-V using Cluster Shared Volumes (CSV) for storage

Failover Cluster is required. All servers must be running the same version of Windows Server 2016.

### Using Storage QoS in a software-defined storage solution

Storage Quality of Service is built into the Microsoft software-defined storage solution provided by Scale-Out File Server and Hyper-V. The Scale-Out File Server exposes file shares to the Hyper-V servers using the SMB3 protocol. A new Policy Manager has been added to the File Server cluster, which provides the central storage performance monitoring.

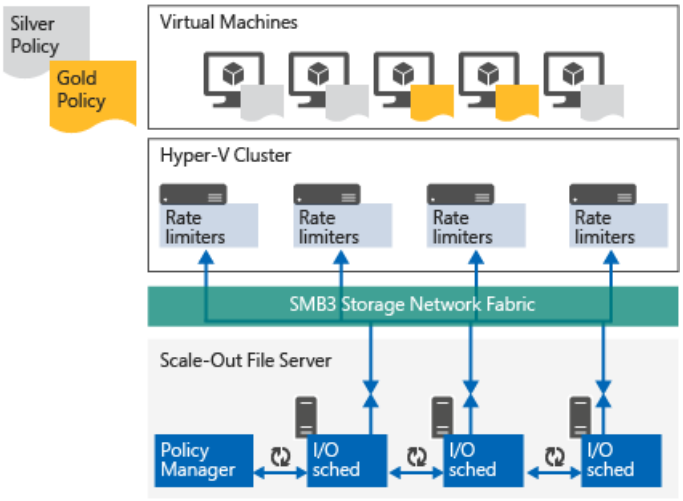



Figure 1: Using Storage QoS in a software-defined storage solution in Scale-Out File Server

As Hyper-V servers launch virtual machines, they are monitored by the Policy Manager. The Policy Manager communicates the Storage QoS policy and any limits or reservations back to the Hyper-V server, which controls the performance of the virtual machine as appropriate.

When there are changes to Storage QoS policies or to the performance demands by virtual machines, the Policy Manager notifies the Hyper-V servers to adjust their behavior. This feedback loop ensures that all virtual machines VHDs perform consistently according to the Storage QoS policies as defined.

### Glossary

| TERM | DESCRIPTION |
|---|---|
| Normalized IOPs | All of the storage usage is measured in "Normalized IOPs." This is a count of the storage input/output operations per second. Any IO that is 8KB or smaller is considered as one normalized IO. Any IO that is larger than 8KB is treated as multiple normalized IOs. For example, a 256KB request is treated as 32 normalized IOPs.<br>Windows Server 2016 includes the ability to specify the size used to normalize IOs. On the storage cluster, the normalized size can be specified and take effect on the normalization calculations cluster wide. The default remains 8KB. |
| Flow | Each file handle opened by a Hyper-V server to a VHD or VHDX file is considered a "flow". If a virtual machine has two virtual hard disks attached, it will have 1 flow to the file server cluster per file. If a VHDX is shared with multiple virtual machines, it will have 1 flow per virtual machine. |

| TERM | DESCRIPTION |
| --- | --- |
| InitiatorName | Name of the virtual machine that is reported to the Scale-Out File Server for each flow. |
| InitiatorID | An identifier matching the virtual machine ID. This can always be used to uniquely identify individual flows virtual machines even if the virtual machines have the same InitiatorName. |
| Policy | Storage QoS policies are stored in the cluster database, and have the following properties: PolicyId, MinimumIOPS, MaximumIOPS, ParentPolicy, and PolicyType. |
| PolicyId | Unique identifier for a policy. It is generated by default, but can be specified if desired. |
| MinimumIOPS | Minimum normalized IOPS that will be provided by a policy. Also known as "Reservation". |
| MaximumIOPS | Maximum normalized IOPS that will be limited by a policy. Also known as "Limit". |
| Aggregated | A policy type where the specified MinimumIOPS & MaximumIOPS and Bandwidth are shared among all flows assigned to the policy. All VHD's assigned the policy on that storage system have a single allocation of I/O bandwidth for them to all share. |
| Dedicated | A policy type where the specified Minimum & MaximumIOPs and Bandwidth are managed for individual VHD/VHDx. |

# How to set up Storage QoS and monitor basic performance

This section describes how to enable the new Storage QoS feature and how to monitor storage performance without applying custom policies.

### Set up Storage QoS on a Storage Cluster

This section discusses how to enable Storage QoS on either a new or an existing Failover Cluster and Scale-Out File Server that is running Windows Server 2016.

#### Set up Storage QoS on a new installation

If you have configured a new Failover Cluster and configured a Cluster Shared Volume(CSV) on Windows Server 2016, then the Storage QoS feature will be set up automatically.

#### Verify Storage QoS installation

After you have created a Failover Cluster and configured a CSV disk, , **Storage QoS Resource** is displayed as a Cluster Core Resource and visible in both Failover Cluster Manager and Windows PowerShell. The intent is that the failover cluster system will manage this resource and you should not have to do any actions against this resource. We display it in both Failover Cluster Manager and PowerShell to be consistent with the other failover cluster system resources like the new Health Service.

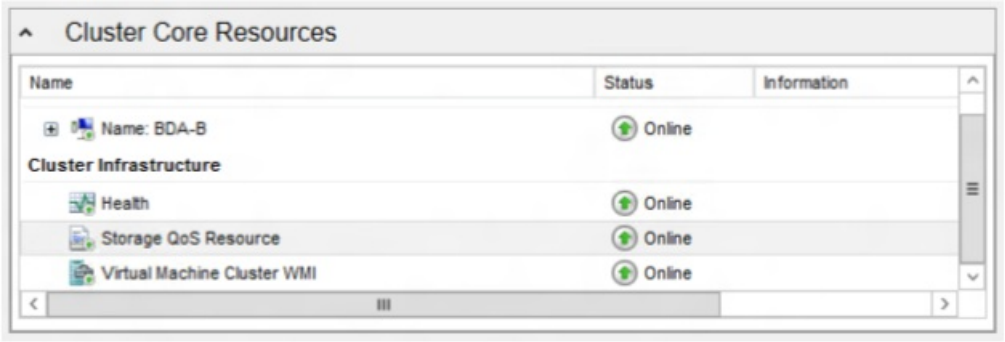



Figure 2: Storage QoS Resource displayed as a Cluster Core Resource in Failover Cluster Manager

Use the following PowerShell cmdlet to view the status of Storage QoS Resource.

```
PS C:\> Get-ClusterResource -Name "Storage Qos Resource"

Name                   State      OwnerGroup         ResourceType
----                   -----      ----------         ------------
Storage Qos Resource   Online     Cluster Group      Storage QoS Policy Manager
```

### Set up Storage QoS on a Compute Cluster

The Hyper-V role in Windows Server 2016 has built-in support for Storage QoS and is enabled by default.

#### Install Remote Administration Tools to manage Storage QoS policies from remote computers

You can manage Storage QoS policies and monitor flows from compute hosts using the Remote Server Administration Tools. These are available as optional features on all Windows Server 2016 installations, and can be downloaded separately for Windows 10 at the Microsoft Download Center website.

