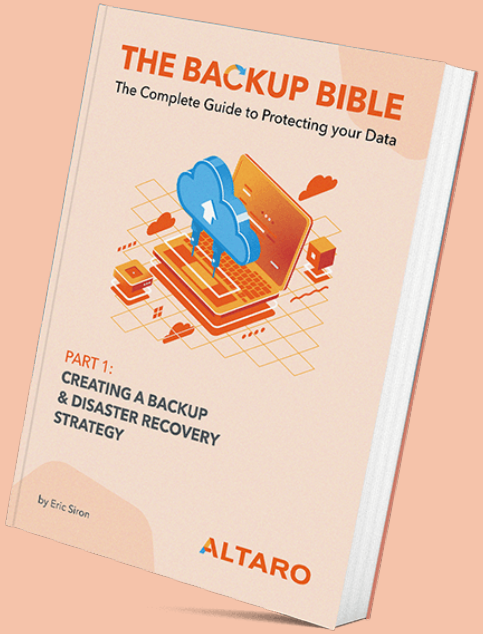
BACKUP BEST PRACTICES
IN ACTION

THE BACKUP BIBLE
The Complete Guide to Protecting your Data

by Eric Siron

ALTARO

This eBook is intended to follow on from Part 1 of the BACKUP BIBLE SERIES:



If you have yet to read that, it might be worth having a look at what you missed. Some sections here will assume knowledge taught there.

Grab your free copy here.

CONTENTS

Introduction 5
- Who Should Read This Book 6
- Terms Used in this Book 6
- Altaro Backup Solutions 7

Putting Your Backup Strategy Into Action 8

Choosing the Right Backup and Recovery Software 10
- Backup Application Features 11
- Trial and Free Software Offerings – What to Look for 12
- Placement of Backup Software 13
- Consistency and Application-Awareness 14
- Hypervisor-Aware Backup Software 15
- Standard Physical Systems Backup Software 15
- Single-Vendor vs. Hybrid Application Solutions 16
- Putting It in Action 17
  - Phase One: Candidate Software Selection 17
  - Phase Two: In-Depth Software Testing 17
  - Phase Three: Final Selection 18

Backup Storage Targets 19
- Magnetic Tape in Backup Solutions 20
- Optical Media in Backup Solutions 21

ALTARO BACKUP

Direct-Attached Storage and Mass Media Devices in Backup Solutions....23
Networked Storage in Backup Solutions....24
Using Commodity Computing Equipment as Backup Storage....25
Cloud Storage in Backup Solutions....26
Putting It in Action....28
Steps to Performing Hardware Selection....28
Securing and Protecting Backup Data....30
Risk Analysis for Backup....31
Ransomware Risks to Backup....32
Security by Redundancy....32
The Role of Retention and Rotation Policies in Backup Security....32
Protecting Your Backups with Multiple Tiers....33
Using Account Control to Protect Your Backups....34
Encrypting Your Backup Data....34
Isolating Your Backup Systems....35
Shielding Backup Systems with Firewalls....35
Air-Gapping for Isolation....36
Caring for Offline Data....37
Putting it in Action....38
Risk Analysis Activities....38
Creating Backup Redundancy Policies....39
Establishing an Encryption Policy....39
Shielding Backup with Physical and Network Protections....40
Fully Isolating Backup Systems....41
Deploying Backup....43
Documenting Your Backup System....45
Documentation Procedures and Tools....46
Sample Backup Documentation for a Small Organization....47
Sample Backup Documentation for a Larger Organization....50
Defining Backup Schedules....55
Understanding How the Value of Data Affects Backup Scheduling....56
Understanding How the Frequency of Change Affects Backup Scheduling....56
Understanding How Backup Application Features Affect Scheduling....56
Putting it in Action....58
Grandfather-Father-Son Sample Plan....59
Online Media Sample Plan....59

Continuous Backup Sample Plan 60
Mixed Backup Plan Example 60
Monitoring and Testing Your Backups 62
Monitoring Your Backup System 63
Testing Backup Media and Data 63
Putting it in Action 64
Maintaining Your Systems 65
Putting it in Action 66
What's Next 67
Altaro Backup 68
More Great IT Content 69

INTRODUCTION

When tedium sets in, people make mistakes. Few things in the technology world can drain a person like a protracted implementation. Successful installation processes require a disciplined approach. You must allocate sufficient time, expect setbacks and interruptions, and regularly check your work. Creating a solid plan can help you to avoid the worst problems and reach operational status quickly.

In part one, we focused on creating an overall disaster recovery plan. In this eBook, we will put that plan into motion. By necessity, these two parts will have some overlap, primarily around acquiring equipment, software, and services. However, before beginning your implementation, verify that you have worked all the way through part one. Introducing significant changes during the rollout procedure will cause problems and delays.

The sections in this book start by discussing the related theory. After that, they move on to practice with a "Putting it in Action" sub-section. Do not skip ahead to the implementation portions until you fully understand the underlying concepts.

WHO SHOULD READ THIS BOOK

This book was written for individuals tasked with putting a disaster recovery plan into action. It will continue the first part's goal of using accessible, easy-to-understand language. However, due to the technical nature of the topics, some areas may present challenges. Therefore, readers with some Windows Server administration and backup application experience will have the easiest time with the material.

TERMS USED IN THIS BOOK

Part one of this series included a short list of common backup terms. This part expects you to have a functional understanding of all the same words:

1. **Backup:** A "cold" instance of duplicated data.
2. **Business continuity:** The ability of an organization to continue performing its desired activities and functions throughout an emergency situation.
3. **Disaster recovery:** The process of returning to full functionality after an emergency.
4. **Replica:** A "warm" or "hot" instance of duplicated data.

This book will not define any of these terms further. If you do not fully understand them, please read refer to part one.

ALTARO BACKUP SOLUTIONS

Altaro is an award-winning developer of a range of backup solutions including Hyper-V & VMware Backup and Replication, Office 365 Backup, Physical Server Backup and Endpoint Backup (coming soon). Altaro also offers an attractive Partner Program for VARs, resellers and IT consultants as well as dedicated programs for Managed Service Providers (MSPs). With 50,000+ customers in 121+ countries, 10,000 partners and 2,000+ MSPs, Altaro provides affordable enterprise-class functionality coupled with outstanding 24/7 support.

This eBook has been designed to cover the theory and practical exercise of backup and disaster recovery planning. It contains references to Altaro Backup solutions where relevant, but it is not specifically about Altaro or a guide to using Altaro products.
As such the information contained here is relevant to whichever backup software you choose to deploy

PUTTING YOUR BACKUP STRATEGY INTO ACTION

Part one ended with a gathering of the data necessary to design a disaster recovery strategy. Now, we transition to implementation. The connection point is usually when you have received the bulk of your hardware and software purchase and can put it to use. If you have not even submitted orders yet, that's no problem. If you already have everything, that's fine as well. You must design the architecture, which you might find easier to perform before you decide what to buy.

In simple terms, you must move from deciding what to protect on to deciding how to protect it. for some things, your organization might choose to use printed hard copies. Those survive power outages and need no technical expertise to use. You will need to find a way to adequately keep these items safe. Consider their risk from events such as fire, flood, and theft. If the contents of the documents are vital but not a risk to security, then perhaps creating and distributing multiple copies is the best answer. Technology may not help much for these types of problems.

To guard your digital information, you need three major things:

- Backup software
- Backup storage
- Security strategy

If you start by selecting your backup application, that can guide you toward the most appropriate hardware platform and security approach. You could also start with a physical storage system that you like, but this may restrict your options for software solutions.

In the past, companies rarely put much thought or effort into backup security. Soon, they learned – the hard way – that bad actors found enough value in data backups to steal them. That prompted the backup industry to introduce security features into their products. Later, ransomware authors began targeting backup applications to prevent them from saving victims' data.

In this second part of The Backup Bible, we will tackle all these concerns. You will learn how to architect and deploy a solution that enables the plan that you built in the first part. Individual sections will explore and expand on the ideas presented above.

CHOOSING THE RIGHT BACKUP AND RECOVERY SOFTWARE

ALTARO BACKUP

Backup Solutions Trusted by 50,000+ Businesses

MORE INFO

Your software selection will have monumental long-term impact on your disaster recovery and business continuity operations. Once you successfully implement your choice of application(s), inertia will set in almost immediately. Most vendors offer renewal pricing substantially below their first-year cost, which makes loyalty attractive. Switching to another provider might prove prohibitively expensive. Even if you get attractive pricing from a competitor, you still need to invest considerable time and effort to make the switch. For these reasons, you should not rush to a determination.

At its core, every single backup application has exactly one purpose: make duplicate copies of bits. Any reasonably talented scripter can build a passable bit duplication system in a short amount of time. Due to the ease of satisfying that core function, the backup software market has a staggering level of competition. With so many available choices, you get some good and some bad news. The good news: you have no shortage of feature-rich, mature options to choose from. The bad news: you have no shortage of feature-rich, mature options to choose from.

You likely will not try out more than a few vendors before you either run out of time or become overwhelmed. In the upcoming sections, you will find many pointers to help you quickly pare down your options to a reasonable subset before installing your first trial package.

BACKUP APPLICATION FEATURES

To distinguish themselves in a marketplace crowded with dozens of other companies trying to sell a product that performs the same fundamental role, backup program manufacturers spend a great deal of time on the supporting features. Like anyone else, they tend to brag about whatever they feel that they do especially well. So, you can often get an overall feeling about a product just by looking at its marketing literature. If they frequently use words like “simple” and “easy”, then you should expect to find a product that will not need a lot of effort to use. If you see several references to “fast” and “quick” and the like, then the application likely focuses on optimizations that reduce the amount of time to perform backup or restore operations. Businesses that work from a value angle tend to use words like “affordable” and “economical”. Words like “trusted” and “leader” tend to indicate a mature product with a dedicated following.

So, if you go to the homepage of a backup vendor and see phrases containing words that speak to you, then you are almost certainly

in that company's target market. At the very least, they think that they have something to offer that fits your needs. You will have to do more work to determine if their product lives up to the promise. However, if you see nothing that addresses your primary concerns, take that as a warning sign. For instance, if you mostly want a stable product with responsive support that you can afford, you might want to avoid a company that prides itself on bleeding-edge capabilities, places its support links after everything else, and makes it difficult to even find pricing.

TRIAL AND FREE SOFTWARE OFFERINGS – WHAT TO LOOK FOR

Every major backup application manufacturer offers a trial, and most offer a free version of their products. You should take advantage of these opportunities. With so many quality products on the market, avoid anything that you cannot try prior to purchase.

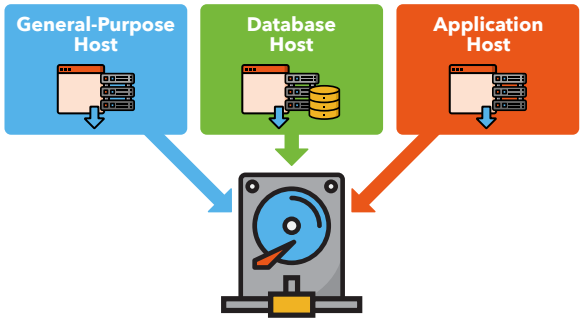
As you test software, use your plan from part one as your guide. If the program cannot satisfy anything on that list, then you must gauge the importance of that deficit. Find out if the program provides an alternative method to achieve the goal. If it does not, then you must choose between augmenting this program with another or skipping the product altogether.

As for free software, it works perfectly well for trial purposes. However, exercise extreme caution if you intend to use it long-term. Commercial software companies need income to survive, so they invariably build their free tiers in some way that showcases the power of their software but still makes the paid tiers desirable. You can even find a few completely free programs provided by contributors out of the goodness of their hearts. These are rarely enterprise-ready and almost never maintained for very long. In all cases, you cannot expect to receive significant support for free products. Think long and hard before deciding to entrust your organization's disaster recovery and business continuity to such tools.

