



# SANTA'S ELVES

*Joy's and Plastics*

NOS 230 Fall 2023 Presentation  
Presented by  
Elliott Richter & Anthony Manenti

# Overview of Contents

1. Your Presenters
2. Who is SETAP?
3. Setting up the servers
4. Creating the DC and Domain
5. Setting up the HV
6. NOS Desktops & RSAT
7. Building the Active directory OUS and Security groups
8. Importing the Users and creating the home folders
9. Setting up the HV server
10. Setting up the File server
11. Mapping drives and setting up shares
12. Home folder visibility and access
13. Management folders
14. Creating GPOs & file redirection
15. Auditing the Domain
16. Generating a Baseline for the DC server
17. Backing up the server
18. Problems and solutions along the way
19. User Access Demonstration

# Your Presenters :

Elliott Richter

- Cloud Admin and Support Dual Degree Programs
- Working with servers for 1.5 years
- Freelance Computer Tech for 3 decades
- Enjoys prototyping, kayaking, hiking, 3D Printing, Drafting, Riding Motorcycles



Anthony Manenti

- Cloud and IT Systems Administration Degree Program
- Working as Software Engineer for 3 Years (MERN and Ruby on Rails)
- Worked in Computer Repair for about a decade.
- Enjoys Bikepacking, Playing Guitar, Legos, and the Outdoors





*What is SETAP?*

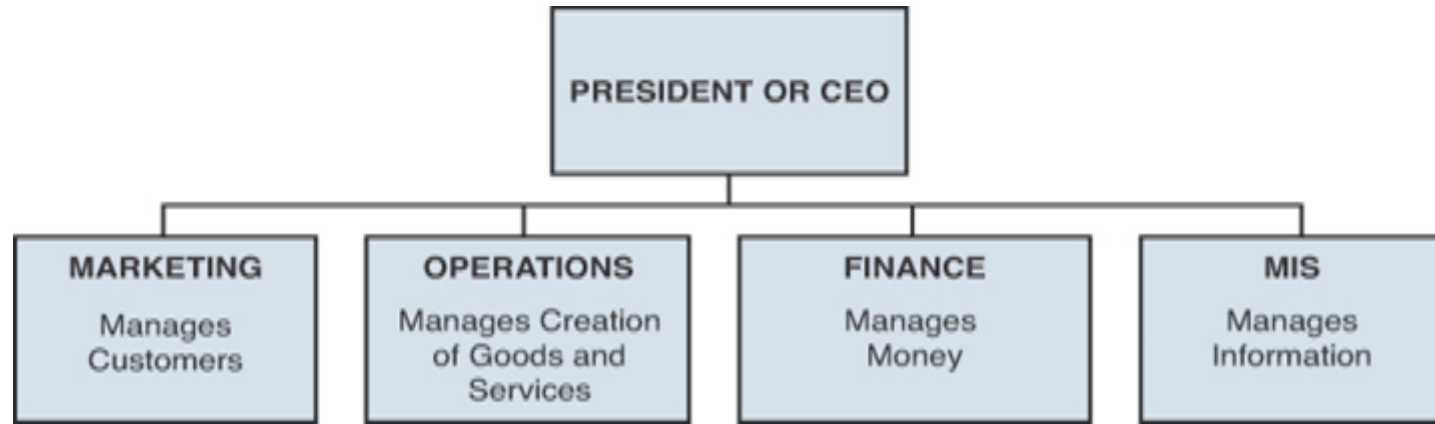
# Who exactly is SETAP?

- Organization that specializes in and produces Fine Toys and Custom Molded Plastics.
- Located out of the Northern Arctic Region
- Currently has 1 Main Facility / Production plant
- Busiest Production Season is in the Winter
- Corporate Branches has Representatives located in Malls near you
- Global Distributors with customers in every country
- 206 Employees over 11 Departments
- High quality production with rapid turnaround times at a price that is highly affordable.

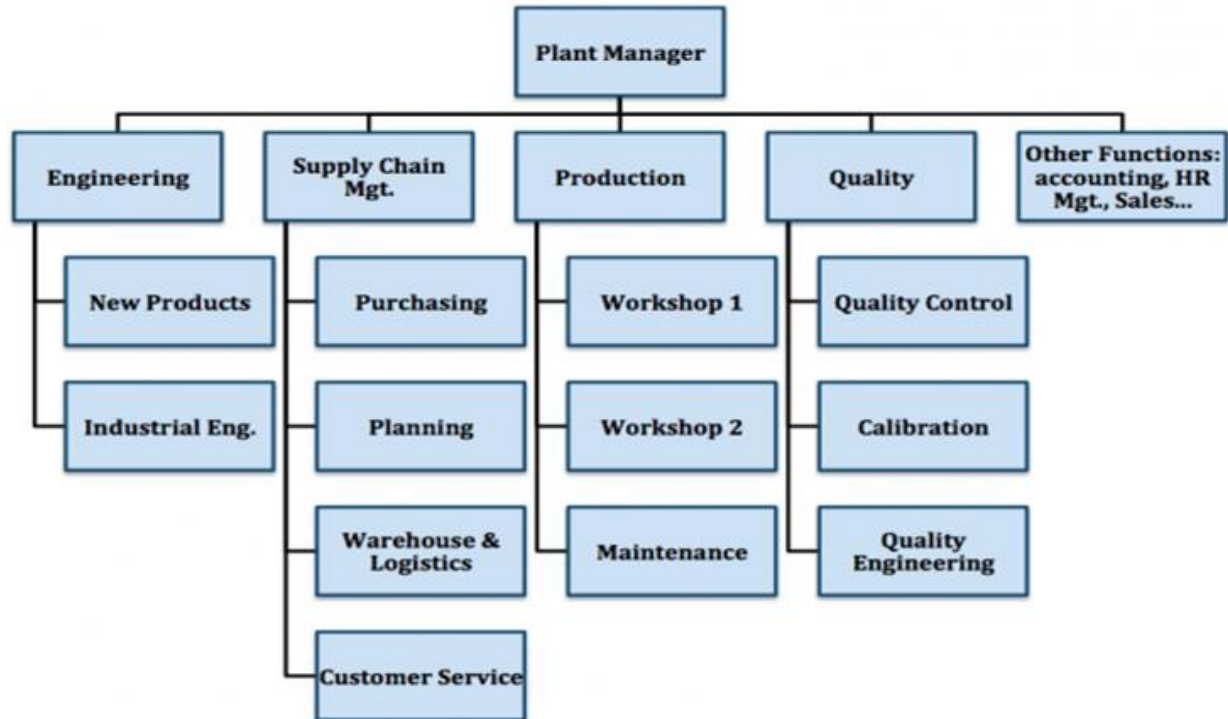


***“Quality So Good, You’d Think It Was Christmas Every Day!”***

# Company Organization: The Top Brass



# Company Organization: The Plant





# *The SETAP Domain*



# Setting up the Domain -AD DC Server

- First setting the static IP address and subnet
- Configuring Windows Update to download, but not install updates.
- Setting up Firewall
- Setting proper sharing permissions
- Setting up the domain and registering this as the DC

# Setting up the Domain -AD DC Server

- Setting up the Administrative Accounts and changing the “Administrator” name
- Recheck configuration of Windows Update to download, but not install updates through server manager.
- Set DSRM recovery password and
- Began Installing Active Directory and Management tools

# Setting up the Domain -AD DC Server

- Installing Active Directory using the Server Manager - Add roles and features wizard
- Creating the forest and domain and Promoting the server to Domain Controller
- Making the domain controller discoverable on the domain
- Enabling Remote Desktop Connections to authorized domain admins
- Server/Network Information on following slide

# Our Servers:

The screenshot displays the Windows Server Manager interface for a local server named SanElvAD-DC1. The left-hand navigation pane lists various server roles and services, including Local Server, All Servers, AD DS, DNS, File and Storage Services, IIS, NPAS, Print Services, and WSUS. The main area is divided into three sections: PROPERTIES, EVENTS, and SERVICES.

