

Active Directory Is Not Dead

New AD and Security Features in Windows Server vNext LTSC Preview (2025?)

Mgr. Michael Grafnetter

MVP | MCT | CEI

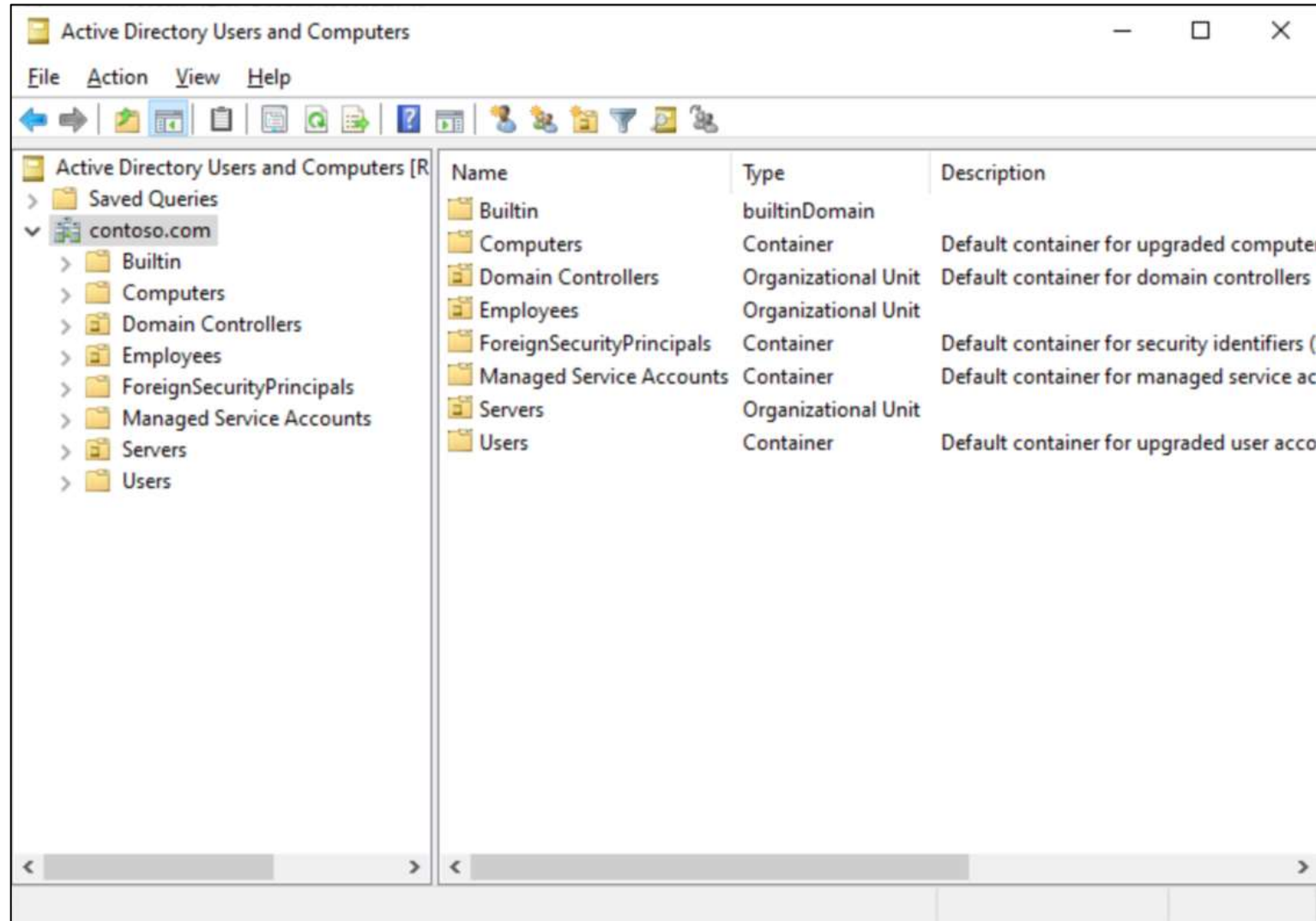
www.dsinternals.com

 [@MGrafnetter](https://twitter.com/MGrafnetter)