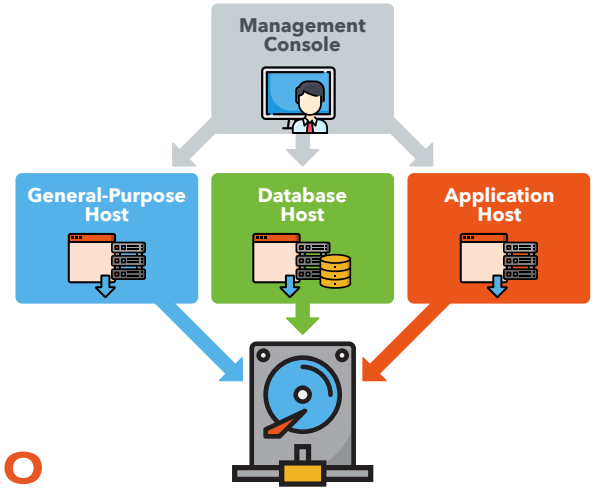
PLACEMENT OF BACKUP SOFTWARE

As you look through your software options, you will find considerable differences in deployment and management behaviors. Take note of their installation requirements and procedures. Common options:

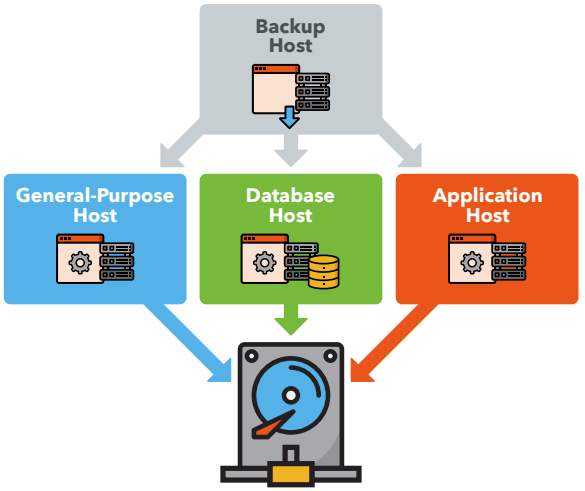
- Per-host installation, data direct to storage, no centralization



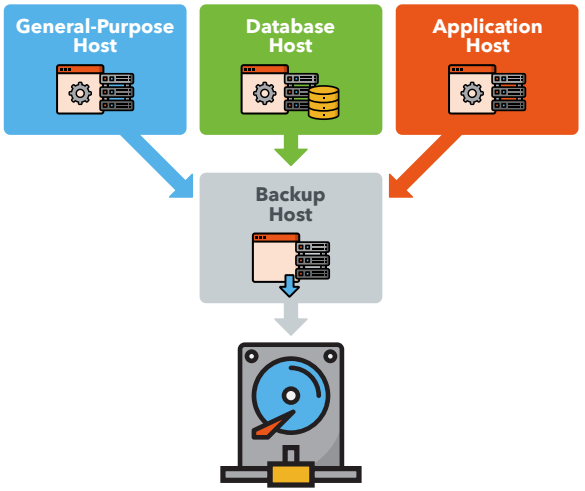
- Per-host installation, data direct to storage, managed from a central console



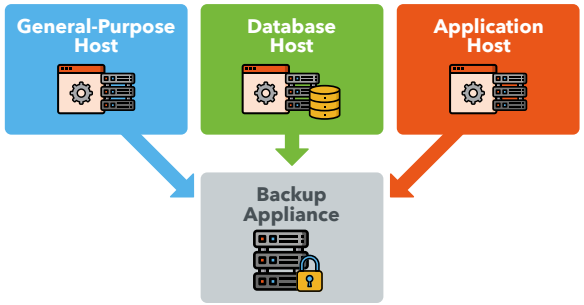
- Central installation, agents on hosts, data direct to storage



- Central installation, agents on hosts, data funneled through the central system



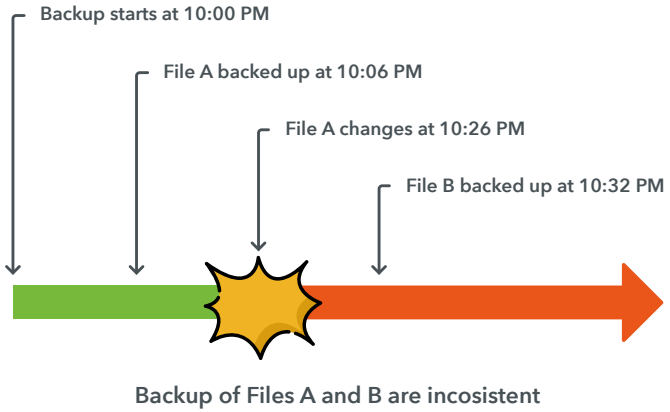
- Appliance-based installation, agents on hosts, data stored on or funneled through appliance



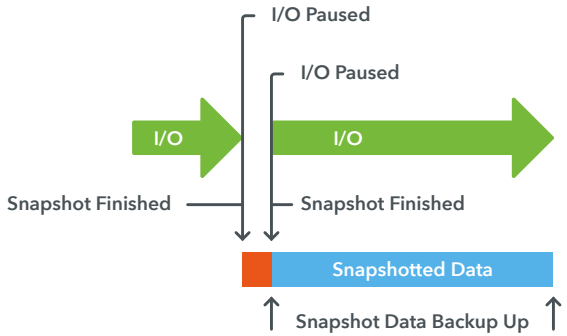
You will find other architectures. Before you purchase anything, ensure that you understand how to deploy it. If you will need to rack a physical appliance or make capacity for a virtual appliance, you do not want that to catch you by surprise. If your preferred program requires a dedicated server instance, that may have licensing implications beyond the backup application's cost.

CONSISTENCY AND APPLICATION-AWARENESS

In the past, we could not capture a consistent backup. Operations would simply read files on disk in order as quickly as possible. But, if a file changed after the backup copied it but before the job completed, then the backup's contents were inconsistent. If another program had a file open, then the backup would usually skip it.



Microsoft addressed these problems with Volume Shadow Copy Services (VSS). A backup application can notify VSS when it starts a job. In response, VSS will pause disk I/O and create a "snapshot" of the system. The snapshot isolates the state of all files as they were at that moment from any changes that occur while the backup job runs. The backup signals VSS when it has finished backing up, and VSS merges the changed data into the checkpoint and restores the system to normal operation. With this technique, on-disk files are completely consistent. However, it cannot capture memory contents. If you restore that backup, it will be exactly as though the host had crashed at the time of backup. For this reason, we call this type of backup "crash-consistent". It only partially addresses the problem of open files.



All Files Consistent; Memory Contents and Paused Transactions Lost (Crash-Consistent)

VSS-aware applications can ensure complete consistency of the files that they control. Their authors can write a component that registers with VSS (called a "VSS Writer"). When VSS starts a snapshot operation, it will notify all registered VSS writers. In turn, they can write all pending operations to disk and prevent others from starting until the checkpoint completes. Because it has no active I/O at the time the backup is taken, the backup will capture everything about the program. We call this an "application-consistent" backup.

As you shop for backup programs, keep in mind that not everyone uses the terms "crash-consistent" and "application-consistent" in the same way. Also, Linux distributions do not have a native analog to VSS. Research the way that each candidate application deals with open files and running applications.

HYPERVISOR-AWARE BACKUP SOFTWARE

If you employ any hypervisors in your environment, you should strongly consider a backup solution that can work with them directly. You can back up client operating systems using agents installed just like physical systems if you prefer. However, hypervisor-aware backup applications can appropriately time guest backups to not overlap and employ optimization strategies that great reduce time, bandwidth, and storage needs.

When it comes to your hypervisors, investigate applications with the same level of flexibility as Altaro VM Backup. You can install it directly on a Hyper-V host and operate it from there, use a management console from your PC, or make use of Altaro's Cloud Management Console to manage all of your backup systems from a web browser. Such options allow you to control your backup in a way that suits you.

STANDARD PHYSICAL SYSTEMS BACKUP SOFTWARE

Few organizations have moved fully to virtualized deployments. So, you likely have physical systems to protect in addition to your virtual machines. Some vendors, such as Altaro, provide a separate

solution to cover physical systems. Others use customized agents or modules within a single application. However, some companies have chosen to focus on one type of system and cannot protect the other.

SINGLE-VENDOR VS. HYBRID APPLICATION SOLUTIONS

In small environments, administrators rarely even consider using solutions that involve multiple vendors. Each separate product has its own expertise requirements and licensing costs. You cannot manage backup software from multiple vendors using a single control pane. You may not be able to find an efficient way to store backup data from different manufacturers. Using a single vendor allows you to cover the most systems with the least amount of effort.

On the other hand, organizations with more than a handful of servers almost invariably have some hybridization – in operating systems, third-party software, and hardware. Using different backup programs might not pose a major challenge in those situations. Using multiple programs allows you to find the best solution for all your problems instead of accepting one that does “enough”.

“ I once had a customer that was almost fully virtualized. They placed high priority on a granular backup of Microsoft Exchange with the ability to rapidly restore individual messages. Several vendors offer that level of coverage for Exchange in addition to virtual machine backup. Unfortunately, no single software package could handle both to the customer’s satisfaction.

To solve this problem, we selected one application to handle Exchange and another to cover the virtual machines. The customer achieved all of their goals and saved substantially on licensing. “

PUTTING IT IN ACTION

Using the above guidance and the plan that you created in part one, you have enough information to start investigating programs that will satisfy your requirements.

PHASE ONE: CANDIDATE SOFTWARE SELECTION

Begin by collecting a list of available software. You will need to find a way to quickly narrow down the list. To that end, you can apply some quick criteria while you search, or you can build the list first and work through it later. Maintain this list and the reasons that you decided to include or exclude a product.

Create a table to use as a tracking system. As an example:

Product	Version	Within	Physical	Hyper-V Virtual Machines	Backup to Cloud	Active Support
Product A	7.0	Yes	Yes	No	No	No
Product B: Advanced Edition	2.1	No				
Product B: Started Edition	2.1	Yes	Yes	No	Yes	Yes
Product C	4.9	Yes	Yes	Yes	Yes	Yes

It might seem like a bit much to create this level of documentation, but it has benefits:

- **Historical purposes:** Someone might want to know why a program was tested or skipped
- **Reporting:** You may need to provide an accounting of your selection process
- **Comparisons:** Such a table forms a feature matrix

Because this activity only constitutes the first phase of selection, use criteria that you can quickly verify. To hasten the process, check for any deal-breaking problems first. You can skip any other checks for that product. While the table above shows simple yes/no options, you can use a more nuanced grading system where it makes sense. Keep in mind that you want to shorten this list, not make a final decision.

PHASE TWO: IN-DEPTH SOFTWARE TESTING

You will likely spend the most time in phase two. Phase one should have left you with a manageable list of programs to explore more completely. Now you need to spend the time to work through them to find the solution that works best for your organization.

Keep in mind that you can use multiple products if that works better than a single solution.

For this phase, you will need to acquire and install software trials. Some recommendations:

- Install trialware on templated virtual machines that you can quickly rebuild
- Use test systems that run the same programs as your production systems
- Test backing up multiple systems
- Test encryption/decryption
- Test complete and partial restores

Extend the table that you created in phase one. If you used spreadsheet software to create it, consider creating tabs for each program that you test. You could also use a form that you build in a word processor. Make sure to thoroughly test each program. Never assume that any given program will behave like any other.