**PROPERTIES**  
For SanElvAD-DC1

Computer name	SanElvAD-DC1	Last installed updates	11/12/2023 2:10 PM
Domain	setap.com	Windows Update	Download updates only, using Microsoft Update
		Last checked for updates	Today at 9:44 AM
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-05:00) Eastern Time (US & Canada)
Ethernet0	10.16.230.110, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2019 Datacenter	Processors	Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
Hardware information	VMware, Inc. VMware7,1	Installed memory (RAM)	16 GB
		Total disk space	79.4 GB

**EVENTS**  
All events | 72 total

Server Name	ID	Severity	Source	Log	Date and Time
SANELVAD-DC1	8198	Error	Microsoft-Windows-Security-SPP	Application	11/26/2023 10:07:27 AM
SANELVAD-DC1	1085	Warning	Microsoft-Windows-GroupPolicy	System	11/26/2023 10:07:23 AM
SANELVAD-DC1	502	Error	Microsoft-Windows-Folder-Redirection	Application	11/26/2023 10:07:23 AM
SANELVAD-DC1	6006	Warning	Microsoft-Windows-Winlogon	Application	11/26/2023 9:47:21 AM
SANELVAD-DC1	5781	Warning	NETLOGON	System	11/26/2023 9:45:42 AM
SANELVAD-DC1	5781	Warning	NETLOGON	System	11/26/2023 9:45:42 AM
SANELVAD-DC1	5781	Warning	NETLOGON	System	11/26/2023 9:45:42 AM

**SERVICES**  
All services | 231 total

Server Name	Display Name	Service Name	Status	Start Type
SANELVAD-DC1	Application Layer Gateway Service	ALG	Stopped	Manual
SANELVAD-DC1	Application Identity	AppIDSvc	Stopped	Manual (Triggered)
SANELVAD-DC1	Application Management	AppMgmt	Stopped	Manual

Our ADDC Server -  
SanElvAD-DC1

# SANELVAD-DC1 Server Info:

Domain Name: setap.com

IP Range: 10.16.230.110-120

Computer Name: SanElvAD-DC1

Physical Address: 00-50-56-82-2E-19

DNS Server: 127.0.0.1

Secondary DNS: 192.168.18.6

Default Gateway: 10.16.0.1

Subnet Mask: 255.255.0.0

Main Administrator Password:

-Redacted-

Restore (disaster) Password:

-Redacted-

Operating System: MS Server 2019  
DataCenter

Hardware: Dell Inc. PowerEdge R620

Processors: Intel® Xeon® CPU

E5-2680 0 @ 2.7GHz,

Installed RAM: 16 GB

Total Disk Space: 79.3 GB

Windows Firewall: Domain:On

Remote Management: On

Remote Desktop: Enabled

# Setting up the Domain - Hyper-V Server

- Once DC was up and running, we could connect the HV to the domain
- Configured Network adapters with static IP
- Made the server domain discoverable
- Installed Active Directory with server manager wizard
- Connected to existing domain using advanced settings tab in PC Name options
- Installed Hyper V roles and features with server manager wizard
- Server information is on the following slides

# Our Servers:

## Our HyperV Server - SanElv-HV

The screenshot displays the Windows Server Manager interface for a HyperV Server named SanElv-HV. The interface is divided into several sections:

- Server Manager:** Shows the server name (SanElv-HV) and domain (setap.com). It also displays the last installed updates (10/21/2023 10:38 AM) and the last checked for updates (Today at 9:46 AM).
- Windows Defender Firewall:** Shows the firewall status (Public On, Private On) and the Remote Desktop status (Enabled).
- Windows Defender Antivirus:** Shows the antivirus status (Real-Time Protection: On) and the Windows Defender Antivirus Feedback & Diagnostics status (On).
- Network Settings:** Shows the network configuration, including the Ethernet adapter (vEthernet {Intel(R) 82574L Gigabit Network Connection #2 - Virtual Switch}) and the Ethernet adapter (vEthernet {New Virtual Switch}).
- Operating system version:** Shows the operating system version (Microsoft Windows Server 2019 Datacenter).
- Processors:** Shows the processor information (Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz).

**EVENTS**

All events | 28 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
SANELV-HV	8198	Error	Microsoft-Windows-Security-SPP	Application	11/26/2023 9:49:44 AM
SANELV-HV	1014	Warning	Microsoft-Windows-DNS Client Events	System	11/26/2023 9:42:11 AM
SANELV-HV	1014	Warning	Microsoft-Windows-DNS Client Events	System	11/26/2023 9:41:58 AM
SANELV-HV	8020	Warning	Microsoft-Windows-DNS Client Events	System	11/26/2023 9:41:51 AM
SANELV-HV	8020	Warning	Microsoft-Windows-DNS Client Events	System	11/26/2023 9:41:49 AM
SANELV-HV	10154	Warning	Microsoft-Windows-Remote Management	System	11/26/2023 9:41:49 AM
SANELV-HV	1129	Error	Microsoft-Windows-GroupPolicy	System	11/26/2023 9:41:48 AM

**SERVICES**

All services | 212 total

Filter

Server Name	Display Name	Service Name	Status	Start Type
SANELV-HV	Wired AutoConfig	dot3svc	Stopped	Manual
SANELV-HV	Microsoft App-V Client	AppVClient	Stopped	Disabled
SANELV-HV	Windows Remote Management (WS-Management)	WinRM	Running	Automatic
SANELV-HV	Smart Card Removal Policy	SCPolicySvc	Stopped	Manual

# SANELV-HV Server Info:

Domain Name: setap.com

IP Range: 10.16.230.110-120

Computer Name: SanElv-HV

Ethernet0

IP Address: 10.16.230.111

Physical Address:

00-50-56-82-F0-2E

DNS Server: 10.16.230.110

Secondary DNS: 192.168.18.6

Default Gateway: 10.16.0.1

Subnet Mask: 255.255.0.0

Ethernet1

IP Address: 10.16.230.112

Physical Address: 00-50-56-  
82-BA-0E

DNS Server: 10.16.230.110

Secondary DNS: 192.168.18.6

Default Gateway: 10.16.0.1

Subnet Mask: 255.255.0.0

Operating System: MS Server 2019  
DataCenter

Hardware: Dell Inc. PowerEdge R620

Processors: Intel® Xeon® CPU  
E5-2680 0 @ 2.7GHz,

Installed RAM: 32 GB

Total Disk Space: 199.4 GB

Windows Firewall: Domain:On

Remote Management: On

Remote Desktop: Enabled





# *RSAT and NOS Desktops*

# Setting up the Domain - NOS Desktops

- Renaming the computers using Advanced Settings in PC name
- Configuring the Network Settings
- Configuring the Remote Desktop Settings
- Making the Computer Discoverable on the Domain/Network
- Connecting the Desktop to the Domain

# RSAT & Remote Desktop Setup and Demonstration

Setting up RSAT and Remote Desktop on the server

- Setting up RSAT (Remote Server Admin Tools)
- Verified version we needed and installed from Microsoft
- Configured Desktops and Connected them to Domain using advanced settings in PC Name window
- Installed RSAT and enabled it under the Windows Administrator Tools
- Active Directory can now be used on the desktops
- Login just like on the domain servers with SETAP\ (and the username here)

Demonstration of logging into admin and client accounts from NOS Desktop Following this slide



# *A Tour of SETAP Active Directory*

# A Tour of Active Directory Setup

## Overview:

- 206 users (including admins) - using the PS1 script to automate the import method and create all home folders
- OUs for the departments
- Security groups
- Home folder creation

# AD Structure - OUs, Users, and Groups

Our Directory tree was designed after the various departments of the organization