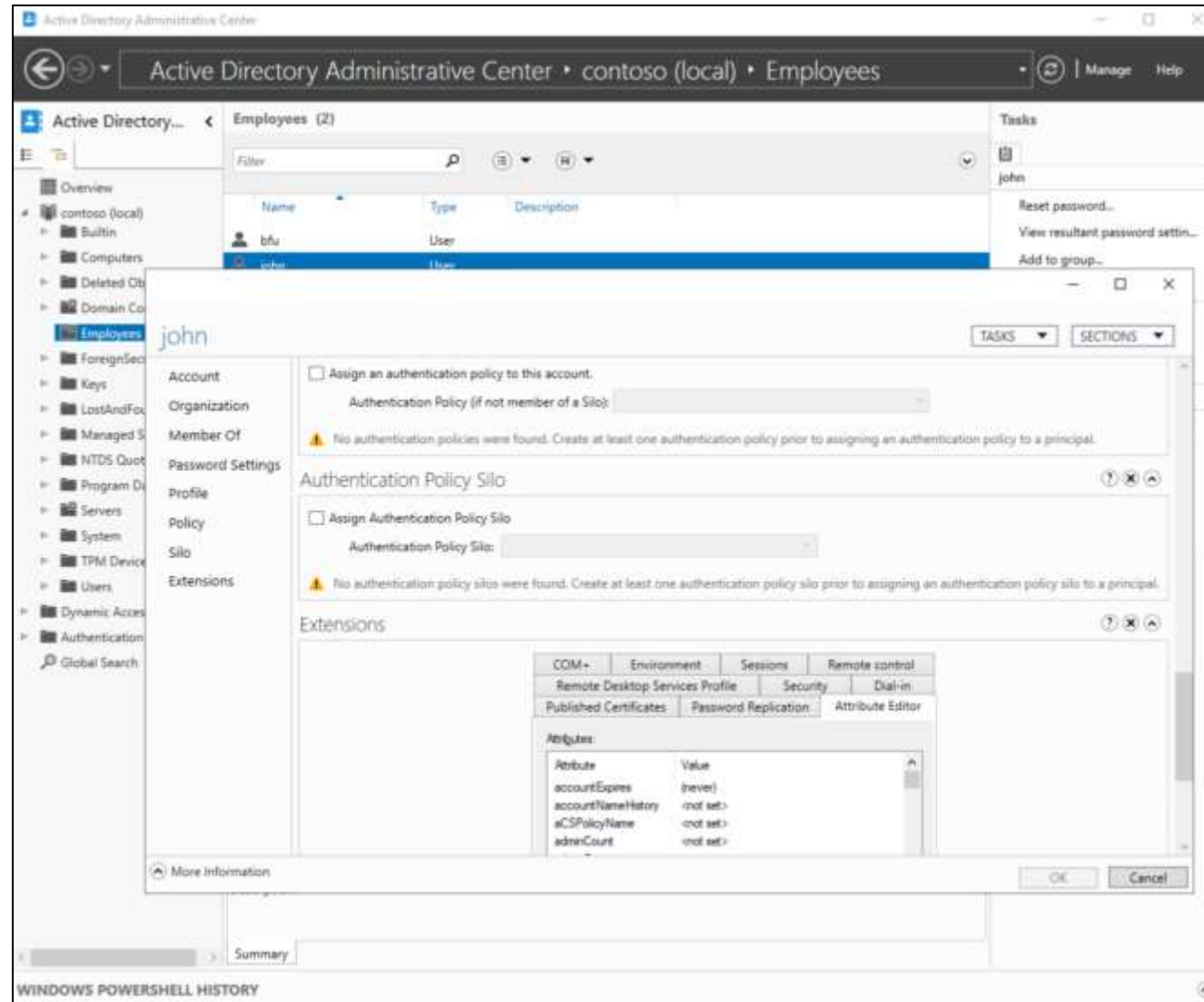


Is Active Directory Dead?