PHASE THREE: FINAL SELECTION

Hopefully, you will end phase two with a clear choice. Either way, you will likely need to notify the key stakeholders from phase one of your selection status. If you need additional input or executive sign-off to complete the process, work through those processes.

Unless you chose a completely cloud-based disaster recovery approach, you will still need to acquire hardware. Remember that, due to threats of malware and malicious actors, all business continuity plans should include some sort of in-house solution that you can take offline and offsite. If you have not yet made your hardware choices, then you might want to work through the next section before closing phase three of software selection.

BACKUP STORAGE TARGETS

ALTARO BACKUP

Backup Solutions Trusted by 50,000+ Businesses

MORE INFO

The days of tape-only solutions have come to an end. Other media has caught up to it in cost, capacity, convenience, and reliability. You now have a variety of storage options. Backup applications that can only operate with tape have little value in modern business continuity plans.

Unless you will buy everything from a vendor or service provider that designs your solution, make certain to match your software with your hardware. Use the software's trial installation or carefully read through the manufacturer's documentation to determine which media types it works with and how it uses them.

Backup software targets the following media types:

- Magnetic tape
- Optical disc
- Direct-attached hard drives and mass media devices
- Media-agnostic network targets
- Cloud storage accounts

MAGNETIC TAPE IN BACKUP SOLUTIONS

I.T. departments have relied on tape for backup since the dawn of the concept of backup. The technology has matured well and mostly kept up with the pace of technology. However, the physical characteristics of magnetic tape place a severe speed limit on backup and restore operations.

PROS OF MAGNETIC TAPE:

- Most backup software can target it
- Tape media has relatively low cost per gigabyte
- Reliable for long-term storage
- Lightweight media, easy to transport offsite
- Readily reusable

CONS OF MAGNETIC TAPE:

- Extremely slow
- Tape drives have a relatively high cost
- Media susceptible to magnetic fields, heat, and sunlight

> *I have seen many techniques for tape management through the years. One of the worst involved a front desk worker who diligently took the previous night's tape offsite each night – leaving it on their car dashboard. It would bake in the sunlight for a few hours each night. So, even though the company and its staff meant well, and dutifully followed the recommendation to keep backups offsite, they wound up with warped tapes that had multiple dead spots.*
>
> *At the opposite end, one customer used a padded, magnetically shielded carrying case to transport tapes to an alternative site. There, they placed the tapes into a fireproof safe in a concrete room.*
> *I was called upon once to try to restore data from a tape that was ten years old. It took almost a week to find a functioning tape drive that could accommodate it.*

For most organizations, the slow speed of tape presents its greatest drawback. You can find backup applications that support on-demand features such as operating directly from backup media. That will not happen from a tape.

Tape has a good track record of reliability. Tapes stored on their edges in cool locations away from magnetic fields can easily survive ten years or more. Sometimes, the biggest problem with restoring from old tape is finding a suitable, functioning tape drive.

OPTICAL MEDIA IN BACKUP SOLUTIONS

For a brief time, optical technology advances made it attractive. Optical equipment carries a low cost and interfaces well with operating systems. It even supports drag-and-drop interactivity with Windows Explorer. They were most popular in the home market. Some optical systems found their way into datacenters. However, magnetic media quickly regained the advantage as capacities outgrew optical media exponentially.

PROS OF OPTICAL MEDIA:

- Very durable media
- Shelf life of up to ten years
- Inexpensive, readily interchangeable equipment
- Drag-and-drop target in most operating systems
- Lightweight media, easy to transport offsite

CONS OF OPTICAL MEDIA:

- Very limited storage capacity
- Extremely slow
- Few enterprise backup applications will target optical drives
- Poor reusability
- Wide variance in data integrity after a few years

When recordable optical media first appeared on the markets, people found its reliability attractive. CDs and DVDs do not care about magnetic fields at all and have a higher tolerance for heat and sunlight. Also, because the media itself has no mechanism at all, they survive rough handling better than tape.

However, they have few other advantages over other media types. Even though the ability to hold 700 megabytes on a plastic disc was impressive when recordable CDs first appeared, optical media capacities did not keep pace with magnetic storage. By the time recordable DVDs showed up with nearly five gigabytes of capacity, hard drives and tapes were already moving well beyond that limit.

Furthermore, people discovered – often the hard way – that even though optical discs have hardy structural material, their data-retaining material has much shorter life. Even though a disc may look just fine, its contents may have become unreadable long ago. Recordable optical media has a wide range of data life, from a few years to several decades. Predicting media life span has proven difficult.

Because of its speed, low capacity, and need for frequent testing, you should avoid optical media in your disaster recovery solution.

DIRECT-ATTACHED STORAGE AND MASS MEDIA DEVICES IN BACKUP SOLUTIONS

You do not need to limit your backup solutions to systems that distinguish between devices and media. You can also use external hard drives and multi-bay drive chassis. Some attach temporarily, usually via USB. Others, especially the larger units, use more permanent connections such as Fiber Channel. These types of systems have become more popular as the cost of magnetic disks has declined. They have a somewhat limited scope of applications in a disaster recovery solution, but some organizations can put them to great use.

PROS OF DIRECTLY ATTACHED EXTERNAL DEVICES:

- Fast
- Reliable for long-term storage
- Inexpensive when using mechanical drives
- Easily expandable
- High compatibility
- Use as a standard file system target

CONS OF DIRECTLY ATTACHED EXTERNAL DEVICES:

- Difficult to transport
- Additional concerns when disconnecting
- Mechanical drives have many failure points
- Expensive when using solid-state drives
- Not a valid target in every backup application

Portability represents the greatest concern when using directly attached external devices for backup. Unlike tapes and discs, the media does not simply eject once the backup concludes. With USB devices, you should notify the operating system of pending removal so that it has a chance to wrap up any writes, which could include metadata operations and automatic maintenance. Directly connected Fiber Channel devices usually do not have any sort of quick-detach mechanism. In an emergency, people should concern themselves more with evacuation than spending time going through a lengthy detach process. In normal situations, people tend to find excuses to avoid tedious processes. Expect these systems to remain stationary and onsite.

Once upon a time, such restrictions would have precluded these solutions from a proper business continuity solution. However, as you will see in upcoming sections, other advances have made them quite viable. With that said, you should not use a directly attached device alone. Any such equipment must belong to a larger solution.

You may run into some trouble using external devices with some backup applications. Fortunately, you should never run into any modern programs that absolutely cannot backup to a disk target. However, some may only allow you to use disk for short-term storage. Others may not operate correctly with removable disks. If you purchase your devices before your software, make certain to fully test interoperability.

Even though mechanical hard drives have advanced significantly in terms of reliability, they still have a lot of moving parts. Furthermore, designers of the typical 3.5-inch drive did not build them for portability. They can travel, but not as well as tapes or discs. Even if you don't transport them, they still have more potential failure points than tapes. Do not overestimate this risk, but do not ignore it, either.

NETWORKED STORAGE IN BACKUP SOLUTIONS

Network-based solutions share several characteristics with directly attached storage. Where you find differences between the two, you also find tradeoffs. You could use the same pro/con list for networked solutions as you saw above for direct-attached systems. We place the emphasis on different points, though.

In the "pros" column, networked storage gets even higher marks for its expandability. Typically, storage units built for the network sport multiple bays. They usually have more slots than common USB-based systems. You can start with a few drives and add more as needed. Some even allow you to connect multiple chassis, physically or logically. In short, you can extend your backup storage indefinitely with such solutions.

You will pay a higher overall cost per gigabyte for network-attached storage due to the network components. The need for manufacturers to build in the necessary infrastructure to present their devices as network citizens tends to have a side effect: even more features. Almost all provide some level of security filtering. Less expensive devices, typically marketed as "Network-Attached Storage" (NAS), may not provide much more than that. Higher-end equipment,

commonly called “Storage Area Network” (SAN), boasts many more features. You can often make SAN storage show up in connected computers much like directly attached disks. In all, the more you pay, the more you get. Unfortunately, though, cost increases more rapidly than features.

What you gain in capacity and features, you lose in portability. Many NAS and SAN systems are rack-mounted, so you cannot transport them to a safe offsite location without significant effort. But, because these devices have a network presence, you can place them in remote locations. Using them requires some sort of site-to-site network connection, which introduces security concerns, possible reduction in speed, and more points of failure.

Even though placing networked storage offsite involves additional risks, it also presents opportunity. Most NAS and SAN devices have replication technology. You can back up to a local device and configure it to automatically replicate to remote site(s). If your device cannot perform replication, or if you have different devices and they cannot replicate to each other, your backup software may have its own replication methods.

USING COMMODITY COMPUTING EQUIPMENT AS BACKUP STORAGE

Up to this point, we have talked about network-attached devices only in terms of dedicated appliances. SANs have earned a reputation for carrying price tags that exceed their feature sets. In the best case, that reduces your budget’s purchasing power. More commonly, an organization cannot afford to put a SAN to its fullest potential – if they can afford one at all.

As a result, you now have choices in software-based solutions that run on standard server-class computing systems. Some backup applications can target anything that presents a standard network file protocol, such as NFS or SMB. Software vendors and open-source developers provide applications that provide network storage features on top of general-purpose operating systems. These solutions fill the price and feature space between NAS and SAN devices. They do require more administrative effort to deploy and maintain than dedicated appliances, however.

CLOUD STORAGE IN BACKUP SOLUTIONS

Several technological advances in the past few years have made internet-based storage viable. Most organizations now have access to reliable, high-speed internet connections at low cost.
You can leverage that to solve one of the most difficult problems in backup: keeping backup data in a location safe from local disasters.
Of course, these rewards do not come without risk and expense.

PROS OF CLOUD BACKUP:

- Future-proof
- Offsite from the beginning
- Wide geographical diversity
- Highly reliable
- Effectively infinite expandability
- Access from anywhere
- Security

" When I built my first backup solution with the intent of targeting a dedicated appliance, I quickly learned that hardware vendors emphasize the performance features of their systems. Since I only needed large capacity, I priced a low-end rack-mount server with many drive bays filled with large SATA drives. I saved quite a bit over the appliance options. "

CONS OF CLOUD BACKUP:

- Dependencies outside your control
- Expensive to switch vendors
- Possibility of unrecoverable interruptions
- Speed

To keep their promises to customers, cloud vendors replicate their storage across geographical regions as part of the service (cheaper plans may not offer this protection). So, even though do you need to worry about failures in the chain of network connections between you and your provider and about outages within the cloud provider, you know that you will eventually regain access to your data. That gives cloud backup an essentially unrivaled level of reliability.

The major cloud providers all go to great lengths to assure their customers of security. They boast of their compliance with accepted, standardized security practices. Each has large teams of security experts with no other role than keeping customer data safe. That means that you do not need to concern yourself much with breaches at the cloud provider's level. However, you will need to maintain the security of your account and access points. As with any other internet-based resource, the provider must make your data available to you somehow. Malicious attackers might target your entryway instead of the provider itself. So, you still accept some responsibility for the safety of your cloud-based data.

When using cloud storage for backup, two things have the highest probability of causing failure. Your internet provider presents the first. If you cannot maintain a reliable connection to your provider, then your backup operations may fail too often. Even if you have a solid connection, it might not have sufficient bandwidth to support your backup needs. For the latter problem, you can choose backup software such as Altaro VM Backup that provides compression and deduplication features specifically to reduce the network load.

Your second major concern is interim providers. While you can trust your cloud provider to exercise continuous security diligence, many third-party providers follow less stringent practices. If your backup system transmits encrypted data directly to a cloud account that you control, then you have little to worry about. Verify that your software uses encryption and keep up on updates, and you will have little to worry about beyond the walls of your institution. However, some providers ship your data to an account under their control that they

resell to customers. If they fall short on security measures, then they place your data at great risk. Vet such providers very carefully.