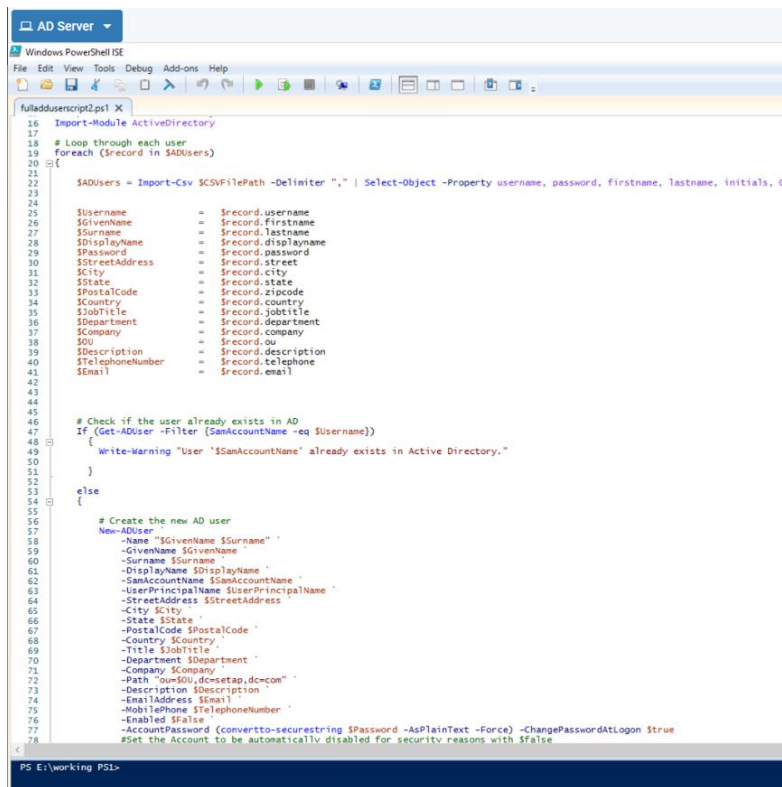
11 Departments Total

Screenshot of the OU Structure on following slide

# AD Structure - OUs, Users, and Groups

Active Directory Users and Computers				Active Directory Users and Computers			
File Action View Help				File Action View Help			
Active Directory Users and Computers [SanElv-DC1.setap.com]				Active Directory Users and Computers			
Name Type Description				Name Type Description			
<ul style="list-style-type: none"> <li>Saved Queries</li> <li>setap.com <ul style="list-style-type: none"> <li>Accounting <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Admin Staff <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Builtin <ul style="list-style-type: none"> <li>Computers</li> </ul> </li> <li>Domain Controllers</li> <li>Employee Security Groups</li> <li>Engineering <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Executives <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Facilities <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>ForeignSecurityPrincipals</li> <li>GPOTest</li> <li>Group Policies</li> <li>HR <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Managed Service Accounts</li> <li>Management <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Marketing <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>OIT <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Production <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Quality</li> </ul> </li> </ul>				<ul style="list-style-type: none"> <li>Engineering <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Executives <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Facilities <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>ForeignSecurityPrincipals</li> <li>GPOTest</li> <li>Group Policies</li> <li>HR <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Managed Service Accounts</li> <li>Management <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Marketing <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>OIT <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Production <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Quality <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Sales <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Secret Project Development <ul style="list-style-type: none"> <li>Department Groups</li> <li>Users</li> </ul> </li> <li>Supply Chain Mgt <ul style="list-style-type: none"> <li>Computers</li> <li>Department Groups</li> <li>Users</li> </ul> </li> </ul>			
Adam Dixon	User			Alisa Sullivan	User		
Adelaide Crawford	User			Alissa Allen	User		
Adrianna Scott	User			Amelia Gibson	User		
Agata Higgins	User			Annabella Stewart	User		
Agata Richardson	User			Antony Andrews	User		
Aida West	User			April Barnes	User		
Amelia Turner	User			Brad Dixon	User		
Brianna Stevens	User			Brianna Robinson	User		
Charlie Cole	User			Bruce Holmes	User		
Chester Nelson	User			Chester Morrison	User		
Connie Higgins	User			Connie Barnes	User		
Daisy Miller	User			Daryl Warren	User		
David Roberts	User			David Robinson	User		
Freddie Andrews	User			David Thomas	User		
Freddie Harper	User			Dexter Riley	User		
Freddie Perkins	User			Dominik Myers	User		
Isabella Foster	User			Dominik Thomas	User		
Jasmine Ryan	User			Eddy Adams	User		
Jasmine Walker	User			Edgar Dixon	User		
joseph.vanderbuilt	User			Eleanor Foster	User		
Julian Douglas	User			Ellia Gray	User		
Julian Stewart	User			Emma Fowler	User		
Kate Reed	User			Fiona Warren	User		
Kelsey Richardson	User			Florrie Robinson	User		
Kevin Johnson	User			Freddie Sullivan	User		
Luke Crawford	User			Gianna Taylor	User		
Lydia Ellis	User			Grace Ferguson	User		
Maddie Holmes	User			Haris Campbell	User		
Maya Gray	User			Haris Henderson	User		
Oliver Howard	User			Isabella Watson	User		
Paige Anderson	User			Jared Dixon	User		
Rafael Johnson	User			Jared Thompson	User		
Reid Foster	User			Jenna Walker	User		
Rubie Riley	User			Jessica Myers	User		
Tara Phillips	User			Justin Walker	User		
Vanessa Rogers	User			Kate Henderson	User		
Vivian Stevens	User			Kate Phillips	User		
				Kelsey Riley	User		
				Kimberly Grant	User		
				Lucia Tucker	User		
				Maya Mitchell	User		
				Melissa Campbell	User		
				Michael Roberts	User		
				Michelle Brown	User		
				Mike Bailey	User		
				Miller Richardson	User		
				Nicole Anderson	User		
				Preston Murphy	User		

# Script to Import Users and Create Home Folders



```
16 Import-Module ActiveDirectory
17
18 # Loop through each user
19 foreach ($record in $ADUsers)
20 {
21     $ADUsers = Import-Csv $CSVFilePath -Delimiter "," | Select-Object -Property username, password, firstname, lastname, initials, 0
22
23     $Username = $record.username
24     $GivenName = $record.firstname
25     $Surname = $record.lastname
26     $DisplayName = $record.displayName
27     $Password = $record.password
28     $StreetAddress = $record.street
29     $City = $record.city
30     $State = $record.state
31     $PostalCode = $record.zipcode
32     $Country = $record.country
33     $JobTitle = $record.jobtitle
34     $Department = $record.department
35     $Company = $record.company
36     $OU = $record.ou
37     $Description = $record.description
38     $TelephoneNumber = $record.telephone
39     $Email = $record.email
40
41     # Check if the user already exists in AD
42     If (Get-ADUser -Filter {SamAccountName -eq $Username})
43     {
44         Write-Warning "User '$SamAccountName' already exists in Active Directory."
45     }
46     else
47     {
48         # Create the new AD user
49         New-ADUser `
50             -Name "$GivenName $Surname" `
51             -GivenName $GivenName `
52             -Surname $Surname `
53             -DisplayName $DisplayName `
54             -SamAccountName $SamAccountName `
55             -UserPrincipalName $UserPrincipalName `
56             -StreetAddress $StreetAddress `
57             -City $City `
58             -State $State `
59             -PostalCode $PostalCode `
60             -Country $Country `
61             -Title $JobTitle `
62             -Department $Department `
63             -Company $Company `
64             -Path "ou=$OU,dc=etap,dc=com" `
65             -Description $Description `
66             -EmailAddress $Email `
67             -MobilePhone $TelephoneNumber `
68             -Enabled $False `
69             -AccountPassword (Convertto-SecureString $Password -AsPlainText -Force) -ChangePasswordAtLogon $True
70         #Set the Account to be automatically disabled for security reasons with $False
71     }
72 }
```

- Written in Powershell
- Creates and appends a log file with each execution
- Imports Active Directory
- Imports CSV file and assigns field parameters to unique variables
- Loops and executes for every entry in CSV:
  - Checks if user exists first, if they do skips and notifies they exist.
  - If not, continues to importing data into Active Directory.
  - Then checks to see if there is a home folder created already for that user. If so, notifies one exists already, if not then creates a new one.
- Closes the log file and ends script