Active Directory Management Tools



Active Directory Management Tools



Active Directory Management Tools

The screenshot displays the Windows Admin Center interface for managing Active Directory Domain Services (AD DS) on a server named **ad2025-dc.contoso.com**. The left sidebar contains navigation options: Overview, Settings, Tools, and a list of tools including Azure Backup, Azure File Sync, Azure hybrid center, Azure Kubernetes Service, Azure Monitor, Certificates, Devices, DFS, Events, Files & file sharing, Firewall, Installed apps, Local users & groups, Microsoft Defender for Cloud, Networks, Packet monitoring, and Performance Monitor. The **Active Directory** tool is selected.

The main pane shows the **Active Directory Domain Services** overview. The **Browse** tab is active, displaying a tree view of the directory structure. The **Users** container is selected, showing a list of users and groups. The list includes:

name	type
Domain Admins	group
Domain Computers	group
Domain Controllers	group
Domain Guests	group
Domain Users	group
Enterprise Admins	group
Enterprise Key Admins	group
Enterprise Read-only Domain Controllers	group
External Trust Accounts	group
Forest Trust Accounts	group
Group Policy Creator Owners	group
Guest	user
john	user
Key Admins	group
Krbtgt	user
Protected Users	group
RAS and IAS Servers	group
Read-only Domain Controllers	group
Schema Admins	group

Below the list, the **Detail - john** section shows the user's properties:

Name	Type	Sam Account Name
john	user	john

Active Directory Management Tools

Windows Admin Center | Server Manager

ad2025-dc.contoso.com

Search Tools

Tools

- Active Directory
- Azure Backup
- Azure File Sync
- Azure hybrid center
- Azure Kubernetes Service
- Azure Monitor
- Certificates
- Devices
- DNS
- Events
- Files & file sharing
- Firewall
- Installed apps
- Local users & groups