"Cost" did not appear on either the pro or con list. Cost will always be a concern, but how it compares to onsite storage will differ between organizations. Using cloud storage allows you to eliminate so-called "capital expenditures": payments, usually substantial, made up-front for tangible goods. If you have an internet connection, you will not need to purchase any further equipment. You also wipe out some "operational expenses": recurring costs to maintain goods and services. You will need to pay your software licensing fees, and your cloud provider will regularly bill you for storage and possibly network usage. However, you will not need to purchase storage hardware, nor will your employees need to devote their time to maintaining it. You transfer all the hassle and expense of hardware ownership to your provider in exchange for a lower overall fee.

Unfortunately, you cannot transfer your entire backup load to a cloud provider. Due to the risks and speed limits of relying on an internet connection, it still makes the most sense to keep at least some of your solution onsite. So, you should still expect some capital expense and local maintenance activities.

PUTTING IT IN ACTION

The previous section helped you to work through your software options. If you have made a final selection, then that has at least some control over your hardware purchase. If not, then you can explore your hardware options and work back to picking software.

STEPS TO PERFORMING HARDWARE SELECTION

Truthfully, your budget plays the largest restrictor in hardware options. So, start there. Work through the features that you want to arrive at your project scope. Your general process looks like this:

1. Determine budget
2. Establish other controlling parameters
    a. Non-cloud replication only works effectively if you have multiple, geographically distant sites
    b. Inter-site and cloud replication need sufficient bandwidth to carry backup data without impeding business operations
    c. Rack space

4. Decide on preferred media type(s). The above explanations covered the pros and cons of the types. Now you need to decide what matters to your organization:
    a. Cost per terabyte
    b. Device/media speed
    c. Media durability
    d. Media transportability
5. Prioritize desired features:
    a. Deduplication
    b. Internal redundancy (RAID, etc.)
    c. External redundancy (hardware-based replication)
    d. Security (hardware-based encryption, access control, etc.)

If you find that the cost of a specific hardware-based feature exceeds your budget, then your software might offer it. That can help you to achieve the coverage that you need at a palatable expense.

Once you have concluded your hardware selection, you could proceed to acquiring your software and equipment. However, it makes sense to work through the next portion on security before making any final decision. You might decide on a particular course for securing data that influences your purchase.

SECURING AND PROTECTING BACKUP DATA

Multiple high-profile breaches have made everyone painfully aware of the need for data security. The theft of unencrypted backup tapes from a few major organizations widened the scope to include backup. Unfortunately, information technology departments have not done much to improve protection of cold data. Since attackers typically target active data and online systems, technology professionals and data security firms focus efforts there. For many years, businesses have avoided compromise of backup systems more by luck than by effort. In the age of ransomware, that luck will run out in dramatic fashion.

While we often think of "data security" in terms of warding off malicious intrusion, it has broader scope. Data damaged by accident or catastrophe is just as lost as data encrypted by ransomware. You must protect your information from all dangers, not just evil intent.

RISK ANALYSIS FOR BACKUP

Hopefully, you have already performed some sort of risk analysis for your production systems. If so, you already have an idea of the importance of the various items that you back up. Most of that transfers directly to the backup copies. However, you should consider all your backup data as a target. Large organizations often segregate data in backups due to time or capacity constraints, but many coalesce all of it into one place. If you decide not to encrypt the backups of data that has no value to a thief, such as documents that you make available to the public for free, then an attacker may find a way to use that as a keyhole to get to your encrypted data.

As you think of risks to your backup data, remember one of the primary reasons that backup belongs to your disaster recovery solution: it can help your data to survive physical loss or damage to your live systems. Geographical dispersion provides a direct answer to those concerns. A proper protection system places significant distance between at least some of your backup data and its home site.

Different geographical locations face unique threats. Coastal facilities must suffer through hurricanes. Heavily forested areas deal with more fires. Inland plains deal with tornadoes. Dense urban areas sometimes go through periods of destructive civil unrest or worse. Think through the ways that your business continuity system protects you from the realistic dangers that you face.

RANSOMWARE RISKS TO BACKUP

Ransomware creates a unique challenge. Where traditional attacks try to steal or destroy your data, ransomware wants to prevent you from accessing it. Standard disaster recovery technique easily thwarted early ransomware. Administrators would simply wipe out the live system entirely and rebuild from the latest backup.

As ransomware proved itself a uniquely lucrative vector for malicious actors, it received greater development efforts. Where the initial iterations of this type of malware would try to spread following the techniques of viruses and worms, newer programs can specifically target backup software. If uncaught, they will encrypt all data that they can reach. Such risk should influence your backup deployment.

SECURITY BY REDUNDANCY

We use backup primarily because it makes a distinct copy of our live data. To solidify that protection, we need to have further redundancy within our backups. Each unique copy greatly reduces the odds of a permanent loss. In part one, we covered the multiple lines of defense against data loss. Your disaster recovery system must have its own separate tiers.

THE ROLE OF RETENTION AND ROTATION POLICIES IN BACKUP SECURITY

In and of themselves, retention policies do not impact redundancy. However, they do set how far you can stretch your media. If you have very long retention policies, then you will require more media capacity to achieve the same frequency of full backups. No matter what technology and technique you use to store your backups, never rely on a single copy of anything. Prefer to shorten your retention policy rather than sacrifice having sufficient full backups.

To make the most use of your backup media and storage space, you will establish a rotation practice to reuse it. if you have a tape-based system, then you might opt for a scheme that reuses some tapes but keeps others for long periods of time. If you use a disk-based system, then you might rotate through removable drives or periodically exclude some backups from deduplication. Utilize these techniques in a way that balances the economics of media consumption with the value of multiple full copies.

Rotation can really shine when you leverage it as protection against malware. If malware impacts your backup solution, then it will encrypt anything that the program touches. Only your offline media will remain safe.

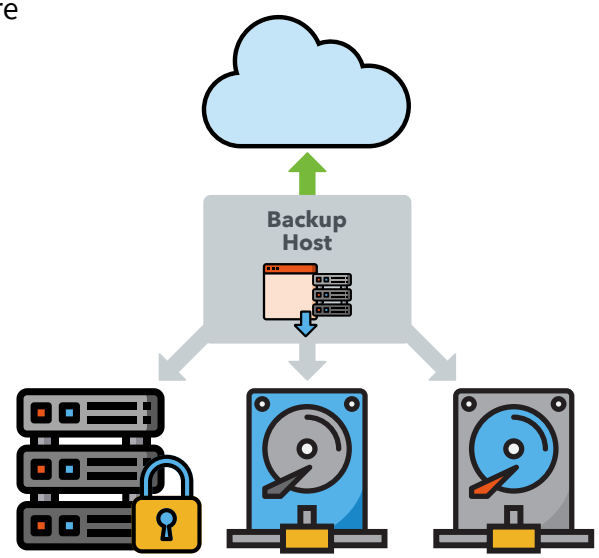
You will need to exercise vigilance over your backup solution so that you can catch infections before one makes its way through your rotation.

PROTECTING YOUR BACKUPS WITH MULTIPLE TIERS

Storage cost per terabyte continually declines as technology advances. You can take advantage of that to create backups of your backups. Whereas your rotation schemes and full backup scheduling will prevent corrupted deduplication data from causing overwhelming loss, they do little to protect data that only exists on a single backup.

You have several ways to address this problem:

- Multiple copies in separate locations made by your backup software



Replication of backup data using built-in NAS/SAN features

- Replication of backup data using external software

You can use multiple approaches as suits your needs and the technology available to you. For instance, you might have your backup software place its data on a NAS and then use a storage replication technology to copy it to another system. An older solution, called disk-to-disk-to-tape, would use backup software to keep recent data on tapes and then transfer it to disk as it aged.

Where possible, try to use the capabilities of your backup software. If someone needs to take over your deployment after your departure, you want them to leave them with the fewest complications possible. While you retain control, you do not want a convoluted system that makes your maintenance activities difficult.

USING ACCOUNT CONTROL TO PROTECT YOUR BACKUPS

Backup has a special role in your information technology environment, but it has the same foundational needs as all your other systems. So, you can apply common security practices to it.

Start by creating a unique account to run backups and lock it down. Scope its abilities to taking backup. If your backup application allows it, consider using different accounts in different contexts. Exercise restraint; do not make an unmanageable mess. Follow the same practices that you should for all vital service accounts:

- Maintain very tight control over the account – treat it like a domain administrator
- Place the account in an organizational unit that grants control to the fewest possible people
- Assign viable rotation and complexity policies to the password
- Change the password immediately if anyone with access leaves the organization for any reason
- Use a properly secured password vault

ENCRYPTING YOUR BACKUP DATA

You can easily reduce the risk of your data falling into the wrong hands by employing encryption. If someone steals a tape or cracks into your cloud account, it will not gain them much if they find encrypted data for which they have no key.

All modern backup software should natively include some form of encryption. Avoid any that does not. When you try the software, ensure that you understand how it implements encryption. If you intend to rely on an application's deduplication and other storage relief features, run comparisons to determine how encryption impacts them.

While encryption does greatly strengthen the security of your backups, do not rely on it alone. If someone steals an encrypted copy of your data, then they have a copy of your data. If your attacker has the expertise, time, and willingness, they will eventually break even the

" Years ago, almost no one encrypted their backup tapes. Some organizations would keep them in a safe deposit box at a bank or in some other kind of secured storage. Only a few took any precautions to secure them during transport or to validate their inventory. Thieves realized that with these lax controls, it was easier to steal data from tapes than to directly attack the company. After a few high-profile breaches, encryption became a much more desirable feature in backup applications. Some countries have passed laws that require certain types of institutions to encrypt sensitive data.

Fortunately, I have never been involved with any organization that had tapes stolen. However, many clients lost track of their tapes. They could usually locate their most recent backups fairly quickly, but anything older than that sometimes… disappeared. Remember that some data, such as a social security number, never truly expires. The data on your archived backup media deserves the same level of protection as the data on your active systems. "

best ciphers with the longest keys. We expect to have many years before anyone breaks through current cryptographic schemes, but we cannot know what vulnerabilities remain hidden or how imminent technological advances will impact codebreaking. Employ all available security measures.

Remember to take special care of the keys used to encrypt your backups. They represent the weakest links with this strategy. Use similar techniques to protect them to those that you implement for important account passwords.

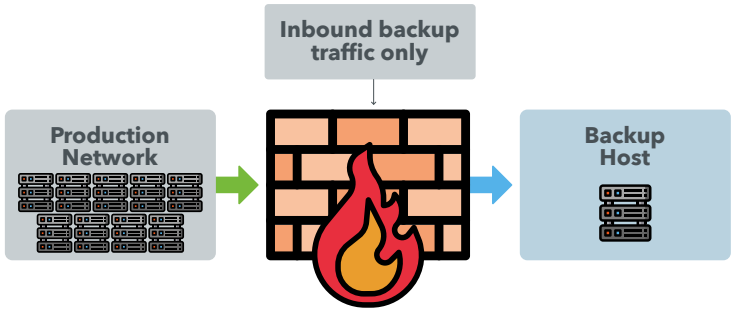
ISOLATING YOUR BACKUP SYSTEMS

Take steps to reduce the surface area of your backup. In some way, backup touches everything in your environment, but the reverse does not need to be true. Isolation techniques range from simple to highly complex; you will need to balance the risk of not employing a method against the effort of implementing it.

SHIELDING BACKUP SYSTEMS WITH FIREWALLS

Your backup application should have the ability to reach out to other systems, but almost nothing needs to reach into its system.

You can put up barriers to external access easily using firewalls.



Every modern operating system includes a native firewall. Several third parties provide add-on software firewalls. Your antimalware software might include a firewall module.