# CSV File Format for Importing Users

```
AD Server
SETAPNewUsers1 - Notepad
File Edit Format View Help
Firstname,initials,lastname,username,email,telephone,password,description,department,jobtitle,OU,company,streetaddress,city,zipcode,state,country
Arthur,,Crawford,CrawfordArthur,a.crawford@setap.com,472-295-2812,Pe$$w0rd1,employee,Management,Quality Manager,Management,SETAP,,,,,
Stella,,Roberts,RobertsStella,s.roberts@setap.com,704-439-8631,Pe$$w0rd1,employee,Management,Engineering Manager,Management,SETAP,,,,,
Aiden,,Adams,AdamsAiden,a.adams@setap.com,701-453-2738,Pe$$w0rd1,employee,Management,Supply Manager,Management,SETAP,,,,,
Sam,,Higgins,HigginsSam,s.higgins@setap.com,629-597-6155,Pe$$w0rd1,employee,Management,Production Manager,Management,SETAP,,,,,
Garry,,Morrison,MorrisonGarry,g.morrison@setap.com,614-418-8584,Pe$$w0rd1,employee,Executives,CEO,Executives,SETAP,,,,,
Julian,,Stewart,StewartJulian,j.stewart@setap.com,601-636-9003,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Oliver,,Howard,HowardOliver,o.howard@setap.com,515-678-5687,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Daryl,,Ferguson,FergusonDaryl,d.ferguson@setap.com,507-867-8870,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Isabella,,Foster,FosterIsabella,i.foster@setap.com,505-977-3462,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Luke,,Crawford,CrawfordLuke,l.crawford@setap.com,505-964-5947,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Freddie,,Perkins,PerkinsFreddie,f.perkins@setap.com,505-959-2588,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Freddie,,Harper,HarperFreddie,f.harper@setap.com,505-943-7720,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Rubie,,Riley,RileyRubie,r.riley@setap.com,505-910-3668,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Jasmine,,Ryan,RyanJasmine,j.ryan@setap.com,304-970-8316,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Jasmine,,Walker,WalkerJasmine,j.walker@setap.com,304-336-6181,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Connie,,Higgins,HigginsConnie,c.higgins@setap.com,304-305-4526,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Adam,,Dixon,DixonAdam,a.dixon@setap.com,303-313-3840,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
David,,Roberts,RobertsDavid,d.roberts@setap.com,301-938-2183,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Vivian,,Stevens,StevensVivian,v.stevens@setap.com,269-969-3931,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Paige,,Anderson,AndersonPaige,p.anderson@setap.com,240-950-9372,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Kelsey,,Richardson,RichardsonKelsey,k.richardson@setap.com,231-462-7594,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Vanessa,,Rogers,RogersVanessa,v.rogers@setap.com,224-918-6299,Pe$$w0rd1,employee,Engineering,Engineer,Engineering,SETAP,,,,,
Freddie,,Murphy,MurphyFreddie,f.murphy@setap.com,223-647-3610,Pe$$w0rd1,employee,Management,Plant Manager,Management,SETAP,,,,,
Rafael,,Johnson,JohnsonRafael,r.johnson@setap.com,220-481-0977,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Tara,,Phillips,PhillipsTara,t.phillips@setap.com,218-423-3807,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Brianna,,Stevens,StevensBrianna,b.stevens@setap.com,218-285-5518,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Kate,,Reed,ReedKate,k.reed@setap.com,215-434-7885,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Charlie,,Cole,ColeCharlie,c.cole@setap.com,214-843-0696,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Reid,,Foster,FosterReid,r.foster@setap.com,214-654-4057,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Maddie,,Holmes,HolmesMaddie,m.holmes@setap.com,213-623-9533,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Maya,,Gray,GrayMaya,m.gray@setap.com,209-820-7456,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Chester,,Nelson,NelsonChester,c.nelson@setap.com,209-455-5306,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Freddie,,Andrews,AndrewsFreddie,f.andrews@setap.com,205-705-1846,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Kevin,,Johnson,JohnsonKevin,k.johnson@setap.com,203-806-6014,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Lydia,,Ellis,EllisLydia,l.ellis@setap.com,203-775-1582,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Amelia,,Turner,TurnerAmelia,a.turner@setap.com,202-415-3953,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Daisy,,Miller,MillerDaisy,d.miller@setap.com,505-644-1115,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Julian,,Douglas,DouglasJulian,j.douglas@setap.com,505-644-1103,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Adrianna,,Scott,ScottAdrianna,a.scott@setap.com,505-644-0934,Pe$$w0rd1,employee,Engineering,Industrial Engineer,Engineering,SETAP,,,,,
Edith,,Cole,ColeEdith,e.cole@setap.com,505-644-0376,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
Frederick,,Davis,DavisFrederick,f.davis@setap.com,505-644-0302,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
George,,Fowler,FowlerGeorge,g.fowler@setap.com,505-644-0941,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
Chloe,,Harris,HarrisChloe,c.harris@setap.com,505-639-0941,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
Preston,,Russell,RussellPreston,p.russell@setap.com,505-637-8983,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
Kevin,,Walker,WalkerKevin,k.walker@setap.com,505-634-7825,Pe$$w0rd1,employee,Supply Chain Mgt,Purchasing,Supply Chain Mgt,SETAP,,,,,
Vivian,,Farrrell,FarrrellVivian,v.farrrell@setap.com,505-634-4341,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
Dominik,,Ferguson,FergusonDominik,d.ferguson@setap.com,505-629-5296,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
Eleanor,,Ferguson,FergusonEleanor,e.ferguson@setap.com,505-626-6497,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
Mike,,Thomas,ThomasMike,m.thomas@setap.com,505-667-9543,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
Fenton,,Cole,ColeFenton,f.cole@setap.com,505-665-6701,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
Alan,,Cooper,CooperAlan,a.cooper@setap.com,505-664-8843,Pe$$w0rd1,employee,Supply Chain Mgt,Planning,Supply Chain Mgt,SETAP,,,,,
James,,Morgan,MorganJames,j.morgan@setap.com,505-654-6878,Pe$$w0rd1,employee,Supply Chain Mgt,Warehouse,Supply Chain Mgt,SETAP,,,,,
Windows (CRLF)
```



# *HyperV, VHD, and Virtual Servers*

# Setting up the Domain - Hyper V VMs

- Creating the Virtual Switch
- Creating the File Server and VHD
- Creating the Shares and Subfolders
- Applying GPOs to redirect the shares
- Applying GPOs to share the mapped drives
- Setting permissions in Security for granting access according to security Groups and specific Users for the Home Folders

# Setting up the Domain - Virtual Switch

- Creating the Virtual switch VM in Hyper V
- Used the create new vm wizard
- Named it and connected it to the external network
- Allowed the system to connect to this adapter
- Configuring it with network settings to be able to connect to the domain

# Virtual Switch Info:

Domain Name: setap.com    IP Range: 10.16.230.110-120

Virtual Switch: vEthernet 82574L Gigabit Network Connection – Virtual Switch

Full Switch Name: vEthernet 82574L Gigabit Network Connection – Virtual Switch

Description: Hyper-V Virtual Ethernet Adapter

MAC: 00-50-56-82-F0-2E

IP Address: 10.16.230.114

DNS Server: 10.16.230.110

Secondary DNS: 192.168.18.6

Default Gateway: 10.16.0.1

Subnet Mask: 255.255.0.0

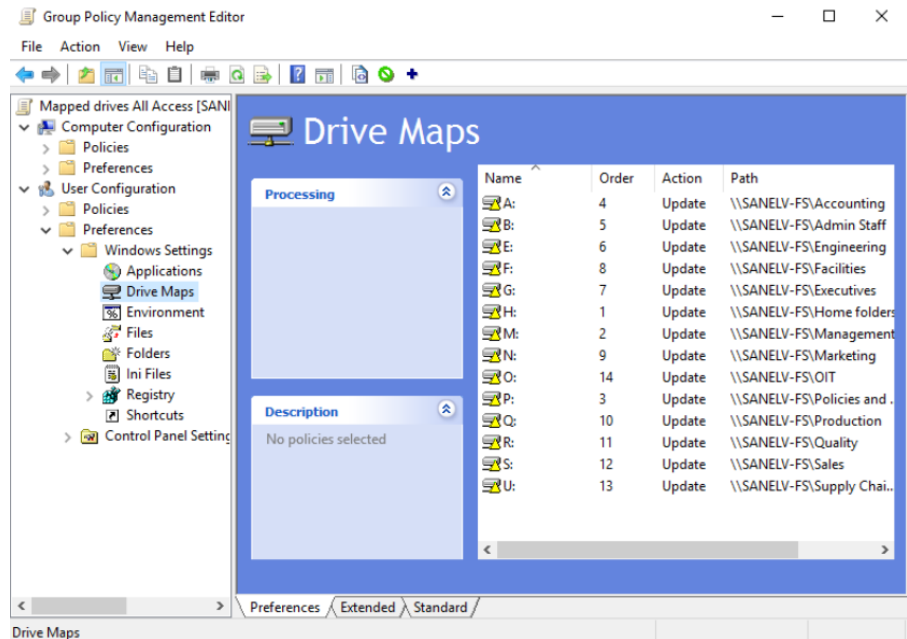
# Setting up the Domain - File Server and VHD

- We used Hyper V Manager to create a Virtual Machine running Windows Server 2019 Enterprise Edition.
- The File Server was given a name SanElv-FS and joined to the setap.com domain.
- The File Server was given an IP address of 10.16.230.113 and connected to a virtual switch.
- A file structure was created with c:\share as the root. This file structure includes folders that are shared and made available over the network.

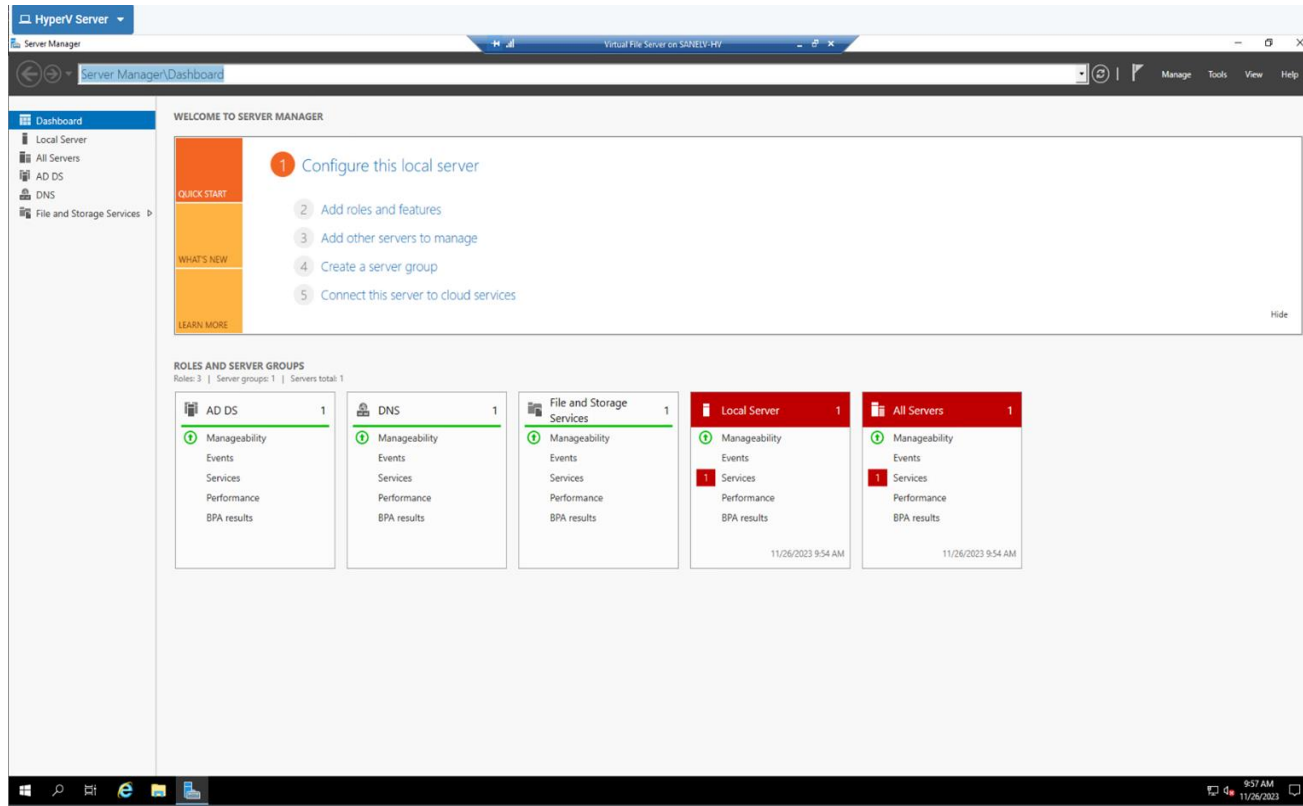
# Setting up the Domain - File Server and VHD