The **RSAT-Clustering** optional feature includes the Windows PowerShell module for remote management of Failover Clustering, including Storage QoS.

- Windows PowerShell: Add-WindowsFeature RSAT-Clustering

The **RSAT-Hyper-V-Tools** optional feature includes the Windows PowerShell module for remote management of Hyper-V.

- Windows PowerShell: Add-WindowsFeature RSAT-Hyper-V-Tools

#### Deploy virtual machines to run workloads for testing

You will need some virtual machines stored on the Scale-Out File Server with relevant workloads. For some tips in how to simulate load and do some stress testing, see the following page for a recommended tool (DiskSpd) and some example usage: DiskSpd, PowerShell and storage performance: measuring IOPs, throughput and latency for both local disks and SMB file shares.

The example scenarios shown in this guide includes five virtual machines. BuildVM1, BuildVM2, BuildVM3 and BuildVM4 are running a desktop workload with low to moderate storage demands. TestVm1 is running an online transaction processing benchmark with high storage demand.

### View current storage performance metrics

This section includes:

- How to query flows using the `Get-StorageQosFlow` cmdlet.
- How to view performance for a volume using the `Get-StorageQosVolume` cmdlet.

#### Query flows using the Get-StorageQosFlow cmdlet

The Get-StorageQosFlow cmdlet shows all current flows initiated by Hyper-V servers. All data is collected by the Scale-Out File Server cluster, hence the cmdlet can be used on any node in the Scale-Out File Server cluster, or

against a remote server using the -CimSession parameter.

**The following sample command shows how to view all files opened by Hyper-V on server using Get-StorageQoSFlow.**

```
PS C:\> Get-StorageQosFlow

InitiatorName    InitiatorNodeNam StorageNodeName  FilePath        Status
                 e
-------------    ---------------- ---------------  --------        ------
                                  plang-fs3.pla... C:\ClusterSt... Ok
                                  plang-fs2.pla... C:\ClusterSt... Ok
                                  plang-fs1.pla... C:\ClusterSt... Ok
                                  plang-fs3.pla... C:\ClusterSt... Ok
                                  plang-fs2.pla... C:\ClusterSt... Ok
                                  plang-fs1.pla... C:\ClusterSt... Ok
TR20-VMM         plang-z400.pl... plang-fs1.pla... C:\ClusterSt... Ok
BuildVM4         plang-c2.plan... plang-fs1.pla... C:\ClusterSt... Ok
WinOltp1         plang-c1.plan... plang-fs1.pla... C:\ClusterSt... Ok
BuildVM3         plang-c2.plan... plang-fs1.pla... C:\ClusterSt... Ok
BuildVM1         plang-c2.plan... plang-fs1.pla... C:\ClusterSt... Ok
TR20-VMM         plang-z400.pl... plang-fs1.pla... C:\ClusterSt... Ok
BuildVM2         plang-c2.plan... plang-fs1.pla... C:\ClusterSt... Ok
TR20-VMM         plang-z400.pl... plang-fs1.pla... C:\ClusterSt... Ok
                                  plang-fs3.pla... C:\ClusterSt... Ok
                                  plang-fs2.pla... C:\ClusterSt... Ok
BuildVM4         plang-c2.plan... plang-fs2.pla... C:\ClusterSt... Ok
WinOltp1         plang-c1.plan... plang-fs2.pla... C:\ClusterSt... Ok
BuildVM3         plang-c2.plan... plang-fs2.pla... C:\ClusterSt... Ok
WinOltp1         plang-c1.plan... plang-fs2.pla... C:\ClusterSt... Ok
                                  plang-fs1.pla... C:\ClusterSt... Ok
```

The following sample command is formatted to show virtual machine name, Hyper-V host name, IOPs, and VHD file name, sorted by IOPS.

```
PS C:\> Get-StorageQosFlow | Sort-Object StorageNodeIOPs -Descending | ft InitiatorName, @{Expression=
{$_.InitiatorNodeName.Substring(0,$_.InitiatorNodeName.IndexOf('.'))};Label="InitiatorNodeName"},
StorageNodeIOPs, Status, @{Expression={$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -
AutoSize

InitiatorName InitiatorNodeName StorageNodeIOPs Status File
------------- ----------------- --------------- ------ ----
WinOltp1      plang-c1                     3482     Ok IOMETER.VHDX
BuildVM2      plang-c2                      544     Ok BUILDVM2.VHDX
BuildVM1      plang-c2                      497     Ok BUILDVM1.VHDX
BuildVM4      plang-c2                      316     Ok BUILDVM4.VHDX
BuildVM3      plang-c2                      296     Ok BUILDVM3.VHDX
BuildVM4      plang-c2                      195     Ok WIN8RTM_ENTERPRISE_VL_BU...
TR20-VMM      plang-z400                    156     Ok DATA1.VHDX
BuildVM3      plang-c2                       81     Ok WIN8RTM_ENTERPRISE_VL_BU...
WinOltp1      plang-c1                       65     Ok BOOT.VHDX
                                             18     Ok DefaultFlow
                                             12     Ok DefaultFlow
WinOltp1      plang-c1                        4     Ok 9914.0.AMD64FRE.WINMAIN....
TR20-VMM      plang-z400                      4     Ok DATA2.VHDX
TR20-VMM      plang-z400                      3     Ok BOOT.VHDX
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
                                              0     Ok DefaultFlow
```

The following sample command shows how to filter flows based on InitiatorName to easily find the storage performance and settings for a specific virtual machine.

```
PS C:\> Get-StorageQosFlow -InitiatorName BuildVm1 | Format-List

FilePath           : C:\ClusterStorage\Volume2\SHARES\TWO\BUILDWORKLOAD\BUILDVM1.V
                     HDX
FlowId             : ebfecb54-e47a-5a2d-8ec0-0940994ff21c
InitiatorId        : ae4e3dd0-3bde-42ef-b035-9064309e6fec
InitiatorIOPS      : 464
InitiatorLatency   : 26.2684
InitiatorName      : BuildVM1
InitiatorNodeName  : plang-c2.plang.nttest.microsoft.com
Interval           : 300000
Limit              : 500
PolicyId           : b145e63a-3c9e-48a8-87f8-1dfc2abfe5f4
Reservation        : 500
Status             : Ok
StorageNodeIOPS    : 475
StorageNodeLatency : 7.9725
StorageNodeName    : plang-fs1.plang.nttest.microsoft.com
TimeStamp          : 2/12/2015 2:58:49 PM
VolumeId           : 4d91fc3a-1a1e-4917-86f6-54853b2a6787
PSComputerName     :
MaximumIops        : 500
MinimumIops        : 500
```

The data returned by the `Get-StorageQosFlow` cmdlet includes:

- The Hyper-V hostname (InitiatorNodeName).
- The virtual machine's name and its Id (InitiatorName and InitiatorId)
- Recent average performance as observed by the Hyper-V host for the virtual disk (InitiatorIOPS, InitiatorLatency)
- Recent average performance as observed by the Storage cluster for the virtual disk (StorageNodeIOPS, StorageNodeLatency)
- Current policy being applied to the file, if any, and the resulting configuration (PolicyId, Reservation, Limit)
- Status of the policy
    - **Ok** - No issues exist
    - InsufficientThroughput- A policy is applied, but the Minimum IOPs cannot be delivered. This can happen if the minimum for a VM, or all VMs together, are more than the storage volume can deliver.
    - **UnknownPolicyId** - A policy was assigned to the virtual machine on the Hyper-V host, but is missing from the file server. This policy should be removed from the virtual machine configuration, or a matching policy should be created on the file server cluster.