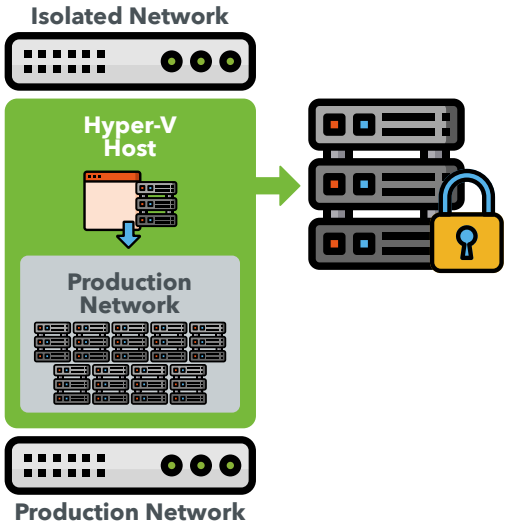
Hardware firewalls bolster software firewalls immensely. Most smaller organizations typically employ them only at the perimeter, but they can add substantial security to your internal networks as well.
Even inexpensive devices provide isolation and protection.
You can also configure routers and switches with VLANs or network address translation to provide additional isolation layers.

AIR-GAPPING FOR ISOLATION

Among all the methods of isolating, air-gapping represents the strongest. However, it also requires the most effort to implement. Before choosing this route, take the time to understand its ramifications. It should not be undertaken on a whim or without input from executive decision makers.

The simplest description of air-gapping is that there is no remote connectivity into a given system. A most extreme example is offline root certification authorities. Administrators create them, publish their public keys and revocation lists, then take them offline and disconnect them. Some even go to extra steps, such as removing their hard drives and placing them in locked storage. To access such a system, a human must perform manual steps that involve physical actions and security measures.

You cannot realistically apply such a drastic procedure to your backup system. However, it serves as a foundational approach. Start there and add the minimum elements to make backup operational. Backup servers need to be powered on and have some way to retrieve data from or push restores to their targets, but nothing else.
To make maintenance easier, the system should have some way of sending notifications to administrators. With all of that configured, you do not absolutely need some way to access the backup server remotely. So, you can set it up to only allow access from a physical console.



The more that you use virtualization in your environment, the easier you make it to use air-gapping. You can configure the hypervisor and backup in one network and everything else in another. If they have no overlap or interconnect, then you have created a proper air gap. You may even choose to go so far as to create an Active Directory domain just to hold these systems. That way, you can benefit from centralized management without connecting your production network to your management network.

The greatest risk with an air-gapped system is its enormous inconvenience. Preventing remote connections includes blocking valid administrative duties, too. It makes patching very difficult. It has no ability to transfer data to a remote location, either, which means that you lose replication capability. You have only two choices: cope with these restrictions or do something that breaks the air-gapping. A poorly air-gapped system is more vulnerable than one that was designed from the start to belong to the network. If you cannot commit to a completely disconnected system into perpetuity, then connect your backup system and build defenses around it.

CARING FOR OFFLINE DATA

The cold data that lives on data tapes and detached hard drives often does not get the protection that it deserves. Usually, IT departments start out with a protocol to care for them, but over time, they lose diligence. We covered encryption in an earlier section, which can serve as a last-ditch safeguard. However, you must make every effort to prevent unauthorized access.

At its core, your approach involves establishing a “chain of custody” for all your backup media. If only one person has responsibility for the media, then that person must follow a defined practice for safely transporting and storing it. Treat this media as though the life of your company depends on it – because it does. Some organizations can even justify outsourcing these tasks to a security company.

Technological advances, reduced costs, and increased convenience have made fully online backup systems viable. Today, you can easily replicate backup data to geographically remote locations without an exorbitant investment. However, the ever-growing threat of ransomware means that you must periodically create offline copies. In the past, that could only mean data that was completely inaccessible by any automated means. That is still the safest option.

However, you can take advantage of modern technology to create alternative approaches. You could manually upload backup data to a location that requires two-factor authentication, for instance. Whatever measures you put in place, ensure that they isolate the remote site in such a way that no compromise of your online backup system or password vault will put offline data at risk.

PUTTING IT IN ACTION

Think of security as a continual process, not a one-time event. We will cover the hardware portions in the next section on deployment. This portion will cover these security actions:

- Perform a risk analysis
- Set policies for software-level/media redundancy
- Establish backup encryption policy
- Determine practices and policies for creating and protecting offline data

You saw the concepts behind these activities above. Now you must put them into practice.

RISK ANALYSIS ACTIVITIES

Much of risk analysis involves asking questions. You should gather input from multiple sources. Usually, one person does not have the visibility to know all likely risks. You can use formal meetings, informal queries, or any other approach that works for your organization. Categorize and list what everyone comes up with. Share them with key stakeholders, as that might bring other ideas to mind. Some starting ideas:

- Internal vs. external categories
- Malicious vs. accidental damage
- Targeted risks (e.g. employee data, client data, account numbers, etc.)
- Equipment failures

- Weather
- Electrical outages

You must keep this list up to date with an explanation of how your solution mitigates each.

CREATING BACKUP REDUNDANCY POLICIES

You will need to have made your software and hardware selections before you can craft your redundancy approach. The features and media types used in your systems will have great influence on your decisions. However, your primary goal must be to create sufficient standalone copies to survive loss or damage.

To qualify as “standalone”, a backup copy must not require any other backup data to exist in order for you to restore it. Furthermore, to provide security, the copy must only exist in an offline, disconnected state. Due to the inconvenience of offline backups, you can either build a schedule that mixes online with the occasional offline complete backup, or you can set a special schedule for offline backups.

You also need to plan for how long these offline copies will exist. The cost, longevity, and ease of storing the media tends to have the greatest control over that. If possible, simply keep them until you can no longer restore from them. Reality often dictates otherwise.

If you can schedule full backups, then you might come up with a schedule such as:

- **Monthly:** full, offline
- **Weekly:** full, online

Some modern backup software that relies heavily on deduplication technology does not allow for scheduled full backups. Instead, these depend on other policies to set the oldest possible backup and calculate deduplication from that point forward. Therefore, they consider full backups to be special, so you will need to perform them manually. The inconvenience of such backups, especially for an already busy IT department, will likely prevent their weekly occurrence. Create a palatable policy that balances the security of multiple full copies against the ease of creating them.

ESTABLISHING AN ENCRYPTION POLICY

You will need to build your backup encryption policy around the way that your backup hardware or software utilizes encryption.

Most software requires a single secret key for encryption. You have three major points for this type:

- Where will you store the key?
- Who will have access to the key?
- How will you ensure that the key will survive catastrophe?

Remember to include the loss of your backup encryption key in your risk analysis!

The location of your key directly dictates access. Since you need it to remain available in the event of a total loss, then your best option is likely a cloud-based password vault. There are multiple software companies that provide such services. Microsoft's Azure has a "Key Vault" product and Amazon Web Services offers "AWS Secrets Manager". Find the solution that works for your organization.

Any backup created with a particular encryption key will always need that key. So, if you change the key, you still need to keep a historical record for as long as a key has protected data.

Your hardware may offer some encryption capabilities. These features are manufacturer dependent. You will need to learn how it works before you can create a policy. If you prefer, you can simply use the software's protection and forgo hardware-level encryption.

SHIELDING BACKUP WITH PHYSICAL AND NETWORK PROTECTIONS

Leverage your infrastructure and network systems to build a layer of protection around your backup systems easily and efficiently. You will need to defend at layers one, two, and three.

1. Implement layer one (physical) protections
    - Place backup hosts and devices in secure locations
    - Create a chain-of-custody process for backup media
    - If possible and cost effective, do not directly share switching hardware between backup systems and other systems
2. Implement layer two (Ethernet) protections
    - Establish a VLAN just for your backup systems, or
    - Use dedicated physical switches for your backup systems and connect them to the rest of your production network through a router

3. Implement layer three (TCP/IP) protections

- If you isolate with a VLAN or dedicated router, create an IP subnet just for backup
- Set up a firewall at the edge of the backup network that blocks all externally initiated ingress traffic
- Configure the software firewall on backup hosts with a similar configuration to the previous firewall

All, or most of the previous isolation techniques should fit within even modest budgets. For greater protection, you have additional options.

- Install intrusion prevention and detection solutions
- Configure network monitoring

Data moving into your backup network will fit easily recognizable patterns. With even a rudimentary monitoring system, you should have no trouble spotting suspicious traffic.

FULLY ISOLATING BACKUP SYSTEMS

Perform a complete risk analysis before you even consider an air-gapped approach. If you do not face significantly high exposure threats from malicious actors. Complete isolation looks simple, but it presents substantial long-term challenges for administrators. Review the discussion above and consult with executives, key stakeholders, and others in your IT department with deployment or maintenance responsibilities.

Due to full isolation, this approach only works for hypervisor-based backups.

To create an air-gapped backup system:

1. Designate an IP subnet for your air-gapped network
2. Decide on a workgroup or management domain configuration
    a. If you will use a management domain, create and configure it before proceeding
3. Connect your hypervisor and backup hosts to a physical network that has no uplink

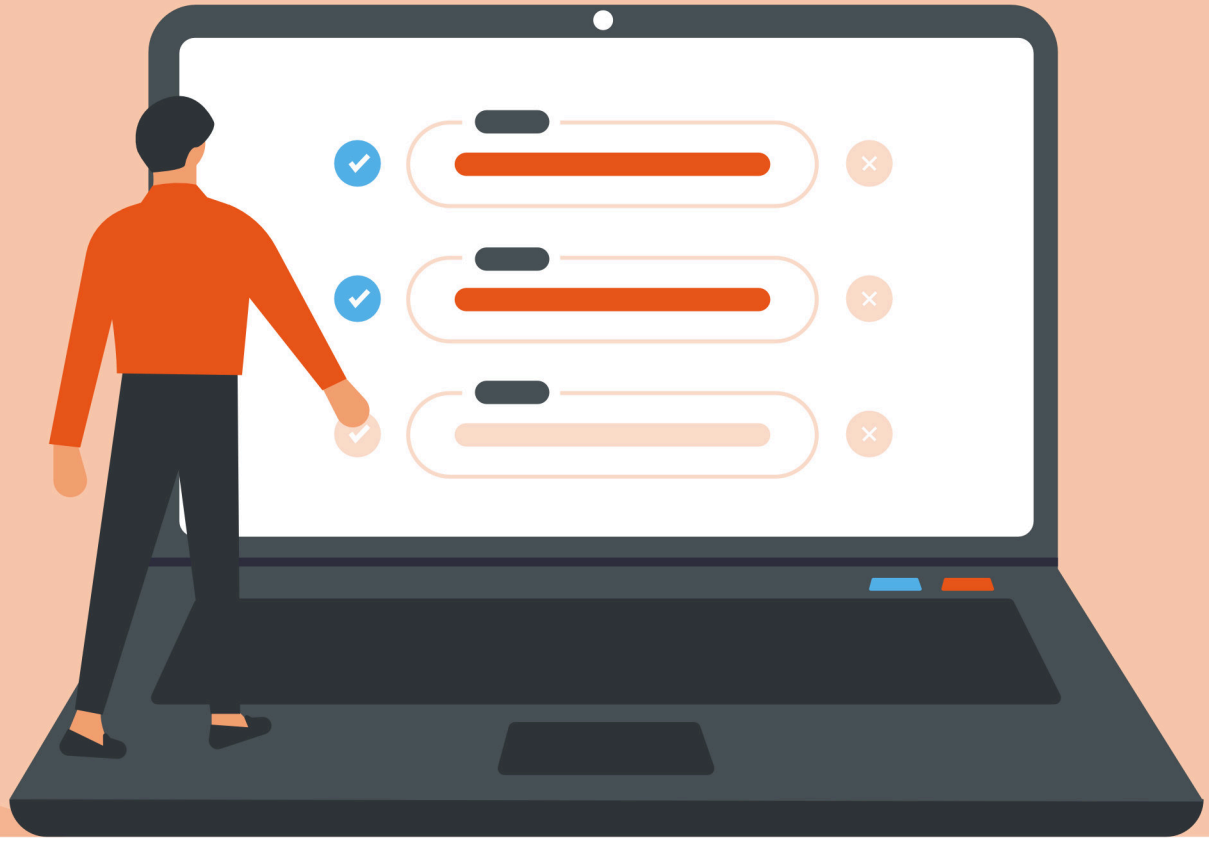
4. Ensure that the physical network links that you use for virtual machines does not provide any layer two or layer three connectivity to the hypervisor's management operating system

5. Create a policy and an accountability process for acquiring and applying software updates

The only practical risks to a properly air-gapped system are internal actors and breakout attacks against your hypervisors or container hosts. It still makes some sense to use anti-malware software as well as intrusion prevention and detection systems.