Each home folder is named to be consistent with a user's username. This allows us to use the username wildcard in a folder redirection GPO linked to every domain user which sets their home folder to the folder on the share.

The Home Folder is then linked to domain users through the use of a Mapped Drive GPO which allows users to easily locate their home folder over the network.



# Our Servers:



Our File Server -  
SanElv-FS



## SANELV-FS Server Info:

Domain Name: setap.com

IP Range: 10.16.230.110-120

Computer Name: SanElv-FS

***(VM operating on SanElv-HV)***

Physical Address: 00-15-5D-01-57-01

IP Address: 10.16.230.113

DNS Server: 10.16.230.110

Secondary DNS: 192.168.18.6

Default Gateway: 10.16.0.1

Subnet Mask: 255.255.0.0

Operating System: MS Server 2019  
DataCenter

Hardware: Dell Inc. PowerEdge R620

Processors: Intel® Xeon® CPU

E5-2680 0 @ 2.7GHz,

Installed RAM: 2 GB

Total Disk Space: 59.4 GB

Windows Firewall: Domain:On

Remote Management: On

Remote Desktop: Enabled

# Creating the Shares

Santa's Elves has a collection of shared folders which are mapped as drives that are accessible over the network only by personnel which possess the explicit permissions to view them.

Every employee at Santa's Elves are permitted to view HR Forms, Policies and Procedures, and each employee is able to access and modify the contents of their home folders.

Each department has its own shared folder which is only available to members of the department.

A Screenshot of the shares is available on the next slide.



Servers  
Volumes  
Disks  
Storage Pools  
**Shares**  
iSCSI  
Work Folders

**SHARES**

All shares | 18 total

TASKS ▾

Filter			
Share	Local Path	Protocol	Availability Type
SANELV-FS (18)			
Accounting	C:\share\Departments\Accounting	SMB	Not Clustered
Admin Staff	C:\share\Departments\Admin Staff	SMB	Not Clustered
Departments	C:\share\Departments	SMB	Not Clustered
Engineering	C:\share\Departments\Engineering	SMB	Not Clustered
Executives	C:\share\Departments\Executives	SMB	Not Clustered
Facilities	C:\share\Departments\Facilities	SMB	Not Clustered
Home Folders	C:\share\Home Folders	SMB	Not Clustered
Management	C:\share\Departments\Managemen...	SMB	Not Clustered
Marketing	C:\share\Departments\Marketing	SMB	Not Clustered
NETLOGON	C:\Windows\SYSVOL\sysvol\setap...	SMB	Not Clustered
Policies and Procedures	C:\share\Policies and Procedures	SMB	Not Clustered
Production	C:\share\Departments\Production	SMB	Not Clustered
Quality	C:\share\Departments\Quality	SMB	Not Clustered
Sales	C:\share\Departments\Sales	SMB	Not Clustered
Secret Project Develop...	C:\share\Departments\Secret Proj...	SMB	Not Clustered
share	C:\share	SMB	Not Clustered
Supply Chain Mgt	C:\share\Departments\Supply Cha...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

Last refreshed on 11/26/2023 9:58:08 AM

**VOLUME**

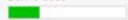
Accounting on SANELV-FS

TASKS ▾

(C:)

Capacity: 59.4 GB

26.1% Used



15.5 GB Used Space

43.9 GB Free Space

[Go to Volumes Overview >](#)**QUOTA**

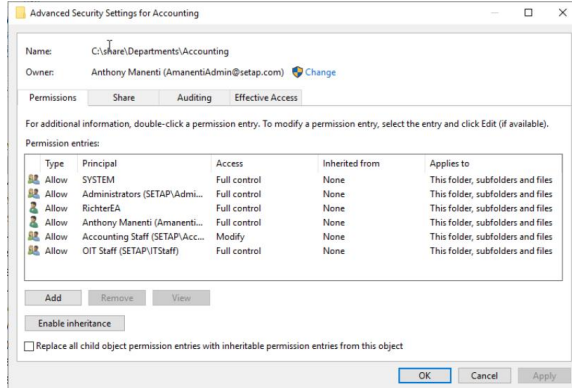
Accounting on SANELV-FS

TASKS ▾

No related quota exists.

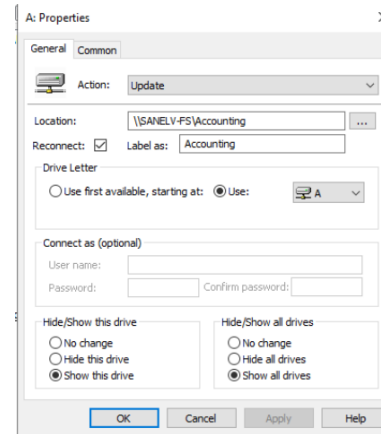
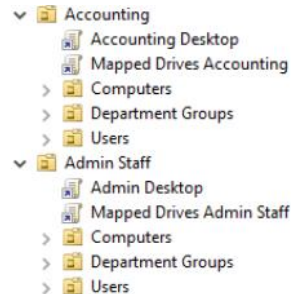
To set a quota, open the Configure Quota dialog box.

# Permissions and Policies



This is an example of our accounting folder permissions. Only Administrators, and OIT staff have full control, but the accounting staff still has the modify permission applies.

Each OU is based on a department. Each department has a mapped drive policy which determines what drives are accessible.



Drive properties are then assigned on the GPO itself.



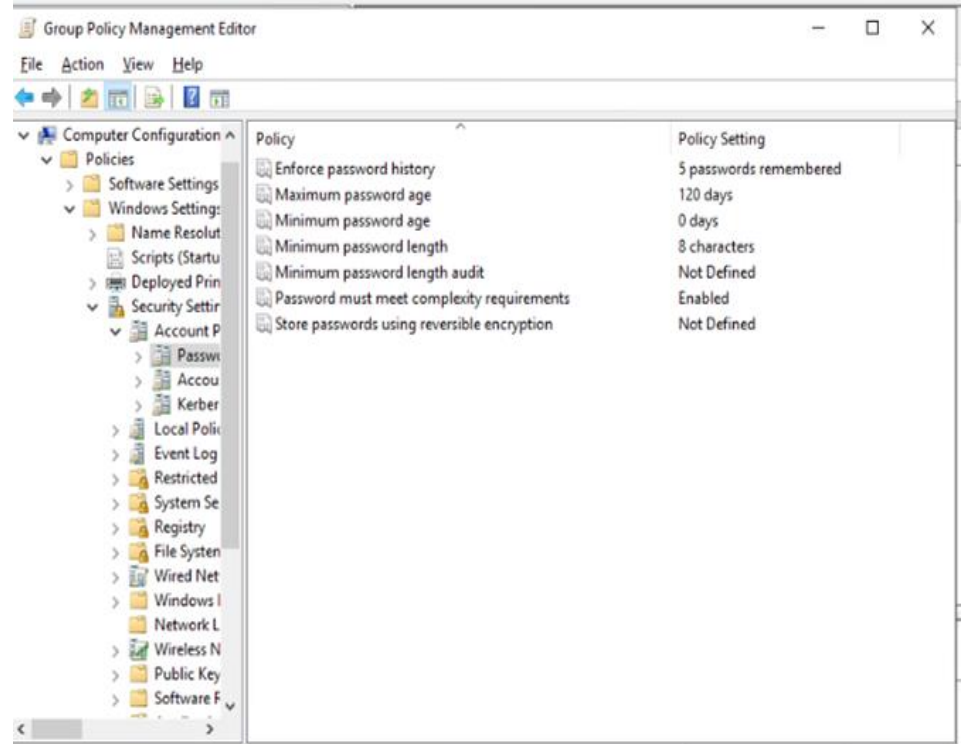
# *GPO's and You*

# Creating Domain GPOs

- GPOs created for assigning policies according to specific security groups.
- Security policies include the various password policies, File and settings restrictions, splash screen warnings, auditing of logons, notification of policy changes
- Assigning access/Shares to certain files and folders based off of which security groups are assigned to
- File redirection
- Mapped drives
- Desktop themes and settings
- Internet browser configuration of tabs

# Password GPOs

- Regulate the Password Requirements for each employee category.
- All Passwords must adhere to the basic criteria:
  - Letters - Uppercase and Lowercase
  - Numbers - 0 through 9
  - Special Characters - non-alphabetic
  - Specified length - according to specific GPOs, minimum is 8 characters
  - Expire after a set time in days
  - History of 5 previously used passwords kept to prevent reuse of known passwords
- In addition to the above:
  - Administrator's passwords expire in 90 days and have a 12 character minimum size
  - Managers' passwords expire in 90 days and have a 12 character minimum size
  - Staff's passwords expire in 120 days and have an 8 character minimum size



# Splash Screen Warning GPO

## WARNING: IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION!

This system is restricted to authorized users only. Individuals who attempt unauthorized access will be prosecuted to the fullest extent of the law. If you are unauthorized, terminate access immediately! Click OK to indicate your acceptance of this information.