Active Directory Domain Services > User properties: john

Account *
Membership

Name *
john

First Name
John

Password

User UPN Logon
john@contoso.com

Protect from Accidental Deletion ☐

User must change password at next log on ☐

User cannot change password ☐

Password never expires ☒

Microsoft Passport or smart card is required for interactive log on ☐

Account Expiration
☒ Never
☐ End of
mm/dd/yyyy

User SamAccountName *
john

Last Name
Doe

Confirm Password

Active Directory Management Tools

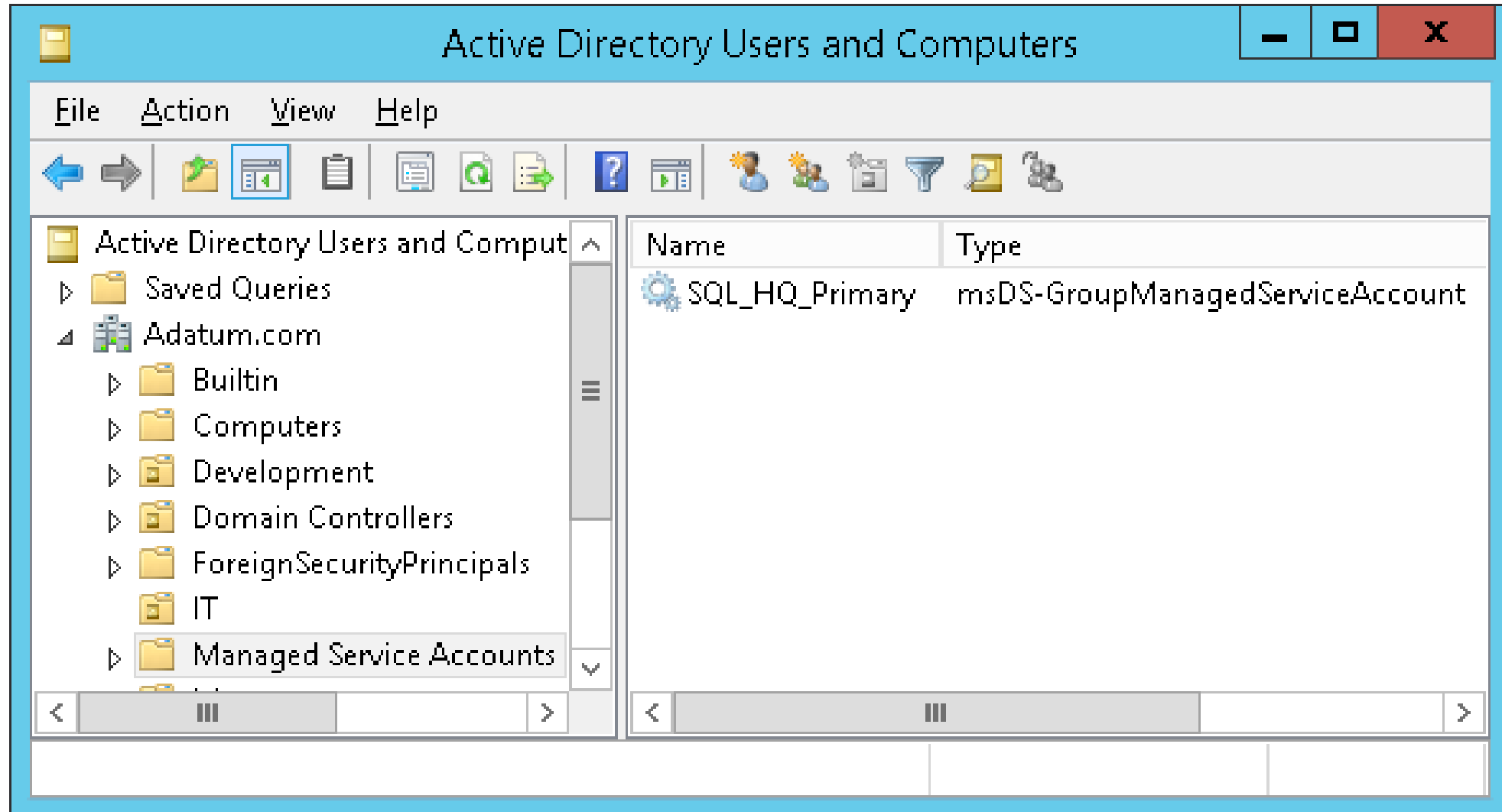
The screenshot displays the Windows Admin Center interface for managing DNS on the server `ad2025-dc.contoso.com`. The left sidebar shows the navigation menu with `DNS` selected. The main content area is titled `DNS` and includes a `PREVIEW` button. It features two tabs: `Forward lookup zones` and `Reverse lookup zones`. Under `Forward lookup zones`, there is a table listing the zones, with `contoso.com` (Primary) selected. Below this, the `Records - contoso.com` section shows a table of existing DNS records. On the right, the `Create a new DNS record` panel is open, showing a dropdown for `DNS record type` with `Host (A)` selected. The `IP address *` field is empty, and the `Time to live (TTL, seconds) *` is set to `3600`. The `Create` and `Cancel` buttons are at the bottom.