Remember the one rule for an air-gapped system: It cannot participate on any network connection except those dedicated to the backup system. It cannot connect to the Internet in any way. If you cannot permanently guarantee absolute isolation, then you should instead follow the steps in the previous section to allow your backups to participate on the network with adequate protections.

DEPLOYING BACKUP



If you have completed all previous tasks, then you have enough to begin deploying your backup solution. The process is straightforward.

1. Acquire software and hardware
2. Place backup hardware
3. Install backup software into your test environment
4. If your software uses agents, push to test systems
5. Fully test your hardware and software. Verify all functionality, even the portions that you might not expect to use.
6. Document the test environment setup and installation process. Take special note of anything that did not go as planned and how you remedied the problem.
7. Install backup software into your production environment
8. If your software uses agents, push to a representative sampling of systems
9. Test expected functionality on the sample systems
10. Document the deployment into production, including fixes and workarounds
11. Continue deploying agents, if necessary, until you have covered your entire environment
12. Capture your initial full backup to store offline and transport it to the offsite location
13. Train staff on usage and have them practice
14. Document backup and restoration processes

Keep your documentation handy. As you work through the post-deployment phases, you will establish other processes and uncover other challenges. Keep careful track of any knowledge that could possibly aid yourself or others in the future. Make the documentation simple to follow, as you have no guarantee that the task of restoration will fall to someone familiar with any of your equipment or software.

First, you need to establish your recurring backup routine. You will see how to do that in the upcoming “Defining Backup Schedules” section. If you have added a replication mechanism to your backup solution, you will implement that once you have completed your initial deployment. Part three of The Backup Bible will cover replication in more detail.

DOCUMENTING YOUR BACKUP SYSTEM

The notes that you gather during your test deployment can be informal. Use any method that will serve to prepare you for the production deployment. You need to put much more effort into the documentation that you create for your permanent installation.

DOCUMENTATION PROCEDURES AND TOOLS

If you don't have a formal documentation process for your IT activities, start one. It's certainly a best practice to document all of your systems, but you absolutely must take full stock of the one that forms the backbone of your disaster recovery process.

Disaster recovery works differently from other systems, so its documentation has unique goals:

- Must be accessible in the absence of typical digital storage, such as an on-premises file server
- Non-technical people must be able to comprehend it
- A sufficient number of people, including personnel outside of IT, must have knowledge of the documentation and access to it

You can use any tools that you like, provided that that can produce documentation that satisfies those goals. Figure out your criteria for meeting them. Ask non-technical stakeholders for their opinions. Someday, they may need to refer to your documentation without your guidance.

If you have access to the desktop Microsoft Office version of OneNote, you will find it more than a capable tool for most needs. It shares many features with Word, so you can create headers and lists. You can paste almost any type of content, but more like PowerPoint, you can position content anywhere on the canvas. Even better, it has a simple, built-in system for categorizing and organizing information using tabs and pages. You can quickly create links to another page, section, or even notebooks. The bad news: Microsoft has ended development on the product as of OneNote 2016. They have "replaced" it with a free version. The new one adds several glitzy features, but does not allow saving files locally, will not open files created in the desktop version, and does not have a printing feature. So, for as long as you have access to the desktop version, you have one great tool.

A few other ideas:

- **Microsoft Word.** It has several features in common with OneNote. It's more difficult to organize and does not have the same free-form layouts, but almost everyone knows how to use it and you can work around its shortcomings.

- **Online Markdown sites.** You can use something like GitHub. They are automatically safe from anything that happens to your site, you can configure access control with two-factor authentication, Markdown is easy to learn, and such sites have exceptional organization and change history tracking.
  The downsides is that non-technical, and even some technical, users do not easily understand how to use them.

- **Purpose-built applications.** Several software makers sell software designed specifically for documenting IT projects. These might also present some difficulty for non-technical users, so make sure to vet them carefully.

Whatever you choose, make certain that it fits your goals.

You will also want to acquire software for taking screenshots. Building good documentation requires plentiful visual examples. Windows 10 includes its own powerful snipping tool. You can download the open source program Greenshot, which has several convenient features, such as "Capture last region", which is extremely helpful when taking screenshots of wizard pages. You can also choose from a few high-quality paid screen capturing tools.

SAMPLE BACKUP DOCUMENTATION FOR A SMALL ORGANIZATION

You can use this sample as a starting point for building your own documentation. It was designed with smaller organizations in mind, particularly those without a dedicated IT department and not enough staff to ensure that someone that has experience with the backup system will be available in a disaster recovery scenario.
Everything in this sample is fictional; it does not use any real-world devices or programs.

BACKUP AND RESTORE PROCEDURE FOR ABC, LLC

Last update: August 1, 2020

This document outlines the organization's configuration and restore procedures.

Hardware Information

- Manufacturer: .....
- Device type: .....
- Model name: .....
- Support telephone: .....
- Support e-mail: .....
- Sales/representative name: .....
- Sales/representative contact: .....
- Website: .....
- Site login information in company key vault
- Original device warranty expiration date: .....

Connection steps:

1. Choose a physical Windows Server system that will operate the backup
2. Download the latest device driver from: .....
3. Install the driver << include screenshots >>
4. Use the included cable to plug the device into a USB slot

Software Information

- Software manufacturer: .....
- Program name: .....
- Support telephone: .....
- Support e-mail: .....
- Sales/representative name: .....
- Sales/representative contact: .....
- Website: .....
- Site login information in company key vault
- License expiration date: .....

Installation steps:

1. Download latest version from: .....
2. Select a physical Windows Server system to operate the software
3. Run downloadfile.exe
4. Click **Next** on the first page

   << include a screenshot >>
5. Install to the default location

<< include a screenshot >>

6. Click **Finish** to install

<< include a screenshot >>

Notes on problems encountered during installation and workarounds:

.....

.....

Steps to connect to cloud account:

1. Open the program from Start menu with the icon

<< include a screenshot >>

2. Enter the login information for a local administrator account
3. Go to the **Cloud Account** section

<< include a screenshot >>

4. Enter our login information from the company key vault

Data restoration steps:

1. Open the program from the Start menu with the icon

<< include a screenshot >>

2. Enter the login information for a local administrator account
3. Go to the **Restore** section
4. Navigate through the tree to find the data that you want to restore, or click the check box at the top left to restore everything

<< include a screenshot >>

5. Choose where to restore following the screenshot below

<< include a screenshot of the selections that you made >>

6. Click the **Restore** button

Backup configuration steps:

1. Open the program from the Start menu with the icon

<< include a screenshot >>

2. Enter the login information for a local administrator account
3. Go to the **Backup** section
4. Click the checkboxes next to C: and D: to select everything

<< include a screenshot >>

5. Click the **Schedule** button
6. Set **Full backup** to **Saturdays, 9 PM**

<< include a screenshot >>

7. Set **Incremental backup** to **Sunday-Friday, 9 PM**

<< include a screenshot >>

8. Set the primary destination to the hardware device and the secondary destination to our cloud account, set up during installation

   << include a screenshot >>

As you look through the template, take note of all the places that might stop a non-technical user. What is a Windows Server? Where do they get one? What hardware devices do we need in functioning order to perform disaster recovery? Who can they call for procedural assistance?

We will look more closely at some of these procedures in part three of The Backup Bible. However, you need to start thinking about how you will address such questions with your users. Start with some training sessions for a few key operators.

While creating your documentation, use screenshots liberally. Even technical people find them helpful when working with unfamiliar software.

SAMPLE BACKUP DOCUMENTATION FOR A LARGER ORGANIZATION

Larger organizations typically have their own templates for project documentation. Follow those guidelines first if they exist. If not, you can start with the above template for smaller organizations. You need to preserve the same fundamental information.

Large organizations typically have differences from smaller companies in their documentation:

- A greater likelihood of available technical staff during a disaster recovery operation
- Single-process recovery documentation usually does not suffice. Categorize documentation along department, application, environment, or any other delineations that make sense
- Ability to safely keep copies in multiple on-premises locations

You can use this template to help you build or augment your documentation. Everything in this sample is fictional; it does not use any real-world devices or programs.

BACKUP AND RESTORE PROCEDURE FOR ZYX CORP

Last update: August 1, 2020

This document outlines the organization's foundational configuration and restore procedures.

Hardware Information

- Manufacturer: .....
- Device type: .....
- Model name: .....
- Support telephone: .....
- Support e-mail: .....
- Sales/representative name: .....
- Sales/representative contact: .....
- Website: .....
- Site login information in company key vault
- Original device warranty expiration date: .....

Departments/applications/environments/etc. that use this device

Location	Purpose

Connection steps:

1. Choose a physical Windows Server system that will control the device
2. Download the latest device driver from: _____
3. Install the driver << include screenshots >>
4. Use the included cable to plug the device into a USB slot

Backup Software Information

- Software manufacturer: .....
- Program name: .....
- Support telephone: .....
- Support e-mail: .....
- Sales/representative name: .....
- Sales/representative contact: .....
- Website: .....
- Site login information in company key vault
- License expiration date: .....

Hardware targets used by this program:

.....

.....

Network targets used by this program:

.....

.....

Cloud targets used by this program:

.....

.....

Installation steps:

1. Download latest version from: .....
2. Select a physical Windows Server system to operate the software
3. Run downloadfile.exe
4. Click **Next** on the first page

   << include a screenshot >>
5. Install to the default location

   << include a screenshot >>
6. Click **Finish** to install

   << include a screenshot >>

Notes on problems encountered during installation and workarounds:

.....

.....