OK

- Appears BEFORE the user logon screen
- User MUST acknowledge the warning by clicking OK button to sign in
- There is no way to deny seeing it
- Clearly states unauthorized users will be prosecuted to fullest extent of the law
- 1st level of security protection for the company domain
- One of the most common GPO settings used



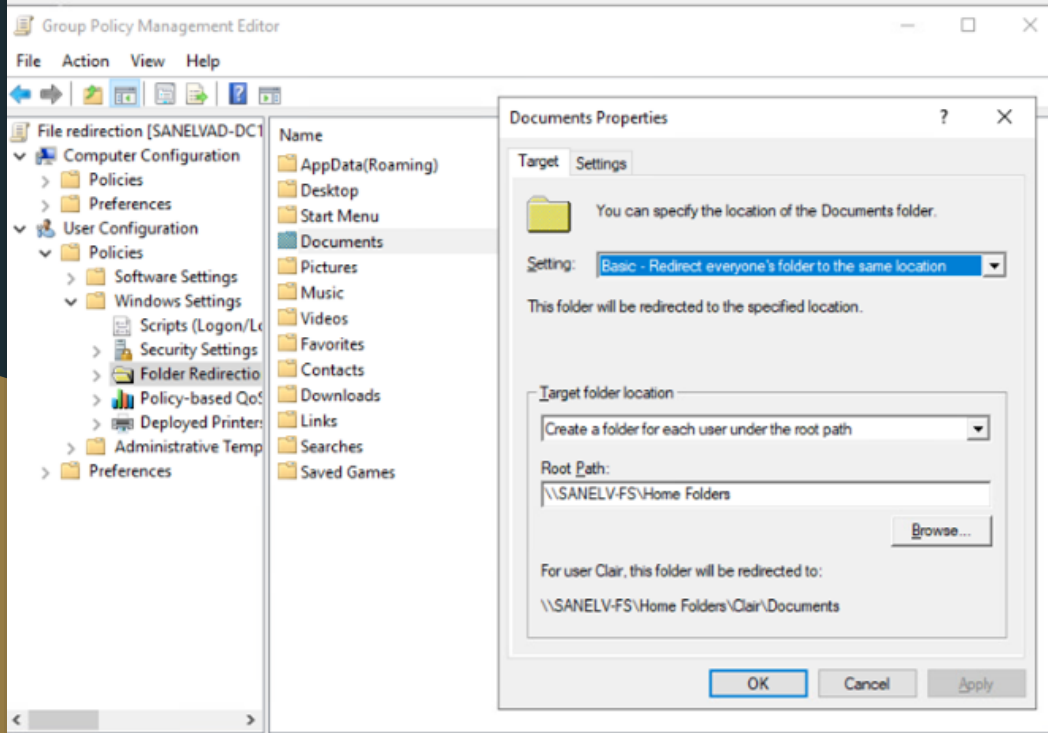


- Created unique desktop backgrounds with SETAP logo and various department names
- One image per department, assigned according to each security group
- Certain permissions are disabled. Such as: change desktop background, theme, colors, icons, etc. are locked
- This helps create a team dynamic and keeps all desktop environments work safe



## User Desktop GPOs

# File Redirection GPO



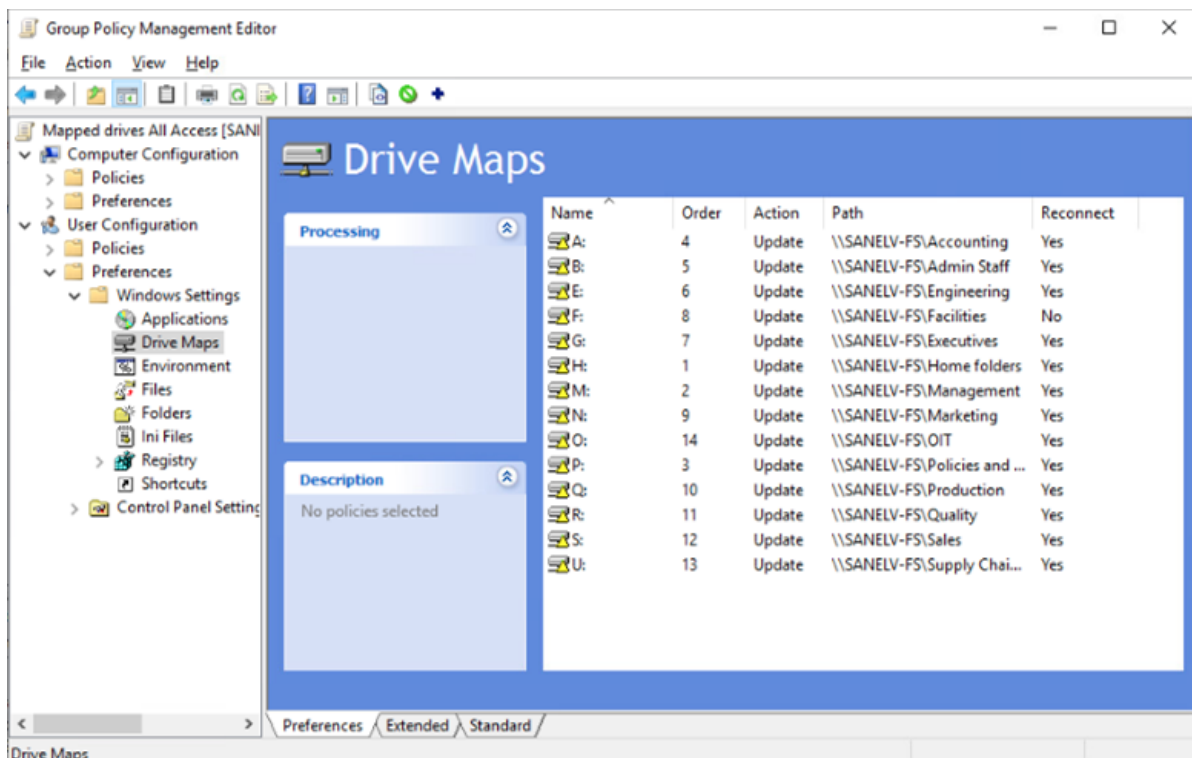
- Redirection occurs upon user logout
- Then the files and folders that were created, saved, or downloaded to their desktop, documents, or pictures folder get redirected to their home folder automatically
- They can then be found in the user's corresponding subfolders
- This applies to all authenticated users in the domain (domain users)

# IE and Edge GPOs

- 2 Tabs are opened for the user at time of browser launch
- Homepages are set to:
  - Setap.com
  - Fedex.com
- These settings are set to be disabled to the user to be changed

# Mapped Drives GPO

- The drives are mapped to the domain using the UNC (Universal Naming Convention)
- Drive letters are chosen to represent each mapped drive
- Once mapped, the drives can be set to reconnect when a user logs on
- The drives can also be applied to specific security groups which allows access to only those you want to access the drives