#### View performance for a volume using Get-StorageQosVolume

Storage performance metrics are also collected on a per-storage volume level, in addition to the per-flow performance metrics. This makes it easy to see the average total utilization in normalized IOPs, latency, and aggregate limits and reservations applied to a volume.

```
PS C:\> Get-StorageQosVolume | Format-List

Interval       : 300000
IOPS           : 0
Latency        : 0
Limit          : 0
Reservation    : 0
Status         : Ok
TimeStamp      : 2/12/2015 2:59:38 PM
VolumeId       : 434f561f-88ae-46c0-a152-8c6641561504
PSComputerName :
MaximumIops    : 0
MinimumIops    : 0

Interval       : 300000
IOPS           : 1097
Latency        : 3.1524
Limit          : 0
Reservation    : 1568
Status         : Ok
TimeStamp      : 2/12/2015 2:59:38 PM
VolumeId       : 4d91fc3a-1a1e-4917-86f6-54853b2a6787
PSComputerName :
MaximumIops    : 0
MinimumIops    : 1568

Interval       : 300000
IOPS           : 5354
Latency        : 6.5084
Limit          : 0
Reservation    : 781
Status         : Ok
TimeStamp      : 2/12/2015 2:59:38 PM
VolumeId       : 0d2fd367-8d74-4146-9934-306726913dda
PSComputerName :
MaximumIops    : 0
MinimumIops    : 781
```

# How to create and monitor Storage QoS Policies

This section describes how to create Storage QoS policies, apply these policies to virtual machines, and monitor a storage cluster after policies are applied.

**Create Storage QoS policies**

Storage QoS policies are defined and managed in the Scale-Out File Server cluster. You can create as many policies as needed for flexible deployments (up to 10,000 per storage cluster).

Each VHD/VHDX file assigned to a virtual machine may be configured with a policy. Different files and virtual machines can use the same policy or they can each be configured with separate policies. If multiple VHD/VHDX files or multiple virtual machines are configured with the same policy, they will be aggregated together and will share the MinimumIOPS and MaximumIOPS fairly. If you use separate policies for multiple VHD/VHDX files or virtual machines, the minimum and maximums are tracked separately for each.

If you create multiple similar policies for different virtual machines and the virtual machines have equal storage demand, they will receive a similar share of IOPs. If one VM demands more and the other less, then IOPs will follow that demand.

**Types of Storage QoS Policies**

There are two types of policies: Aggregated (previously known as SingleInstance) and Dedicated (previously known as MultiInstance). Aggregated policies apply maximums and minimum for the combined set of VHD/VHDX files and virtual machines where they apply. In effect, they share a specified set of IOPS and bandwidth. Dedicated

policies apply the minimum and maximum values for each VHD/VHDx, separately. This makes it easy to create a single policy that applies similar limits to multiple VHD/VHDx files.

For instance, if you create a Aggregated policy with a minimum of 300 IOPs and a maximum of 500 IOPs. If you apply this policy to 5 different VHD/VHDx files, you are making sure that the 5 VHD/VHDx files combined will be guaranteed at least 300 IOPs (if there is demand and the storage system can provide that performance) and no more than 500 IOPs. If the VHD/VHDx files have similar high demand for IOPs and the storage system can keep up, each VHD/VHDx files will get about 100 IOPs.

However, if you create a Dedicated policy with similar limits and apply it to VHD/VHDx files on 5 different virtual machines, each virtual machine will get at least 300 IOPs and no more than 500 IOPs. If the virtual machines have similar high demand for IOPs and the storage system can keep up, each virtual machine will get about 500 IOPs. . If one of the virtual machines has multiple VHD/VHDx files with the same MulitInstance policy configured, they will share the limit so that the total IO from the VM from files with that policy will not exceed the limits.

Hence, if you have a group of VHD/VHDx files that you want to exhibit the same performance characteristics and you don't want the trouble of creating multiple, similar policies, you can use a single Dedicated policy and apply to the files of each virtual machine.

Keep the number of VHD/VHDx files assigned to a single Aggregated policy to 20 or less. This policy type was meant to do aggregation with a few VMs on a cluster.

**Create and apply a Dedicated policy**

First, use the `New-StorageQosPolicy` cmdlet to create a policy on the Scale-Out File Server as shown in the following example:

```
$desktopVmPolicy = New-StorageQosPolicy -Name Desktop -PolicyType Dedicated -MinimumIops 100 -MaximumIops 200
```

Next, apply it to the appropriate virtual machines' hard disk drives on the Hyper-V server. Note the PolicyId from the previous step or store it in a variable in your scripts.

On the Scale-Out File Server, using PowerShell, create a Storage QoS policy and get its Policy ID as shown in the following example:

```
PS C:\> $desktopVmPolicy = New-StorageQosPolicy -Name Desktop -PolicyType Dedicated -MinimumIops 100 -
MaximumIops 200

C:\> $desktopVmPolicy.PolicyId

Guid
----
cd6e6b87-fb13-492b-9103-41c6f631f8e0
```

On the Hyper-V server, using PowerShell, set the Storage QoS Policy using the Policy ID as shown in the following example:

```
Get-VM -Name Build* | Get-VMHardDiskDrive | Set-VMHardDiskDrive -QoSPolicyID cd6e6b87-fb13-492b-9103-
41c6f631f8e0
```

**Confirm that the policies are applied**

Use `Get-StorageQosFlow` PowerShell cmdlet to confirm that the MinimumIOPs and MaximumIOPs have been applied to the appropriate flows as shown in the following example.

```
PS C:\> Get-StorageQoSflow | Sort-Object InitiatorName |
 ft InitiatorName, Status, MinimumIOPs, MaximumIOPs, StorageNodeIOPs, Status, @{Expression=
{$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -AutoSize

InitiatorName Status MinimumIops MaximumIops StorageNodeIOPs Status File
------------- ------ ----------- ----------- -------------- ------ ----
BuildVM1          Ok         100         200            250     Ok BUILDVM1.VHDX
BuildVM2          Ok         100         200            251     Ok BUILDVM2.VHDX
BuildVM3          Ok         100         200            252     Ok BUILDVM3.VHDX
BuildVM4          Ok         100         200            233     Ok BUILDVM4.VHDX
TR20-VMM          Ok          33         666              1     Ok DATA2.VHDX
TR20-VMM          Ok          33         666              5     Ok DATA1.VHDX
TR20-VMM          Ok          33         666              4     Ok BOOT.VHDX
WinOltp1          Ok           0           0              0     Ok 9914.0.AMD6...
WinOltp1          Ok           0           0           5166     Ok IOMETER.VHDX
WinOltp1          Ok           0           0              0     Ok BOOT.VHDX
```