Name	Type
contoso.com	Primary

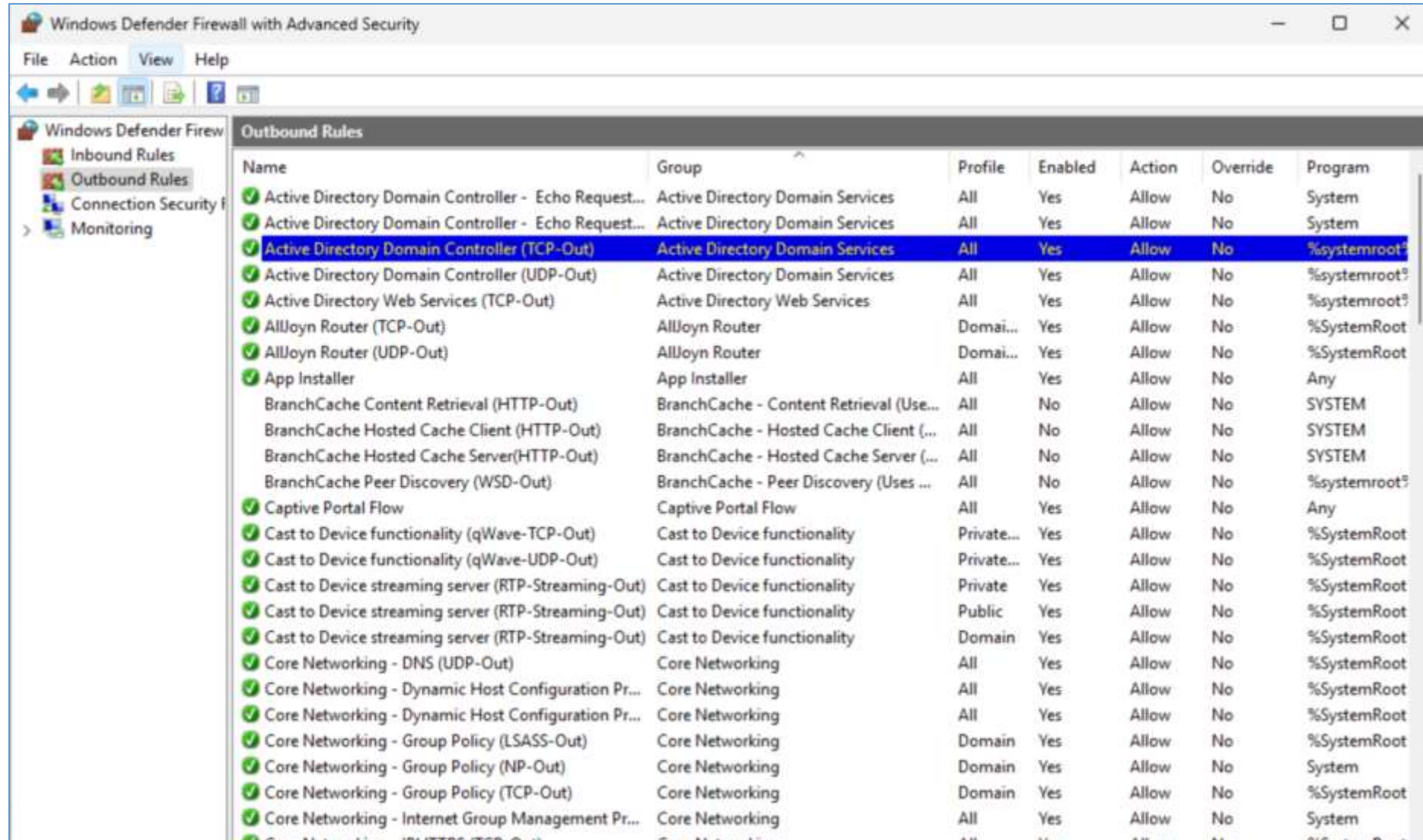
Name	Type
ad2025-dc.contoso.com	Host (A)
AD2025-SRV.contoso.com	Host (A)
admin.contoso.com	Host (A)
contoso.com	Host (A)
DomainDnsZones.contoso.com	Host (A)
ForestDnsZones.contoso.com	Host (A)

Create a new DNS record	
DNS record type	
Host (A)	
Host (AAAA)	
Alias (CNAME)	
Mail exchange (MX)	
contoso.com	
IP address *	
☐ Create associated pointer (PTR) record	
Time to live (TTL, seconds) *	
3600	

Configuring Managed Service Accounts



Domain Controller Firewall Outbound Rules



The screenshot displays the Windows Defender Firewall with Advanced Security console. The left-hand navigation pane shows the hierarchy: Windows Defender Firewall > Outbound Rules. The main pane displays a list of outbound rules. The rule 'Active Directory Domain Controller (TCP-Out)' is selected and highlighted in blue. The table below represents the data shown in the main pane.