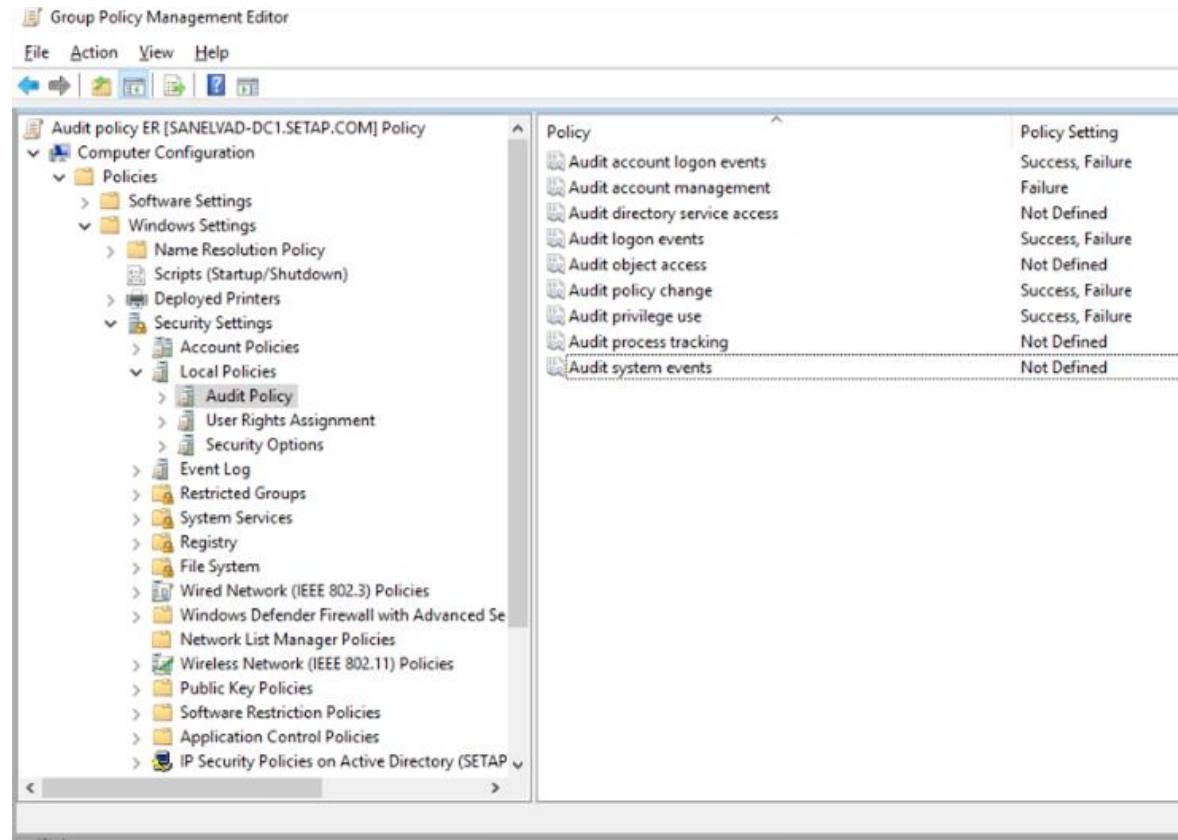


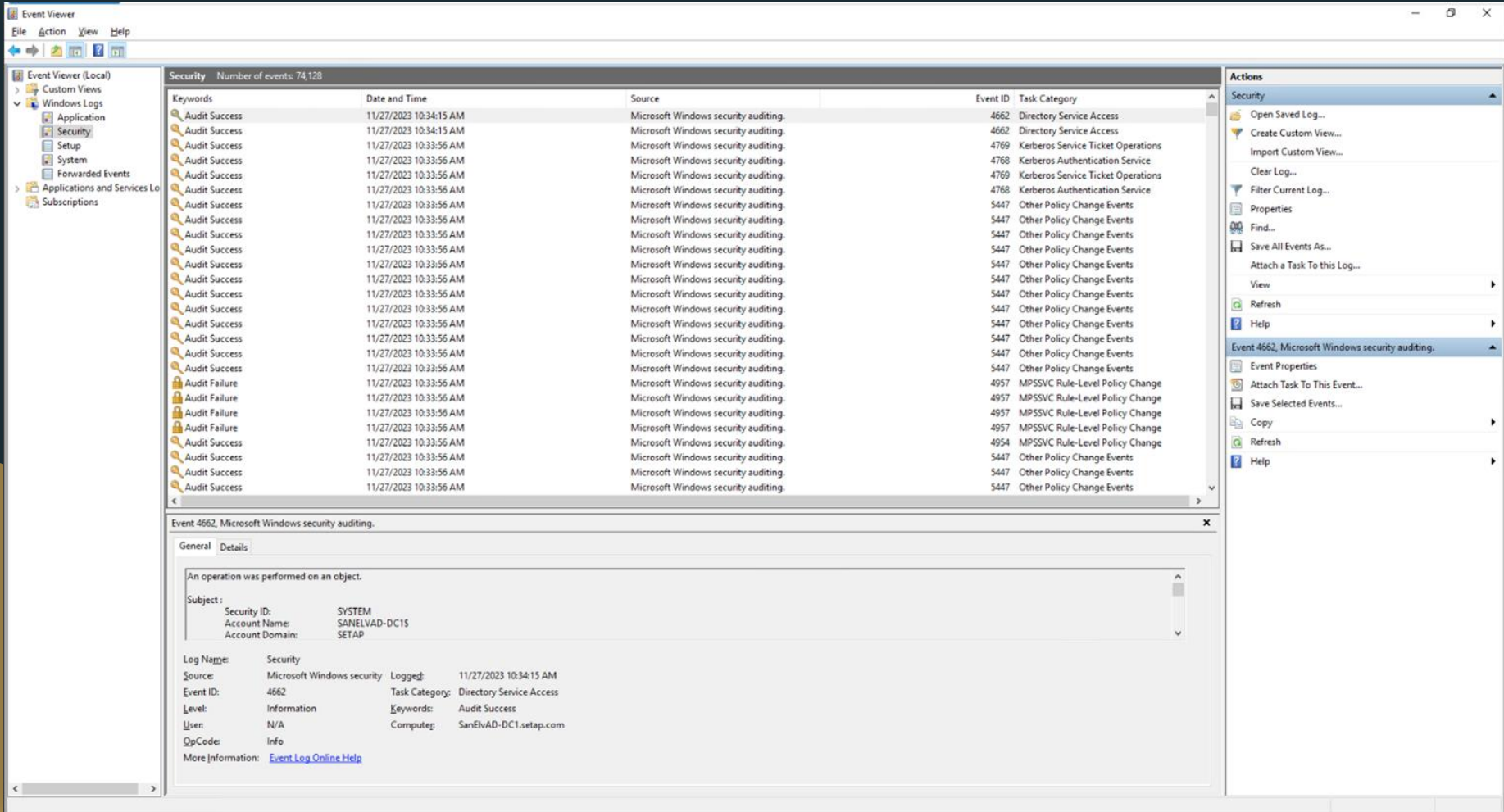
The background is a solid teal color. In the top-left corner, there are three dark blue diagonal stripes. In the bottom-right corner, there are three gold diagonal stripes. The text is centered in the middle of the image.

# *Auditing the Server*

# Audit Policies

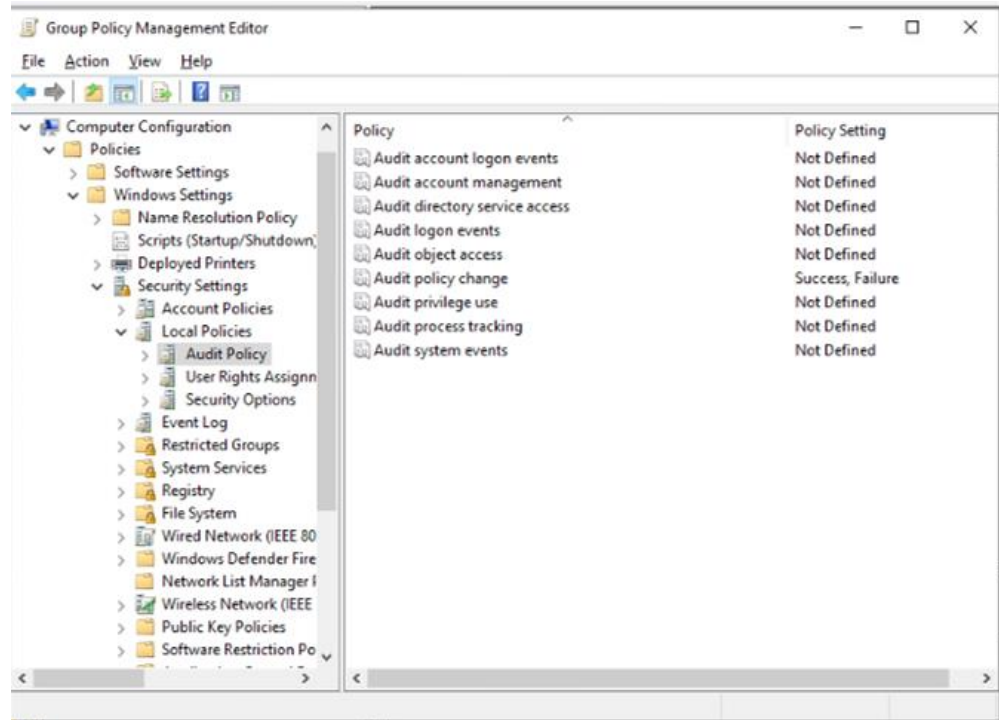
- Audit Policies are set to log any events that trigger these criteria
  - Account logon events
  - Audit logon events
  - Policy changes
  - Privilege use
- These events can be viewed in Windows Event Viewer -> Windows Logs -> Security
- You can then apply a filter to view specific