On the Hyper-V server, you can also use the provided script **Get-VMHardDiskDrivePolicy.ps1** to see what policy is applied to a virtual hard disk drive.

```
PS C:\> Get-VM -Name BuildVM1 | Get-VMHardDiskDrive | Format-List

Path                          : \\plang-fs.plang.nttest.microsoft.com\two\BuildWorkload
                                \BuildVM1.vhdx
DiskNumber                    :
MaximumIOPS                   : 0
MinimumIOPS                   : 0
QoSPolicyID                   : cd6e6b87-fb13-492b-9103-41c6f631f8e0
SupportPersistentReservations : False
ControllerLocation            : 0
ControllerNumber              : 0
ControllerType                : IDE
PoolName                      : Primordial
Name                          : Hard Drive
Id                            : Microsoft:AE4E3DD0-3BDE-42EF-B035-9064309E6FEC\83F8638B
                                -8DCA-4152-9EDA-2CA8B33039B4\0\0\D
VMId                          : ae4e3dd0-3bde-42ef-b035-9064309e6fec
VMName                        : BuildVM1
VMSnapshotId                  : 00000000-0000-0000-0000-000000000000
VMSnapshotName                :
ComputerName                  : PLANG-C2
IsDeleted                     : False
```

### Query for Storage QoS Policies

`Get-StorageQosPolicy` lists all configured policies and their status on a Scale-Out File Server.

```
PS C:\> Get-StorageQosPolicy

Name                 MinimumIops          MaximumIops          Status
----                 -----------          -----------          ------
Default              0                    0                    Ok
Limit500             0                    500                  Ok
SilverVm             500                  500                  Ok
Desktop              100                  200                  Ok
Limit500             0                    0                    Ok
VMM                  100                  2000                 Ok
Vdi                  1                    100                  Ok
```

Status can change over time based on how the system is performing.

- **Ok** - All flows using that policy are receiving their requested MinimumIOPs.

- **InsufficientThroughput** - One or more of the flows using this policy are not receiving the Minimum IOPs

You can also pipe a policy to `Get-StorageQosPolicy` to get the status of all flows configured to use the policy as follows:

```
PS C:\> Get-StorageQosPolicy -Name Desktop | Get-StorageQosFlow | ft InitiatorName, *IOPS, Status, FilePath -
AutoSize

InitiatorName MaximumIops MinimumIops InitiatorIOPS StorageNodeIOPS Status FilePat
                                                                          h
------------- ----------- ----------- ------------- --------------- ------ -------
BuildVM4              100          50           187              17     Ok C:\C...
BuildVM3              100          50           194              25     Ok C:\C...
BuildVM1              200         100           195             196     Ok C:\C...
BuildVM2              200         100           193             192     Ok C:\C...
BuildVM4              200         100           187             169     Ok C:\C...
BuildVM3              200         100           194             169     Ok C:\C...
```

**Create an Aggregated Policy**

Aggregated policies may be used if you want multiple virtual hard disks to share a single pool of IOPs and bandwidth. For example, if you apply the same Aggregated policy to hard disks from two virtual machines, the minimum will be split between them according to demand. Both disks will be guaranteed a combined minimum, and together they will not exceed the specified maximum IOPs or bandwidth.

The same approach could also be used to provide a single allocation to all VHD/VHDx files for the virtual machines comprising a service or belonging to a tenant in a multihosted environment.

There is no difference in the process to create Dedicated and Aggregated policies other than the PolicyType that is specified.

The following example shows how to create an Aggregated Storage QoS Policy and get its policyID on a Scale-Out File Server:

```
PS C:\> $highPerf = New-StorageQosPolicy -Name SqlWorkload -MinimumIops 1000 -MaximumIops 5000 -PolicyType
Aggregated
[plang-fs]: PS C:\Users\plang\Documents> $highPerf.PolicyId

Guid
----
7e2f3e73-1ae4-4710-8219-0769a4aba072
```

The following example shows how to apply the Storage QoS Policy on Hyper-V server using the policyID obtained in the preceding example:

```
PS C:\> Get-VM -Name WinOltp1 | Get-VMHardDiskDrive | Set-VMHardDiskDrive -QoSPolicyID 7e2f3e73-1ae4-4710-
8219-0769a4aba072
```

The following example shows how to viewing effects of the Storage QoS policy from file server:

```
PS C:\> Get-StorageQosFlow -InitiatorName WinOltp1 | format-list InitiatorName, PolicyId, MinimumIOPs,
MaximumIOPs, StorageNodeIOPs, FilePath

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 250
MaximumIops     : 1250
StorageNodeIOPs : 0
FilePath        : C:\ClusterStorage\Volume2\SHARES\TWO\BASEVHD\9914.0.AMD64FRE.WIN
                  MAIN.141218-1718_SERVER_SERVERDATACENTER_EN-US.VHDX

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 250
MaximumIops     : 1250
StorageNodeIOPs : 0
FilePath        : C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\BOOT.VHDX

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 1000
MaximumIops     : 5000
StorageNodeIOPs : 4550
FilePath        : C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\IOMETER.VHDX
PS C:\> Get-StorageQosFlow -InitiatorName WinOltp1 | for
mat-list InitiatorName, PolicyId, MinimumIOPs, MaximumIOPs, StorageNodeIOPs, FilePath

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 250
MaximumIops     : 1250
StorageNodeIOPs : 0
FilePath        : C:\ClusterStorage\Volume2\SHARES\TWO\BASEVHD\9914.0.AMD64FRE.WIN
                  MAIN.141218-1718_SERVER_SERVERDATACENTER_EN-US.VHDX

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 250
MaximumIops     : 1250
StorageNodeIOPs : 0
FilePath        : C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\BOOT.VHDX

InitiatorName   : WinOltp1
PolicyId        : 7e2f3e73-1ae4-4710-8219-0769a4aba072
MinimumIops     : 1000
MaximumIops     : 5000
StorageNodeIOPs : 4550
FilePath        : C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\IOMETER.VHDX
```

Each virtual hard disk will have the MinimumIOPs and MaximumIOPs and MaximumIobandwidth value adjusted based on its load. This ensures that the total amount of bandwidth used for the group of disks stays within the range defined by policy. In the example above, the first two disks are idle, and the third one is allowed to use up to the maximum IOPs. If the first two disks start issuing IO again, then the maximum IOPs of the third disk will be lowered automatically.

**Modify an existing policy**

The properties of Name, MinimumIOPs, MaximumIOPs, and MaximumIoBandwidthcan be changed after a policy is created. However, the Policy Type (Aggregated/Dedicated) cannot be changed once the policy is created.