Steps to connect to device:

1. Open the program from Start menu with the icon

   << include a screenshot >>
2. Enter the login information for a local administrator account
3. Go to the Devices section

   << include a screenshot >>
4. Select the device

Steps to connect to cloud account:

1. Open the program from Start menu with the icon

   << include a screenshot >>
2. Enter the login information for a local administrator account
3. Go to the **Cloud Account** section

   << include a screenshot >>
4. Enter our login information from the company key vault

General data restoration steps:

1. Open the program from the Start menu with the icon

   << include a screenshot >>
2. Enter the login information for a local administrator account
3. Go to the Restore section

4. Navigate through the tree to find the data that you want to restore, or click the check box at the top left to restore everything

   << include a screenshot >>

5. Choose where to restore following the screenshot below

   << include a screenshot of the selections that you made >>

6. Click the Restore button

Backup configuration steps:

1. Open the program from the Start menu with the icon

   << include a screenshot >>

2. Enter the login information for a local administrator account

3. Go to the **Backup** section

4. Click the checkboxes next to C: and D: to select everything

   << include a screenshot >>

5. Click the **Schedule** button

6. Set **Full backup** to **Saturdays, 9 PM**

   << include a screenshot >>

7. Set **Incremental backup** to **Sunday-Friday, 9 PM**

   << include a screenshot >>

8. Set the primary destination to the hardware device and the secondary destination to our cloud account, set up during installation

   << include a screenshot >>

Application 1 Restore Information

Use these steps to restore Application 1:

1. Install Microsoft SQL Server 2017 using our baseline configuration
2. Have a new Windows Server 2019 host ready
3. Follow the general data restoration steps for backup program 1
4. Pick the Application 1 database as a source

   << include a screenshot >>

5. In the restore target dialog box, choose the database server from step 1

   << include a screenshot >>

6. Restore the database
7. Restart the general data restoration steps
8. Pick the name of the original Application 1 application server as a source

   << include a screenshot >>

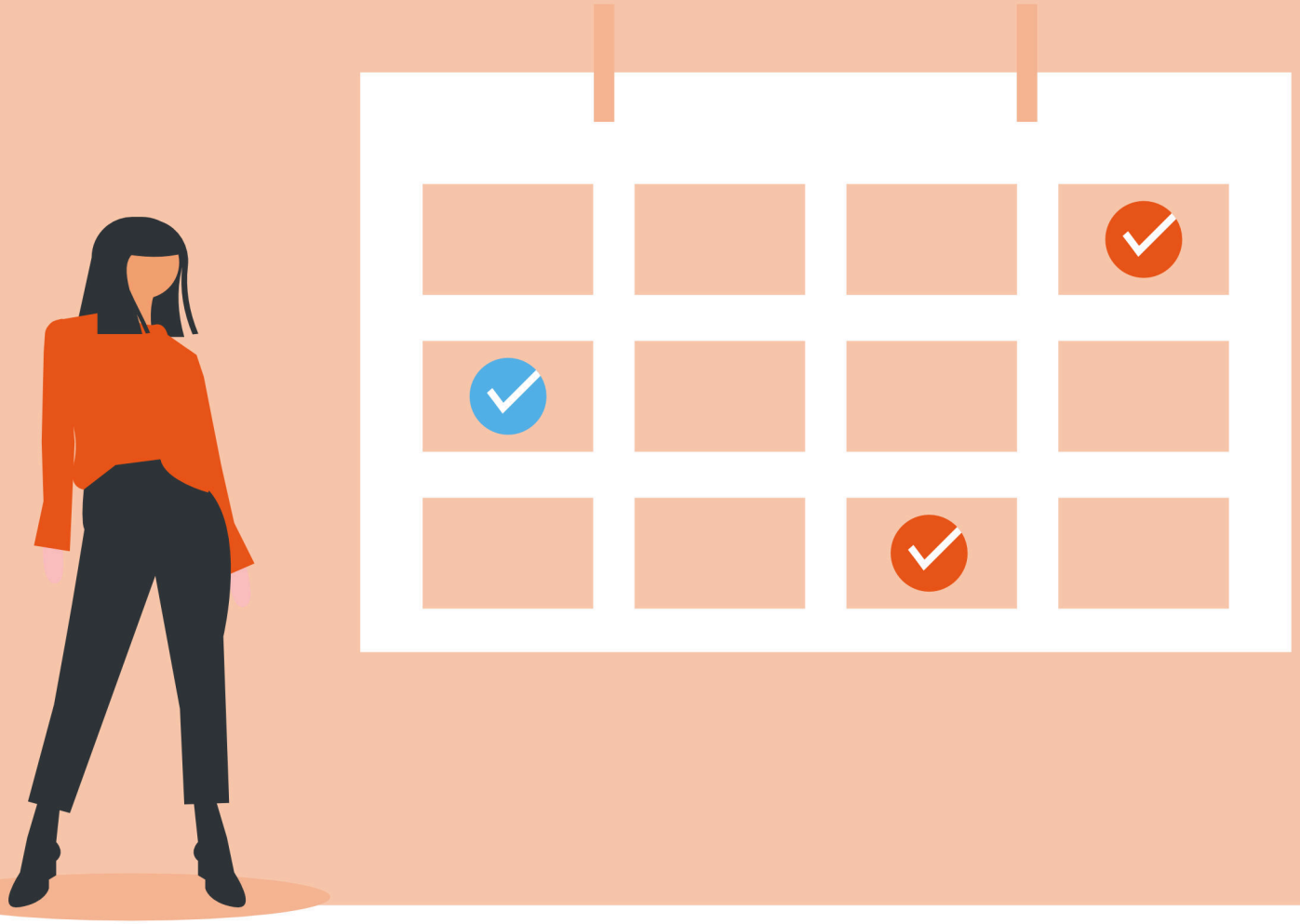
9. Pick the name of the new server from step 2 as the target

   << include a screenshot >>

10. Restore the application
11. Start the “Application 1” service on the restored server
12. Test functionality and connectivity

You will need to duplicate portions of this template to cover as many applications as necessary. You might need to create site-specific.

DEFINING BACKUP SCHEDULES



Now you understand your organization's data protection needs and you have the means to implement. To bring it to life, you need to design the schedules for your backups. Unless you have very little data or a high budget for backup, you will use more than one schedule. You will use three metrics: value, frequency of change, and application features.

UNDERSTANDING HOW THE VALUE OF DATA AFFECTS BACKUP SCHEDULING

The frequency of your full backup schedule directly determines how many copies of data that you will have over time. The more copies you have of any given bits, the greater the odds that at least one copy will survive catastrophe. So, if you have data that you cannot lose under any circumstances, then your schedule should reflect that.

UNDERSTANDING HOW THE FREQUENCY OF CHANGE AFFECTS BACKUP SCHEDULING

Data that changes frequently may need an equally frequent backup. As you recall from part one, recovery point objectives (RPO) set the maximum amount of time between backups, which establishes the boundaries of how much recent data you can lose. You must also consider how often that data changes independently of RTO.

If you have data that does not change often, then you might consider a longer RPO. If you only modify an item every few months, then it might not make sense to back it up every week. However, that might have unintended consequences. As an example, you set a monthly-only schedule for your domain controller because you rarely have staff turnover and only replace a few computers per year. Then, you hire a new employee and supply them with a PC the day after a backup. If anything happens to Active Directory during that month, then you will lose all that information. Your schedule needs to consider such possibilities.

UNDERSTANDING HOW BACKUP APPLICATION FEATURES AFFECT SCHEDULING

You will find that modern commercial backup applications have more in common than different. They all have some way to schedule jobs. Each one uses some way to optimize backups. The exact features in the solutions that you use will influence how you schedule.

The following list provides a starting point for you to determine how to leverage the features in your selected program:

- **Virtual machine awareness:** If your backup software understands how to back up virtual machines, then you can allow it to handle efficient ordering. If not, then you will need to schedule to back up the guest operating systems such that the jobs do not overwhelm your resources.

- **Space-saving features:** If your backup tool can preserve storage space, that has obvious benefits. Everything involves tradeoffs – ensure that you know what you give up for that extra space. Some common considerations:

    - Traditional differential and incremental backups complete more quickly than the full backups they depend on. They mean nothing without their source full backup. Design your schedule to accommodate full backups as time and space allow.
    - Newer delta and deduplication techniques save even more space than differential and incremental jobs but require calculation and tracking in addition to the requisite full backups. They should not use significant CPU time, but you need to test it. Also check to see if and how your application tracks changes. Some will use space on your active disks.
    - If you have extra space in your storage media, then do not depend overly on these technologies. Create more full backups if you can.

- **Time-saving features:** Many of the features in the previous bullet point save time as well as space. As with space, do not try to save time that you do not require.

- **Replication:** Replication functions require bandwidth, which can cause severe bottlenecks when crossing internet links. If a replication job does not complete before the next job begins, then you might end up with unusable backups.

- **Media types:** Due to the wide variance in performance of the various backup media types, the option(s) that you choose will determine how you schedule backups and what space-saving features they use. For instance, if you need to back up several terabytes to tape and a full backup requires twelve hours to perform, then you will only run a full backup when you have twelve hours available.

- **Snapshot features:** If your backup application integrates with VSS or uses some other technique to take crash-consistent or application-consistent backups, then you have greater scheduling options. Backup uses system resources and you do not want one job to conflict with another, but snapshotting allows you to run backups while systems are in use.

You should have become fully acquainted with your backup program during the deployment phase. Take the time to learn how your backup program operates. Keep in mind the need for periodic full backups.

PUTTING IT IN ACTION

Remember that, if possible, you would take a complete backup of all your data at least once per day. Since that would quickly exceed any rational quantity of time and media, you must make compromises.

Guidelines for backup scheduling:

- Full backups need time and resources, even with non-interrupting snapshot technologies. Try to schedule them during low activity periods.
- Full backups do not depend on other backups. Therefore, they have greatest value after major changes. As an example, some organizations have intricate month-end procedures. Taking a backup immediately afterward could save a lot of time in the event of a restore.
- Incremental, differential, delta, and deduplicated backups require relatively little time and space compared to full backups, but they depend on other backups. Use them as fillers between full backups.
- If your backup scheme primarily uses online storage, make certain to schedule backups to offline media. If that is a manual process, implement an accountability plan.
- Just as administrators tend to perform backups at night, they also like to schedule system and software updates at night. Ensure that schedules do not collide.

GRANDFATHER-FATHER-SON SAMPLE PLAN

"Grandfather-father-son" (GFS) schemes are very common. They work best with rotating media such as tapes. One typical example schedule:

- **"Grandfather"**: full backup taken once monthly. Grandfather media is rotated annually (overwrite the January 2020 tape with January 2021 backup, February 2020 with February 2021 data, etc.). One "grandfather" type per year, typically the one that follows your organization's fiscal year end, is never overwritten, following data retention policy.
- **"Father"**: full backup taken weekly. "Father" media is rotated monthly (i.e., you have a "Week 1" tape, a "Week 2" tape, etc.).
- **"Son"**: incremental or differential backups are taken daily and their media overwritten weekly (i.e., you have a "Monday" tape, a "Tuesday" tape, etc.).

The above example is not the only type of GFS scheme. The general rotation practice is how it qualifies. You have one set of very long-term full media, one shorter-lived set of full media, and rapidly rotated media. Some implementations do not keep the annual media. Others do not rotate the monthly full, instead keeping them for the full backup retention period. Some do not rotate the daily media every week. Your organization's needs and budget dictate your practices.

With a GFS scheme, you are never more than a few pieces of media away from a complete restore. Remember that a "differential" style backup needs the latest "son" media and the "father" immediately preceding whereas an "incremental" style backup needs the latest "father" media and all of its "sons".

The downside of a GFS scheme is that you quickly lose the granular level of daily backups. Once you rotate the daily, then you can only go to the most recent monthly or perhaps an annual backup. The greatest risk is to data that is created and destroyed between full backup cycles.

ONLINE MEDIA SAMPLE PLAN

If your backup solution uses primarily online media, then the venerated GFS approach might not work well. Most always-online systems do not have the same concept of "rotation". Instead, they age out old data once it reaches a configured retention policy expiration period.

For these, your configuration will depend on how your backup program stores data. If it uses a deduplication scheme and only keeps a single

full backup, then you have little to do except configure backup frequency and retention policy. Due to the risks posed by having only one complete copy of your data, you must enforce periodic full backups to offline media. You should also consider some form of replication, whether to the cloud or an alternative working site.

CONTINUOUS BACKUP SAMPLE PLAN

Many applications have some form of "continuous" backup. They capture data in extremely small time increments. As an example, Altaro VM Backup has a "Continuous Data Protection" (CDP) feature that allows you to set a schedule as short as five minutes.

Scheduling these types of backups involves three considerations:

- How does the backup application store the "continuous" backup data?
- How quickly does the protected data change?
- How much does the protected data change within the target time frame?