# Policy Audit GPOs

- An event is logged each time a GPO is:
  - Created
  - Modified
  - Removed
- Found under Computer Configuration -> Windows settings -> Security Settings -> Local Policies -> Audit Policy
- Logs to Windows Event Viewer







# *Baselines and Backups*

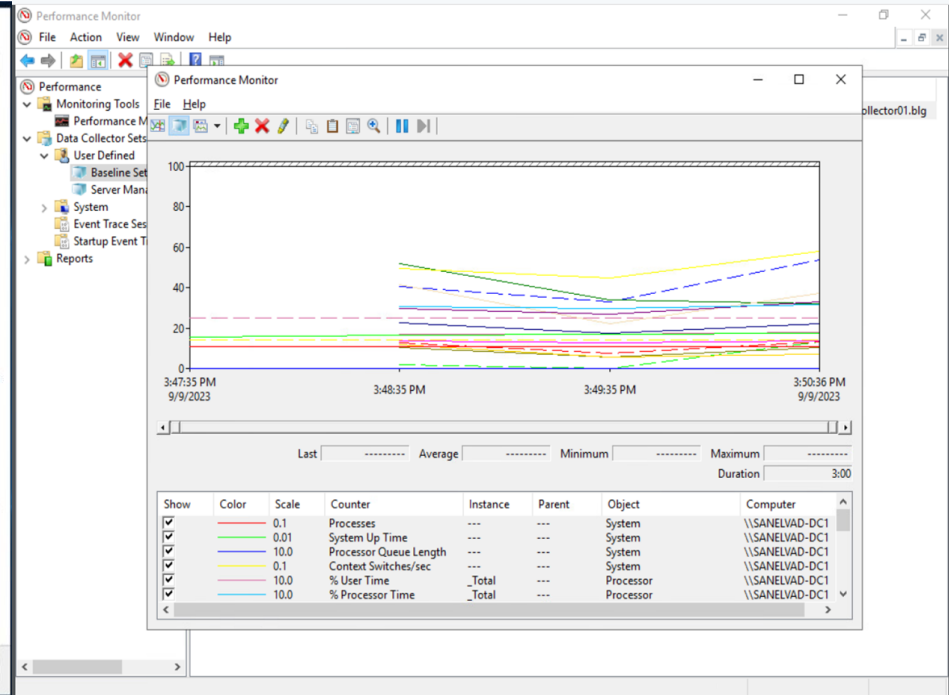
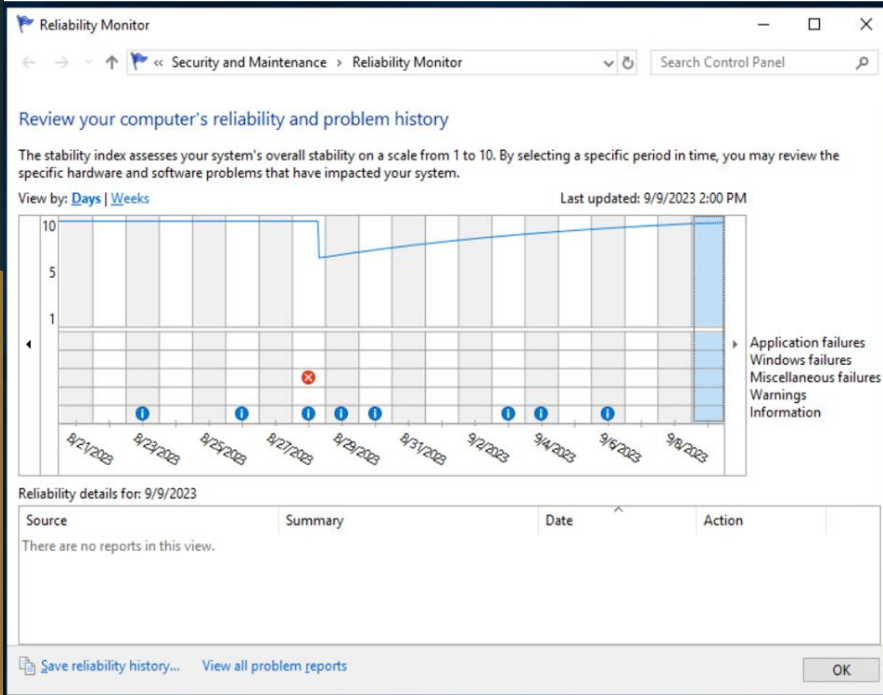
# Server Performance Baselines

Some of the Performance Metrics we track include:

- Processes
- System Up Time
- Processor Que Length
- % user Time
- % Processor Time
- % Privileged Time
- Interrupts / sec
- % Disc Time
- Packets / sec
- Bytes Total / sec
- Pages / sec
- And more

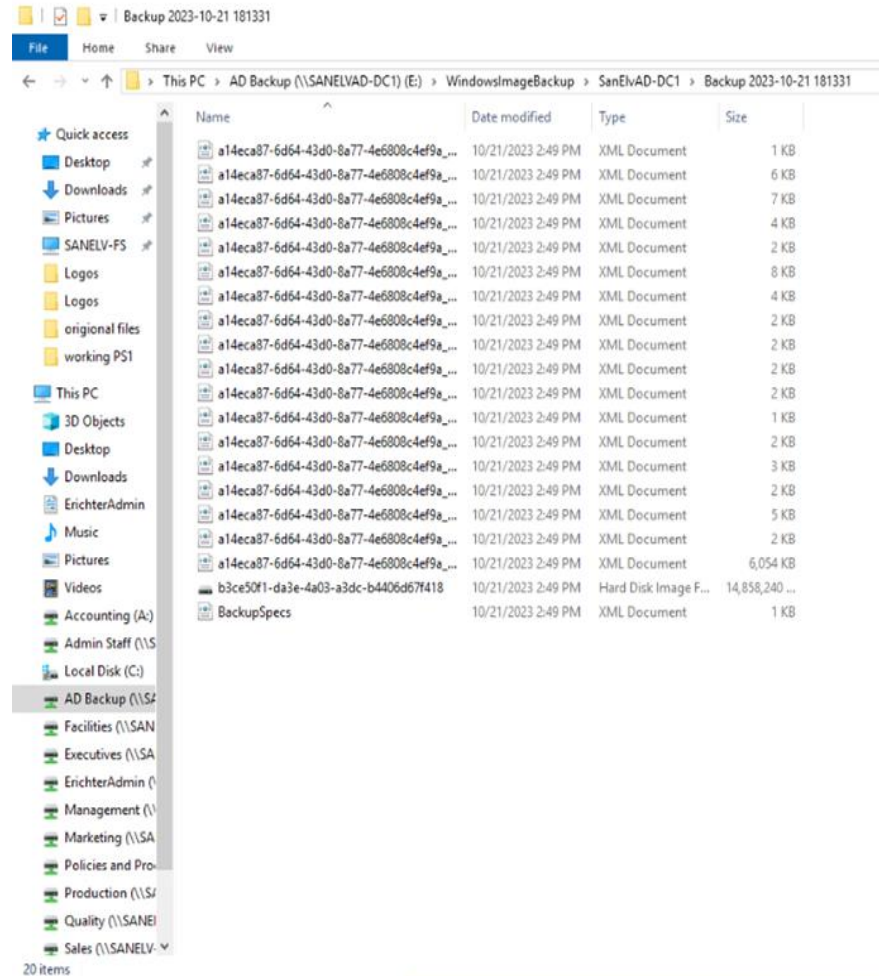
- Baselining allows us to understand what “normal” is for our Domain
- We select counters to track to obtain the data for our baseline
- By performing various baselines at different times (like Peak usage, weekdays, weekends, per shift hours, after hours, etc.) we can identify when there is a problem or an anomaly.
- Helps us narrow down where to start when correcting an issue.
- Baseline reports are saved to the domain backup volume
- Very helpful when used in conjunction with the Resource Monitor
- Screenshots of baselines are on the following slide



# Server Performance Baseline Snapshot



# Backing Up The Domain

- Backing up the domain is essential.
- Helps keep secure and important data from being lost due to various reasons
- Domain backups are set to run weekly
- We installed the Backup features and configured the backup using the Windows Server Backup wizard
- Backups are stored on the AD backup Partition on the SanElvAD-DC1 server





# *Speedbumps Along the Way*

# Issues We Encountered Along The Way

Many of our roadblocks were related to simple mistakes that were non obvious. Sometimes it's easy to take an error code and go deep into the rabbit hole, but keeping it simple is always a good place to start troubleshooting.

Santa's Elves started off with a lot of departments and users. It may have been easier in retrospect to start small on a department by department basis and make sure everything worked before scaling up.

We had to submit 3 tickets for our servers and desktops due to issues outside our control. These included the dreaded stuck updates on both Desktops and a time/date error between the client and domain which arose last night on one desktop.



# *User Access Demonstration*