The following Windows PowerShell cmdlet shows how to change the MaximumIOPs property for an existing policy:

```
[DBG]: PS C:\democripts>> Get-StorageQosPolicy -Name SqlWorkload | Set-StorageQosPolicy -MaximumIops 6000
```

The following cmdlet verifies the change:

```
PS C:\> Get-StorageQosPolicy -Name SqlWorkload

Name                    MinimumIops            MaximumIops            Status
----                    -----------            -----------            ------
SqlWorkload             1000                   6000                   Ok

[plang-fs1]: PS C:\Users\plang\Documents> Get-StorageQosPolicy -Name SqlWorkload | Get-Storag
eQosFlow | Format-Table InitiatorName, PolicyId, MaximumIops, MinimumIops, StorageNodeIops -A
utoSize

InitiatorName PolicyId                              MaximumIops MinimumIops StorageNodeIops
------------- --------                              ----------- ----------- ---------------
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072        1500         250               0
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072        1500         250               0
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072        6000        1000            4507
```

# How to identify and address common issues

This section describes how to find virtual machines with invalid Storage QoS policies, how to recreate a matching policy, how to remove a policy from a virtual machine, and how to identify virtual machines that do not meet the Storage QoS policy requirements.

#### Identify virtual machines with invalid policies

If a policy is deleted from the file server before it's removed from a virtual machine, the virtual machine will keep running as if no policy were applied.

```
PS C:\> Get-StorageQosPolicy -Name SqlWorkload | Remove-StorageQosPolicy

Confirm
Are you sure you want to perform this action?
Performing the operation "DeletePolicy" on target "MSFT_StorageQoSPolicy (PolicyId =
"7e2f3e73-1ae4-4710-8219-0769a4aba072")".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"):
```

The status for the flows will now show "UnknownPolicyId"

```
PS C:\> Get-StorageQoSflow | Sort-Object InitiatorName | ft InitiatorName, Status, MinimumIOPs, MaximumIOPs,
StorageNodeIOPs, Status, @{Expression={$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -
AutoSize

InitiatorName          Status MinimumIops MaximumIops StorageNodeIOPs          Status File
-------------          ------ ----------- ----------- ---------------          ------ ----
                           Ok           0           0               0              Ok Def...
                           Ok           0           0              10              Ok Def...
                           Ok           0           0              13              Ok Def...
                           Ok           0           0               0              Ok Def...
                           Ok           0           0               0              Ok Def...
                           Ok           0           0               0              Ok Def...
                           Ok           0           0               0              Ok Def...
                           Ok           0           0               0              Ok Def...
                           Ok           0           0               0              Ok Def...
BuildVM1                   Ok         100         200             193              Ok BUI...
BuildVM2                   Ok         100         200             196              Ok BUI...
BuildVM3                   Ok          50          64              17              Ok WIN...
BuildVM3                   Ok          50         136             179              Ok BUI...
BuildVM4                   Ok          50         100              23              Ok WIN...
BuildVM4                   Ok         100         200             173              Ok BUI...
TR20-VMM                   Ok          33         666               2              Ok DAT...
TR20-VMM                   Ok          25         975               3              Ok DAT...
TR20-VMM                   Ok          75        1025              12              Ok BOO...
WinOltp1      UnknownPolicyId           0           0               0 UnknownPolicyId 991...
WinOltp1      UnknownPolicyId           0           0            4926 UnknownPolicyId IOM...
WinOltp1      UnknownPolicyId           0           0               0 UnknownPolicyId BOO...
```

**Recreate a matching Storage QoS policy**

If a policy was unintentionally removed, you can create a new one using the old PolicyId. First, get the needed PolicyId

```
PS C:\> Get-StorageQosFlow -Status UnknownPolicyId | ft InitiatorName, PolicyId -AutoSize

InitiatorName PolicyId
------------- --------
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072
WinOltp1      7e2f3e73-1ae4-4710-8219-0769a4aba072
```

Next, create a new policy using that PolicyId

```
PS C:\> New-StorageQosPolicy -PolicyId 7e2f3e73-1ae4-4710-8219-0769a4aba072 -PolicyType Aggregated -Name
RestoredPolicy -MinimumIops 100 -MaximumIops 2000

Name                   MinimumIops            MaximumIops            Status
----                   -----------            -----------            ------
RestoredPolicy         100                    2000                   Ok
```

Finally, verify that it was applied.

```
PS C:\> Get-StorageQoSflow | Sort-Object InitiatorName | ft InitiatorName, Status, MinimumIOPs, MaximumIOPs,
StorageNodeIOPs, Status, @{Expression={$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -
AutoSize

InitiatorName Status MinimumIops MaximumIops StorageNodeIOPs Status File
------------- ------ ----------- ----------- --------------- ------ ----
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               8     Ok DefaultFlow
                 Ok           0           0               9     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
                 Ok           0           0               0     Ok DefaultFlow
BuildVM1         Ok         100         200             192     Ok BUILDVM1.VHDX
BuildVM2         Ok         100         200             193     Ok BUILDVM2.VHDX
BuildVM3         Ok          50         100              24     Ok WIN8RTM_ENTERPRISE_VL...
BuildVM3         Ok         100         200             166     Ok BUILDVM3.VHDX
BuildVM4         Ok          50         100              12     Ok WIN8RTM_ENTERPRISE_VL...
BuildVM4         Ok         100         200             178     Ok BUILDVM4.VHDX
TR20-VMM         Ok          33         666               2     Ok DATA2.VHDX
TR20-VMM         Ok          33         666               2     Ok DATA1.VHDX
TR20-VMM         Ok          33         666              10     Ok BOOT.VHDX
WinOltp1         Ok          25         500               0     Ok 9914.0.AMD64FRE.WINMA...
```

**Remove Storage QoS Policies**

If the policy was removed intentionally, or if a VM was imported with a policy that you don't need, it may be removed.

```
PS C:\> Get-VM -Name WinOltp1 | Get-VMHardDiskDrive | Set-VMHardDiskDrive -QoSPolicyID $null
```

Once the PolicyId is removed from the virtual hard disk settings, the status will be "Ok" and no minimum or maximum will be applied.

```
PS C:\> Get-StorageQoSflow | Sort-Object InitiatorName | ft InitiatorName, MinimumIOPs, MaximumIOPs,
StorageNodeIOPs, Status, @{Expression={$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -
AutoSize

InitiatorName MinimumIops MaximumIops StorageNodeIOPs Status File
------------- ----------- ----------- --------------- ------ ----
                        0           0               0     Ok DefaultFlow
                        0           0              16     Ok DefaultFlow
                        0           0              12     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
                        0           0               0     Ok DefaultFlow
BuildVM1              100         200             197     Ok BUILDVM1.VHDX
BuildVM2              100         200             192     Ok BUILDVM2.VHDX
BuildVM3                9           9              23     Ok WIN8RTM_ENTERPRISE_VL_BUILDW...
BuildVM3               91         191             171     Ok BUILDVM3.VHDX
BuildVM4                8           8              18     Ok WIN8RTM_ENTERPRISE_VL_BUILDW...
BuildVM4               92         192             163     Ok BUILDVM4.VHDX
TR20-VMM               33         666               2     Ok DATA2.VHDX
TR20-VMM               33         666               1     Ok DATA1.VHDX
TR20-VMM               33         666               5     Ok BOOT.VHDX
WinOltp1                0           0               0     Ok 9914.0.AMD64FRE.WINMAIN.1412...
WinOltp1                0           0            1811     Ok IOMETER.VHDX
WinOltp1                0           0               0     Ok BOOT.VHDX
```