If your backup program takes full, independent copies at each interval, then you could run out of media space very quickly. If it uses a deduplication-type storage mechanism, then it should use considerably less. Either way, your rate of data churn will determine how much space you need.

For systems with a very high rate of change, your backup system might not have sufficient time to make one backup before the next starts. That can lead to serious problems, not least of which is that it cannot provide the continuous backup that you want.

You can easily predict how some systems will behave; others need more effort. You may need to spend some time making a setting, watching how it performs, and adjusting.

MIXED BACKUP PLAN EXAMPLE

You do not need to come up with a one-size-fits-all schedule. You can set different schedules. Use your RTOs, RPOs, retention policies, and capacity limits as guidance.

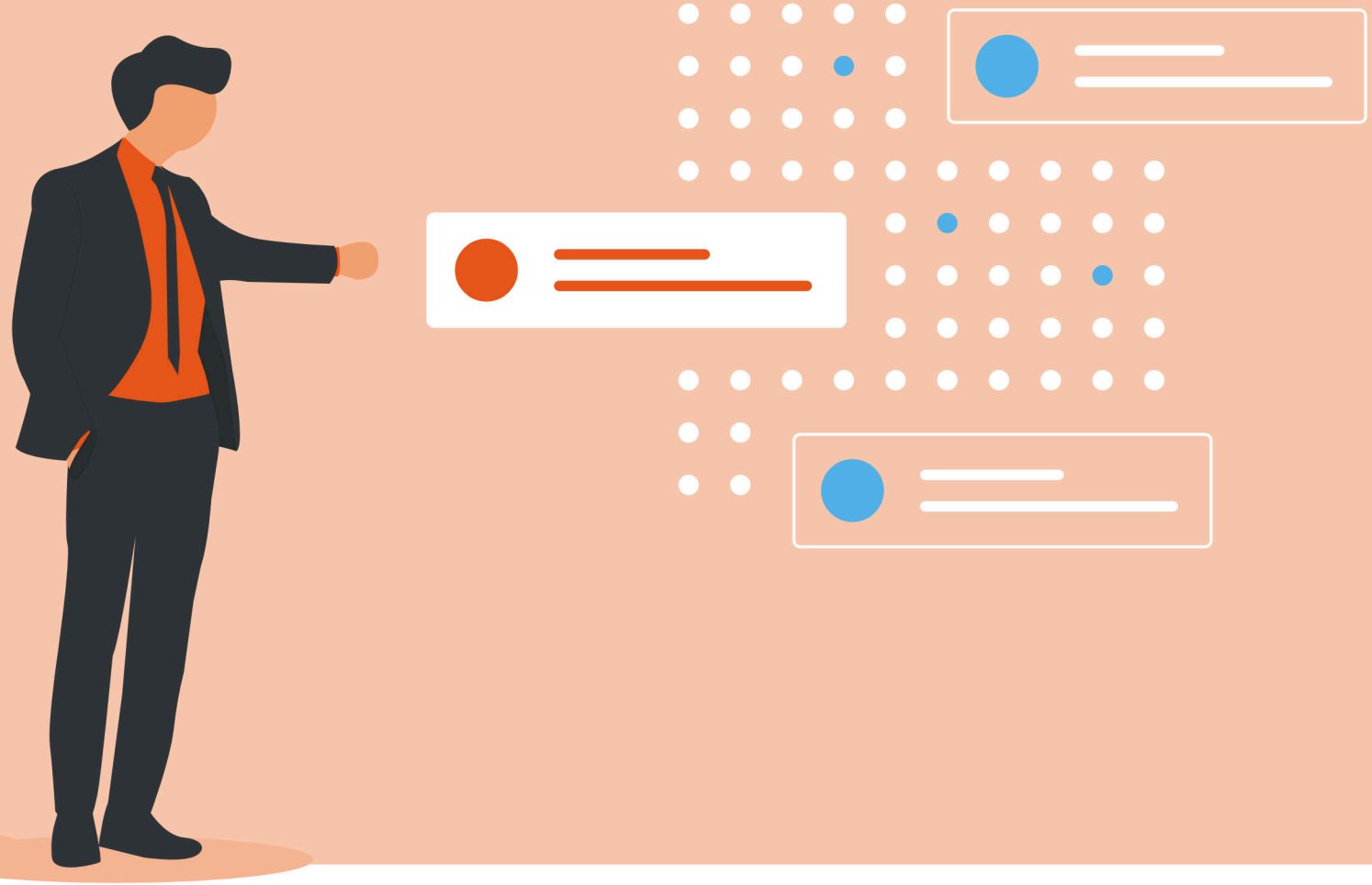
One possibility:

- Domain controllers: standard GFS with one-year retention
- Primary line-of-business application server (app only): monthly full, scheduled after operating system and software updates, with three-month retention

- Primary line-of-business database server: continuous, six-month retention
- Primary file server: standard GFS with five-year retention
- E-mail server: uses a different backup program that specializes in Exchange, daily full, hourly differential, with five-year retention
- All: replicated to remote site every day at midnight
- All: monthly full offline, following retention policies

“ REMEMBER TO DOCUMENT EVERYTHING! “

MONITORING AND TESTING YOUR BACKUPS



As you might expect, setting up backup is just the beginning. You will need to keep it running into perpetuity. Similarly, you cannot simply assume that everything will work. You need to keep constant vigilance over the backup system, its media, and everything that it protects.

MONITORING YOUR BACKUP SYSTEM

Start with the easiest tools. Your backup program almost certainly has some sort of notification system. Configure it to send messages to multiple administrators. If it creates logs, use operating system or third-party monitoring software to track those as well. Where available, prefer programs that will repeatedly send notifications until someone manually stops it or it detects problem resolution.

Set up a schedule to manually check on backup status. Partially, you want to verify that its notification system has not failed. Mostly, you want to search through job history for things that didn't trigger the monitoring system. Check for minor warnings and correct what you can. Watch for problems that recur frequently but work after a retry. These might serve as early indications of a more serious problem.

TESTING BACKUP MEDIA AND DATA

You cannot depend on even the most careful monitoring practices to keep your backups safe. Data at rest can become corrupted. Thieves, including insiders with malicious intent, can steal media. You must implement and follow procedures that verify your backup data.

Keep an inventory of all media. Set a schedule to check on each piece. When you retire media due to age or failure, destroy it. Strong magnets work for tapes and spinning drives. Alternatively, drill a hole through mechanical disks to render them unreadable. Break optical media and SSDs any way that you like.

Organizations that do not track personal or financial information may not need to keep such meticulous track of media. However, anyone with backup data must periodically check that it has not lost integrity. The only way you can ever be certain that your data is good is to restore it. Establish a regular schedule to try restoring from older media. If successful, make spot checks through the retrieved information to make sure that it contains what you expect.

PUTTING IT IN ACTION

The activities in this section will take time to set up and perform. Do not allow fatigue to prevent you from following these items or tempt you into putting them off.

- Configure your backup system to send alerts on failed jobs at least
- Establish an accountability for manually verifying that the backup program is functioning on a regular basis
- Configure a monitoring system to notify you if your backup software ceases running
- Establish a regular schedule and accountability system to test that you can restore data from backup. Test a representative sampling of online and offline media.

Monitoring backup, especially testing restores, is admittedly tedious work. However, it is vital. Many organizations have suffered irreparable damage because they found out too late that no one knew how to properly restore data. Too many do not realize until they've lost everything that their backup media did not successfully preserve anything.

Some have had backups systems sit in a failed state for months without discovering it. A few minutes of occasional checking can prevent such catastrophes.

MAINTAINING YOUR SYSTEMS

Much of the material in this section exceeds the typical scope of a business continuity plan. When you consider that your primary goal is data protection, then it makes sense to think beyond backup programs and hardware. Furthermore, all the components of your backup belong to your larger technological environment, so you maintain it accordingly.

Fortunately, you can automate common maintenance. Windows will update itself over the internet. The package managers on Linux distributions have the same ability. Windows also allows you to set up an update server on-premises to relay patches from Microsoft. Similarly, you can maintain internal repositories to keep your Linux systems and programs current. In addition to the convenience that such in-house systems provide, you can also leverage them as a security measure. You can automatically update systems without allowing them to connect directly to the internet.

In addition to software, keep your hardware in good working order. Of course, you cannot simply repair modern computer boards and chips. Instead, most manufacturers will offer a replacement warranty of some kind. If you purchase fully assembled systems from a major systems vendor, such as Dell or Hewlett-Packard Enterprise, they offer warranties that cover entire systems as a whole. They also have options for rapid delivery or in-person service by a qualified technician. If at all possible, do not allow out-of-warranty equipment to remain in service.

PUTTING IT IN ACTION

Most operating systems and software have automated or semi-automated updating procedures. Hardware typically requires manual intervention. It is on the system administrators to keep current.

- Where available, configure automated updating. Ensure that it does not coincide with backup, or that your backup system can successfully navigate operating system outages.
- Establish a pattern for checking for firmware and driver updates. These should not occur frequently, so you can schedule updates as one-off events.
- Monitor the Internet for known attacks against the systems that you own. Larger manufacturers have entries on common vulnerabilities and exposures (CVE) lists. Sometimes they maintain their own, but you can also look them up at: https://cve.mitre.org/. Vendors usually release fixes in standard

patches, but some will issue “hotfixes”. Those might require manual installation and other steps.

- If your hardware has a way to notify you of failure, configure it. If your monitoring system can check hardware, configure that as well. Establish a regular routine for visually verifying the health of all hardware components.

Maintenance activities consume a large portion of the typical administrator’s workload, so these procedures serve as a best practice for all systems, not just those related to backup. However, since your disaster recovery plan hinges on the health of your backup system, you cannot allow it to fall into disrepair.

WHAT’S NEXT

Reading this part of The Backup Bible is just the beginning. You have quite a lot of work ahead with testing, deploying, documenting and testing some more. Do not hurry through any of this. It might be years before you need to call this system into recovery action – if ever. You need to ensure that it works flawlessly if that day ever comes.

In the third and final part of The Backup Bible, we will look at that process. You will gain insights into the disaster recovery process. You can use that to help you prepare for the worst.

ALTARO BACKUP

HYPER-V | VMWARE | PHYSICAL | OFFICE 365

Hyper-V & VMware Backup & Replication

For Companies

Award-winning virtual machine (VM) backup and replication solution for Hyper-V and VMware environments

Learn more

For MSPs

Monthly subscription program enabling Managed Service Providers to offer Hyper-V, VMware and physical server backup services

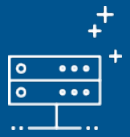
Learn more

Physical Server Backup

Back up the physical servers on your network through this P2V solution and benefit from fast and easy recovery should they be impacted by a disaster

Learn more

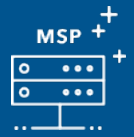
Office 365 Backup



For Companies

Office 365 mailbox backup and recovery solution with centralized backup management and storage to Altaro's Microsoft Azure infrastructure

Learn more



For MSPs

Monthly subscription program enabling Managed Service Providers to provide Office 365 mailbox backup, recovery and backup management services

Learn more

50,000+ Customers

10,000+ Partners

2,000+ MSPs

121 Countries

MORE GREAT IT CONTENT

Continue your learning on the Altaro Dojo, our dedicated learning platform for IT professionals:

FOLLOW ALTARO AT:

SHARE THIS RESOURCE!

Liked the eBook? Share it now on:

ALTARO BACKUP

PUBLISHED BY ALTARO SOFTWARE

https://www.altaro.com/

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

FEEDBACK INFORMATION

We’d like to hear from you! If you have any comments about how we could improve the quality of this book, please don’t hesitate to contact us by visiting www.altaro.com or sending an email to our Customer Service representative Sam Perry: sam@altarosoftware.com