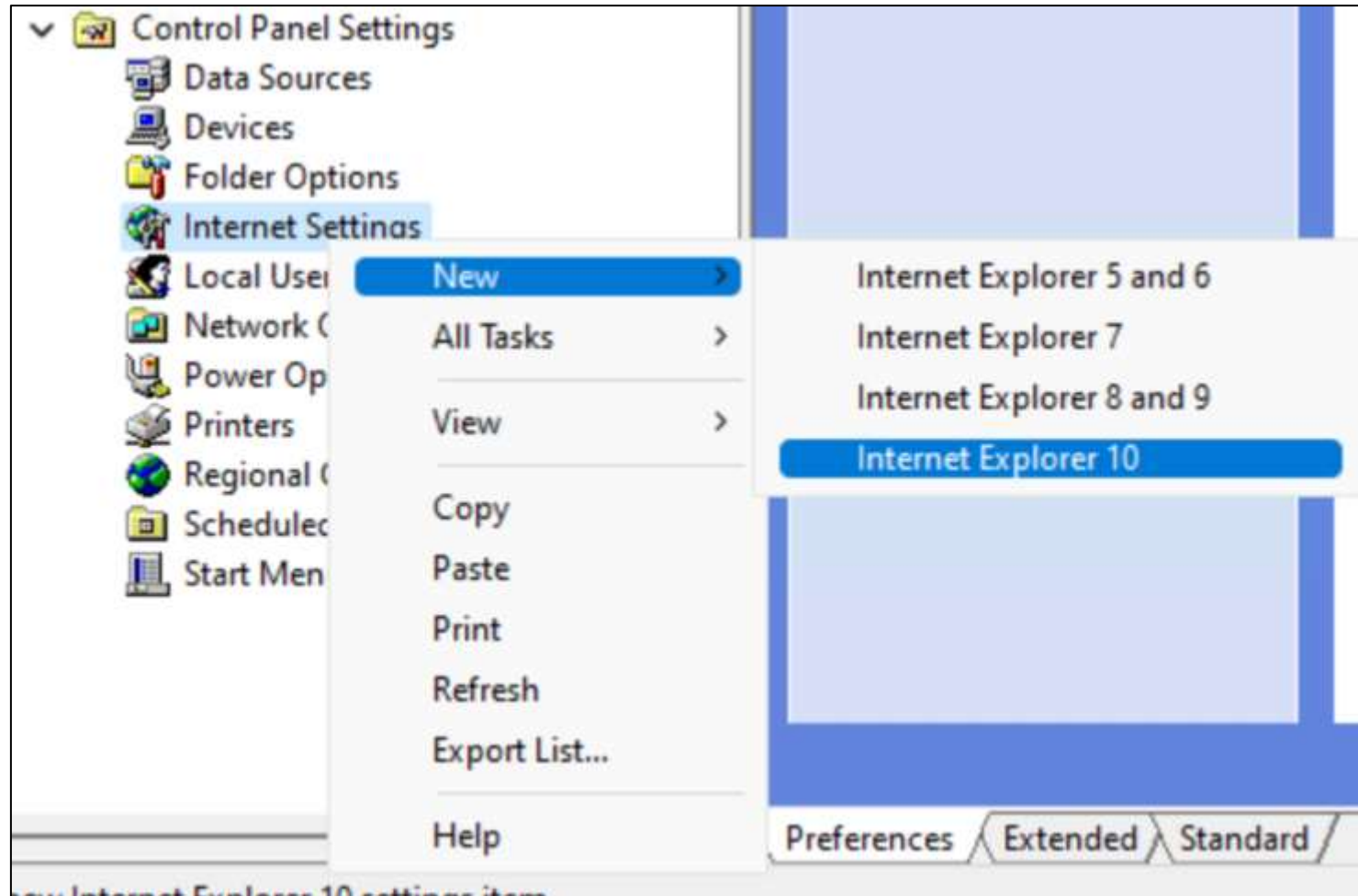
Name	Group	Profile	Enabled	Action	Override	Program
Active Directory Domain Controller - Echo Request...	Active Directory Domain Services	All	Yes	Allow	No	System
Active Directory Domain Controller - Echo Request...	Active Directory Domain Services	All	Yes	Allow	No	System
Active Directory Domain Controller (TCP-Out)	Active Directory Domain Services	All	Yes	Allow	No	%systemroot%
Active Directory Domain Controller (UDP-Out)	Active Directory Domain Services	All	Yes	Allow	No	%systemroot%
Active Directory Web Services (TCP-Out)	Active Directory Web Services	All	Yes	Allow	No	%systemroot%
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot
App Installer	App Installer	All	Yes	Allow	No	Any
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retrieval (Use...	All	No	Allow	No	SYSTEM
BranchCache Hosted Cache Client (HTTP-Out)	BranchCache - Hosted Cache Client (...)	All	No	Allow	No	SYSTEM
BranchCache Hosted Cache Server(HTTP-Out)	BranchCache - Hosted Cache Server (...)	All	No	Allow	No	SYSTEM
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discovery (Uses ...)	All	No	Allow	No	%systemroot%
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any
Cast to Device functionality (qWave-TCP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%SystemRoot
Cast to Device functionality (qWave-UDP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%SystemRoot
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Private	Yes	Allow	No	%SystemRoot
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Public	Yes	Allow	No	%SystemRoot
Cast to Device streaming server (RTP-Streaming-Out)	Cast to Device functionality	Domain	Yes	Allow	No	%SystemRoot
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%SystemRoot
Core Networking - Dynamic Host Configuration Pr...	Core Networking	All	Yes	Allow	No	%SystemRoot
Core Networking - Dynamic Host Configuration Pr...	Core Networking	All	Yes	Allow	No	%SystemRoot
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	No	%SystemRoot
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%SystemRoot
Core Networking - Internet Group Management Pr...	Core Networking	All	Yes	Allow	No	System
Core Networking - Internet Group Management Pr...	Core Networking	All	Yes	Allow	No	%SystemRoot