**Find virtual machines that are not meeting Storage QoS Policies**

The **InsufficientThroughput** status is assigned to any flows that:

- Have a minimum defined IOPs set by policy; and
- Are initiating IO at a rate meeting or exceeding the minimum; and
- Are not achieving minimum IOP rate

```
PS C:\> Get-StorageQoSflow | Sort-Object InitiatorName | ft InitiatorName, MinimumIOPs, MaximumIOPs,
StorageNodeIOPs, Status, @{Expression={$_.FilePath.Substring($_.FilePath.LastIndexOf('\')+1)};Label="File"} -
AutoSize

InitiatorName MinimumIops MaximumIops StorageNodeIOPs                Status File
------------- ----------- ----------- ---------------                ------ ----
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0              15                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
                        0           0               0                    Ok DefaultFlow
BuildVM3               50         100              20                    Ok WIN8RTM_ENTE...
BuildVM3              100         200             174                    Ok BUILDVM3.VHDX
BuildVM4               50         100              11                    Ok WIN8RTM_ENTE...
BuildVM4              100         200             188                    Ok BUILDVM4.VHDX
TR20-VMM               33         666               3                    Ok DATA1.VHDX
TR20-VMM               78        1032             180                    Ok BOOT.VHDX
TR20-VMM               22         968               4                    Ok DATA2.VHDX
WinOltp1             3750        5000               0                    Ok 9914.0.AMD64...
WinOltp1            15000       20000           11679 InsufficientThroughput IOMETER.VHDX
WinOltp1             3750        5000               0                    Ok BOOT.VHDX
```

You can determine flows for any status, including **InsufficientThroughput** as shown in the following example:

```
PS C:\> Get-StorageQosFlow -Status InsufficientThroughput | fl

FilePath           : C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\IOMETER.VHDX
FlowId             : 1ca356ff-fd33-5b5d-b60a-2c8659dc803e
InitiatorId        : 2ceabcef-2eba-4f1b-9e66-10f960b50bbf
InitiatorIOPS      : 12168
InitiatorLatency   : 22.983
InitiatorName      : WinOltp1
InitiatorNodeName  : plang-c1.plang.nttest.microsoft.com
Interval           : 300000
Limit              : 20000
PolicyId           : 5d1bf221-c8f0-4368-abcf-aa139e8a7c72
Reservation        : 15000
Status             : InsufficientThroughput
StorageNodeIOPS    : 12181
StorageNodeLatency : 22.0514
StorageNodeName    : plang-fs2.plang.nttest.microsoft.com
TimeStamp          : 2/13/2015 12:07:30 PM
VolumeId           : 0d2fd367-8d74-4146-9934-306726913dda
PSComputerName     :
MaximumIops        : 20000
MinimumIops        : 15000
```

# Monitor Health using Storage QoS

The new Health Service simplifies the monitoring of the Storage Cluster, providing a single place to check for any

actionable events in any of the nodes. This section describes how monitor the health of your storage cluster using the `debug-storagesubsystem` cmdlet.

### View Storage Status with Debug-StorageSubSystem

Clustered Storage Spaces also provide information on the health of the storage cluster in a single location. This can help administrators quickly identify current problems in storage deployments and monitor as issues arrive or are dismissed.

#### VM with invalid policy

VMs with invalid policies are also reported through the storage subsystem health monitoring. Here is an example from the same state as described in Finding VMs with invalid policies section of this document.

```
C:\> Get-StorageSubSystem -FriendlyName Clustered* | Debug-StorageSubSystem

EventTime                :
FaultId                  : 0d16d034-9f15-4920-a305-f9852abf47c3
FaultingObject           :
FaultingObjectDescription : Storage QoS Policy 5d1bf221-c8f0-4368-abcf-aa139e8a7c72
FaultingObjectLocation   :
FaultType                : Storage QoS policy used by consumer does not exist.
PerceivedSeverity        : Minor
Reason                   : One or more storage consumers (usually Virtual Machines) are
                           using a non-existent policy with id
                           5d1bf221-c8f0-4368-abcf-aa139e8a7c72. Consumer details:

                           Flow ID: 1ca356ff-fd33-5b5d-b60a-2c8659dc803e
                           Initiator ID: 2ceabcef-2eba-4f1b-9e66-10f960b50bbf
                           Initiator Name: WinOltp1
                           Initiator Node: plang-c1.plang.nttest.microsoft.com
                           File Path:
                           C:\ClusterStorage\Volume3\SHARES\THREE\WINOLTP1\IOMETER.VHDX
RecommendedActions       : {Reconfigure the storage consumers (usually Virtual Machines)
                           to use a valid policy., Recreate any missing Storage QoS
                           policies.}
PSComputerName           :
```

#### Lost redundancy for a storage spaces virtual disk

In this example, a Clustered Storage Space has a virtual disk created as a three-way mirror. A failed disk was removed from the system, but a replacement disk was not added. The storage subsystem is reporting a loss of redundancy with HealthStatus **Warning**, but OperationalStatus "**OK** because the volume is still online.

```
PS C:\> Get-StorageSubSystem -FriendlyName Clustered*

FriendlyName                   HealthStatus                   OperationalStatus
------------                   ------------                   -----------------
Clustered Windows Storage o... Warning                        OK

[plang-fs1]: PS C:\Users\plang\Documents> Get-StorageSubSystem -FriendlyName Clustered* | Deb
ug-StorageSubSystem

EventTime                :
FaultId                  : dfb4b672-22a6-4229-b2ed-c29d7485bede
FaultingObject           :
FaultingObjectDescription : Virtual disk 'Two'
FaultingObjectLocation   :
FaultType                : VirtualDiskDegradedFaultType
PerceivedSeverity        : Minor
Reason                   : Virtual disk 'Two' does not have enough redundancy remaining to
                           successfully repair or regenerate its data.
RecommendedActions       : {Rebalance the pool, replace failed physical disks, or add new
                           physical disks to the storage pool, then repair the virtual
                           disk.}
PSComputerName           :
```

**Sample script for continuous monitoring of Storage QoS**

This section includes a sample script showing how common failures can be monitored using WMI script. It's designed as a starting part for developers to retrieve health events in real time.

Example script:

```
param($cimSession)
# Register and display events
Register-CimIndicationEvent -Namespace root\microsoft\windows\storage -ClassName msft_storagefaultevent -
CimSession $cimSession

while ($true)
{
     $e = (Wait-Event)
     $e.SourceEventArgs.NewEvent
     Remove-Event $e.SourceIdentifier
}
```

# Frequently Asked Questions

**How do I retain a Storage QoS policy being enforced for my virtual machine if I move its VHD/VHDx files to another storage cluster**

The setting on the VHD/VHDx file that specifies the policy is the GUID of a policy ID. When a policy is created, the GUID can be specified using the **PolicyID** parameter. If that parameter is not specified, a random GUID is created. Therefore, you can get the PolicyID on the storage cluster where the VMs currently store their VHD/VHDx files and create an identical policy on the destination storage cluster and then specify that it be created with the same GUID. When the VMs files are moved to the new storage clusters, the policy with the same GUID will be in effect.

System Center Virtual Machine Manager can be used to apply policies across multiple storage clusters, which makes this scenario much easier.

**If I change the Storage QoS Policy, why don't I see it take effect immediately when I run Get-StorageQoSFlow**

If you have a flow that is hitting a maximum of a policy and you change the policy to either make it higher or lower, and then you immediately determine the latency/IOPS/BandWidth of the flows using the PowerShell cmdlets, it will take up to 5 minutes to see the full effects of the policy change on the flows. The new limits will be in effect within a few seconds, but the **Get-StorgeQoSFlow** PowerShell cmdlet uses an average of each counter

using a 5 minute sliding window. Otherwise, if it was showing a current value and you ran the PowerShell cmdlet multiple times in a row, you may see vastly different values because values for IOPS and latencies can fluctuate significantly from one second to another.

**What new functionality was added in Windows Server 2016**

In Windows Server 2016 the Storage QoS Policy type names were renamed. The **Multi-instance** policy type is renamed as **Dedicated** and **Single-instance** was renamed as **Aggregated**. The management behavior of Dedicated policies is also modified - VHD/VHDX files within the same virtual machine that have the same **Dedicated** policy applied to them will not share I/O allocations.

There are two new Storage QoS features Windows Server 2016:

- **Maximum Bandwidth**

  Storage QoS in Windows Server 2016 introduces the ability to specify the maximum bandwidth that the flows assigned to the policy may consume. The parameter when specifying it in the **StorageQosPolicy** cmdlets is **MaximumIOBandwidth** and the output is expressed in bytes per second. If both **Maximimlops** and **MaximumIOBandwidth** are set in a policy, they will both be in effect and the first one to be reached by the flow(s) will limit the I/O of the flows.

- **IOPS normalization is configurable**

  Storage QoSin uses normalization of IOPS. The default is to use a normalization size of 8K. Storage QoS in Windows Server 2016 introduces the ability to specify a different normalization size for the storage cluster. This normalization size effects all flows on the storage cluster and takes effect immediately (within a few seconds) once it is changed. The minimum is 1KB and the maximum is 4GB (recommend not setting more than 4MB since it's unusual to have more than 4MB IOs).

  Something to consider is that the same IO pattern/throughput shows up with different IOPS numbers in the Storage QoS output when you change the IOPS normalization due to the change in normalization calculation. If you are comparing IOPS between storage clusters, you may also want to verify what normalization value each is using since that will effect the normalized IOPS reported.

**Example 1: Creating a new policy and viewing the maximum bandwidth on the storage cluster**

In PowerShell, you can specify the units that a number is expressed in. In the following example, 10MB is used as the maximum bandwidth value. Storage QoS will convert this and save it as bytes per second Hence, 10MB is converted into 10485760 bytes per second.

```
PS C:\Windows\system32> New-StorageQosPolicy -Name HR_VMs -MaximumIops 1000 -MinimumIops 20 -
MaximumIOBandwidth 10MB

Name   MinimumIops MaximumIops MaximumIOBandwidth Status
----   ----------- ----------- ------------------ ------
HR_VMs 20          1000        10485760           Ok

PS C:\Windows\system32> Get-StorageQosPolicy

Name    MinimumIops MaximumIops MaximumIOBandwidth Status
----    ----------- ----------- ------------------ ------
Default 0           0           0                  Ok
HR_VMs  20          1000        10485760           Ok

PS C:\Windows\system32> Get-StorageQoSFlow | fL
InitiatorName,FilePath,InitiatorIOPS,InitiatorLatency,InitiatorBandwidth

InitiatorName      : testsQoS
FilePath           : C:\ClusterStorage\Volume2\TESTSQOS\VIRTUAL HARD DISKS\TESTSQOS.VHDX
InitiatorIOPS      : 5
InitiatorLatency   : 1.5455
InitiatorBandwidth : 37888
```

**Example 2: Get IOPS normalization settings and specify a new value**

The following example demonstrates how to get the storage clusters IOPS normalization settings (default of 8KB), then set it to 32KB, and then show it again. Note, in this example, specify "32KB", since PowerShell allows specifying the unit instead of requiring the conversion to bytes. The output does show the value in bytes per second.

```
PS C:\Windows\system32> Get-StorageQosPolicyStore

IOPSNormalizationSize
---------------------
8192

PS C:\Windows\system32> Set-StorageQosPolicyStore -IOPSNormalizationSize 32KB
PS C:\Windows\system32> Get-StorageQosPolicyStore

IOPSNormalizationSize
---------------------
32768
```

## See Also

- Windows Server 2016
- Storage Replica in Windows Server 2016
- Storage Spaces Direct in Windows Server 2016

# Change history for storage topics in Windows Server

11/2/2020 • 7 minutes to read • Edit Online

Applies to: Windows Server 2019, Windows Server 2016, Windows Server (Semi-Annual Channel)

This topic lists new and updated topics in the Storage documentation for Windows Server.

If you're looking for update history for Windows Server, see Windows 10 and Windows Server 2019 update history or Windows Server 2016 update history.

## January 2020

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Understand and deploy persistent memory | Added known hardware issue. |

## December 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Troubleshooting Disk Management | Edited to further refine the guidance, based on customer requests. |
| Extend a volume in Disk Management | Added guidance in response to customer feedback. |
| Change a dynamic disk back to a basic disk | Fixed an error in the command line and added some info based on customer feedback. |

## August 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Storage Migration Service FAQ | Updated to reflect new support for Linux sources. |

## June 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Disk cleanup | New (Migrated from the Previous Versions) |
| Storage Migration Service FAQ | Added performance optimization info. |

## May 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Delete volumes | New |
| Create volumes | Added steps and videos for creating a volume in Windows Admin Center. |
| Extend volumes | Added steps and video for resizing a volume in Windows Admin Center. |

## March 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Monitor with Azure Monitor | New |
| Understand and deploy persistent memory | New |
| Upgrade a Storage Spaces Direct cluster to Windows Server 2019 | New |
| DFS Replication | Migrated from the Previous Versions library |

## February 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Storage Migration Service known issues | Added an issue |

## January 2019

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Understand and monitor storage resync | New topic |

## December 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Use Storage Migration Service to migrate a server | Added some clarification on how we transfer files |
| Cluster to Cluster Storage Replica cross region in Azure | Added validation steps |
| Cluster to Cluster Storage Replica within the same region in Azure | Added validation steps |
| Storage Replica frequently asked questions | Added support statement for Data Deduplication |

## November 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Nested resiliency | New topic |
| Storage Migration Service known issues | New topic |
| DFS Replication: Frequently Asked Questions (FAQ) | Migrated from the Previous Versions library |
| Migrate SYSVOL replication to DFS Replication | Migrated from the Previous Versions library |
| SMB: File and printer sharing ports should be open | Migrated from the Previous Versions library |
| Volume Shadow Copy Service | Migrated from the Previous Versions library |

## October 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| What's new in Storage | Updated to cover what's new in Windows Server 2019 |
| Storage Replica known issues | Added info about a new update. |

## September 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Storage Migration Service overview | New topic |
| Use Storage Migration Service to migrate a server | New topic |
| Storage Migration Service frequently asked questions (FAQ) | New topic |
| iSCSI Target Server | Migrated from the Previous Versions library. |
| iSCSI Target Server scalability limits | Migrated from the Previous Versions library. |

## June 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Server-to-server storage replication | Added info on using Azure VMs, including ExpressRoute. |
| Cluster sets | New topic |

## May 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| NFS overview | Migrated from the Previous Versions library. |

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Deploy NFS | Migrated from the Previous Versions library. |
| Deploy Storage Spaces on a stand-alone server | Migrated from the Previous Versions library. |
| NTFS Overview | Migrated from the Previous Versions library. |
| Use Robocopy to Preseed Files for DFS Replication | Migrated from the Previous Versions library. |
| Vssadmin - Previous Versions command line tool | Migrated from the Previous Versions library. |
| File Server Resource Manager overview | Added info about a new registry setting in Windows Server 2016, version 1803. |
| Server-to-server storage replication | Added info on using Windows Admin Center. |
| Storage Replica known issues | Added new information. |

## April 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Collect data in Storage Spaces Direct | New topic. |
| Storage Spaces overview | New topic. |
| Folder Redirection, Offline Files, and Roaming User Profiles overview | Migrated multiple topics from the Previous Versions library. |
| File sharing using the SMB 3 protocol | Migrated from the Previous Versions library. |
| Improve performance of a file server with SMB Direct | Migrated from the Previous Versions library. |
| SMB security enhancements | Migrated from the Previous Versions library. |

## March 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Disaster recovery with Storage Spaces Direct | New topic. |
| Understanding Quorum in Storage Spaces Direct | New topic. |
| Deploying Storage Spaces Direct | Heavily revised to include both converged and hyper-converged scenarios. |
| Deploying Roaming User Profiles | Moved from Previous Versions library and updated. |
| Storage Replica frequently asked questions | Added Is CSV required to replicate in a stretch cluster or between clusters?. |

## February 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Storage Spaces health and operational states | New topic. |
| Using Storage Spaces Direct with the CSV in-memory read cache | New topic. |

## January 2018

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Drive symmetry considerations in Storage Spaces Direct | New topic. |
| Using Storage Replica with Project Honolulu | New topic. |

## December 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Change a drive letter | New topic. |
| Troubleshooting Disk Management | Rewrote the A disk's status is Not Initialized or the disk is missing entirely section to add extensive troubleshooting steps, based on customer requests. |
| Initialize new disks | Rewrote to attempt to make it easier to understand and address customer questions. |
| Planning volumes in Storage Spaces Direct | Added a table summarizing the resiliency types available on four-node and larger clusters. |
| ReFS overview | Clarified recommended workloads for mirror-accelerated parity and corrected the supported file and volume sizes for ReFS and NTFS. |
| Mirror-accelerated parity | Clarified recommendation to place write-heavy files in separate directories. |
| Storage Replica known issues | Added new information. |

## November 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| What's new in storage | Added info about what's new in Windows Server, version 1709. |
| Add servers or drives | Added information about how Storage Spaces Direct automatically optimizes drive usage after adding drives. |

## October 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Deploying Storage Spaces Direct in a virtual machine guest cluster | New topic. |
| Overview of Disk Management | Published 13 new topics for Windows and Windows Server. |
| Storage Replica overview | Added what's new info for Windows Server, version 1709. |
| Storage Replica known issues | Added new information. |
| Cluster to cluster storage replication | Revised the number of supported cluster nodes for Storage Spaces Direct. |
| Storage Spaces Direct hardware requirements | Added a note about a specific line of NVMe devices. |

## July 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| DFS Namespaces | Published 20 new topics for Windows Server 2016. |
| File Server Resource Manager | Published 33 new topics for Windows Server 2016. |
| Understanding the cache in Storage Spaces Direct | Added a Storage Spaces Direct design considerations video. |
| Storage Replica frequently asked questions | Added more best practices around log volumes. |

## June 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Planning a Work Folders deployment | Added info about Azure AD Application Proxy support & updated requirements. |
| Work Folders | Added info about Azure AD Application Proxy support & updated requirements. |
| Deploying Storage Spaces Direct | Removed Nano Server from supported installation options. |
| File Server Resource Manager | New topic for Windows Server 2016. |

## May 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Data Deduplication overview and Install Data Deduplication | Updated the system requirements to include a newer software update. |

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Deploying Work Folders | Added info about Azure AD Application Proxy support & updated required steps. |
| Deploying Storage Spaces Direct | Added step 1.3 with required features and fixed an obsolete parameter in Enable-NetAdapterQos. |
| Storage Replica frequently asked questions | Added info on how to choose between different replication topologies. |
| Storage Spaces Direct hardware requirements | Changed drive endurance requirements for cache devices. |

## April 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Troubleshooting drive firmware updates | New topic. |
| Work Folders | New topic. |
| Planning a Work Folders deployment | New topic. |
| Deploying Work Folders | New topic. |
| Deploying Work Folders with AD FS and Web Application Proxy (WAP) | New topic. |
| Deploying Storage Spaces Direct | Removed a reference to an obsolete software update and fixed a typo in the sample output. |
| Storage Replica known issues | Added new information. |

## March 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Taking a Storage Spaces Direct server offline for maintenance | New topic. |

## February 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Removing servers in Storage Spaces Direct | New topic. |
| Adding server or drives to Storage Spaces Direct | Revamped with new images and updated content. |
| Storage Spaces Direct hardware requirements | Updated with latest requirements. |

## January 2017

| NEW OR CHANGED TOPIC | DESCRIPTION |
| --- | --- |
| Planning volumes | New topic. |
| Creating volumes | New topic. |
| Extending volumes in Storage Spaces Direct | New topic. |
| ReFS Overview | New topic. |
| Understanding Storage Spaces Direct | New list of links. |
| Planning Storage Spaces Direct | New list of links. |
| Deploying Storage Spaces Direct | New list of links. |
| Managing Storage Spaces Direct | New topic. |
| Storage Replica frequently asked questions | Updated port requirements and clarified how extending replicated volumes works. |
| Storage Replica known issues | Added info about a fix in the December 9, 2016 Cumulative Update and added info about how to resolve an error when extending a replicated volume. |
| Storage Spaces Direct overview | Added visually-oriented Understand/Plan/Deploy/Manage section to serve as a learning map for our topics. |
| Deploying Storage Spaces Direct | Removed some obsolete content and added new links. |