Endpoint Management

- ▼ Computer Configuration
 - ▼ Policies
 - ▼ Software Settings
 - Software installation
 - ▼ Windows Settings
 - > Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - ▼ Security Settings
 - > Account Policies
 - > Local Policies
 - > Event Log
 - > Restricted Groups
 - > System Services
 - > Registry
 - > File System
 - > Wired Network (IEEE 802.3) Policies
 - > Windows Defender Firewall with Advanced Security
 - Network List Manager Policies
 - > Wireless Network (IEEE 802.11) Policies
 - > Public Key Policies
 - > Software Restriction Policies
 - > Application Control Policies
 - > IP Security Policies on Active Directory (CONTOSO.COM)
 - > Advanced Audit Policy Configuration
 - > Policy-based QoS
 - > Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.

- ▼ Preferences
 - ▼ Windows Settings
 - Environment
 - Files
 - Folders
 - Ini Files
 - > Registry
 - Network Shares
 - Shortcuts
 - ▼ Control Panel Settings
 - Data Sources
 - Devices
 - Folder Options
 - Local Users and Groups
 - Network Options
 - Power Options
 - Printers
 - Scheduled Tasks
 - Services

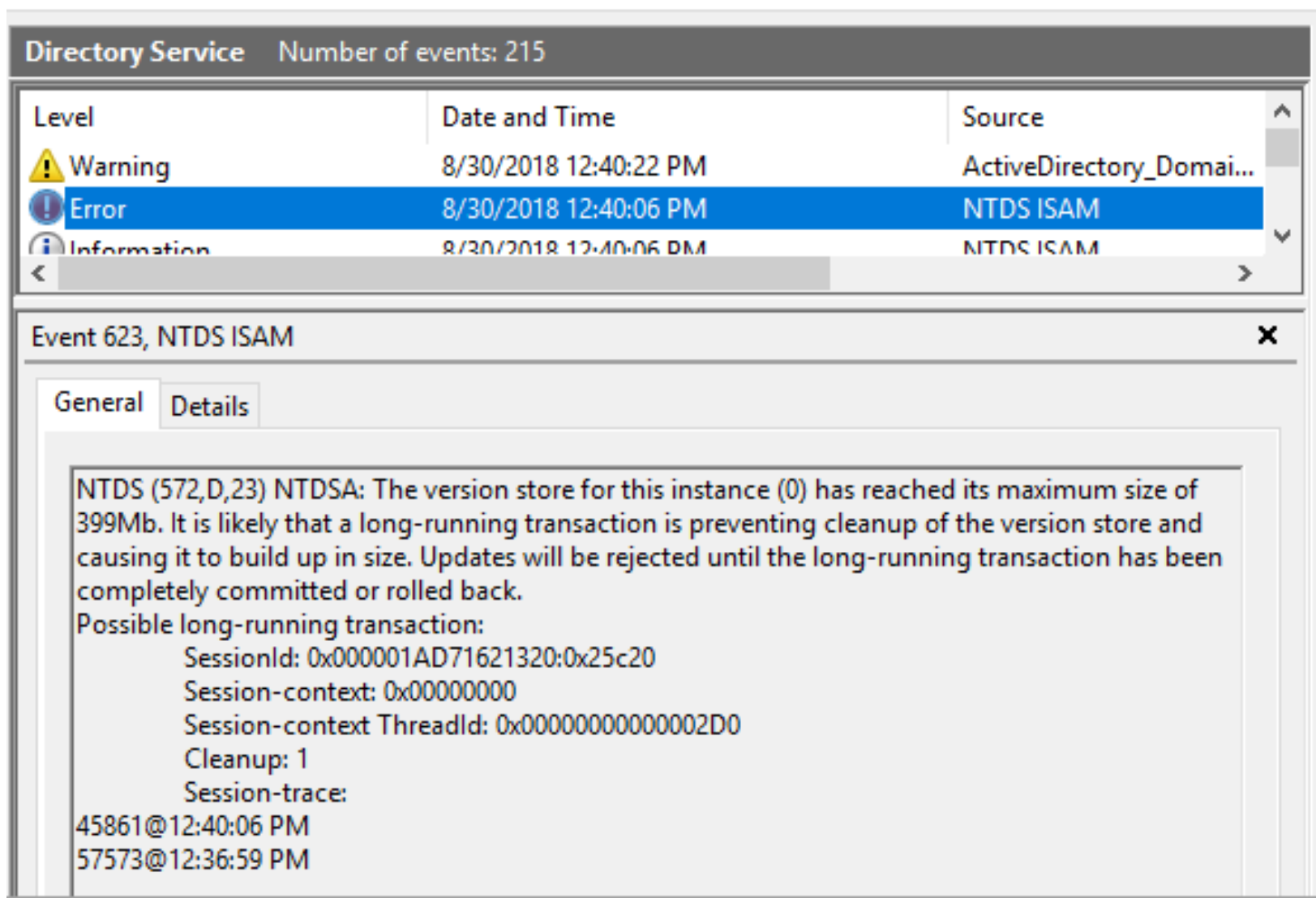
Endpoint Management



User State Roaming

- Roaming Profiles
- Folder Redirection (AppData\Roaming)
- Work Folders
- User State Migration Tool (USMT)
- User Experience Virtualization (UE-V in Windows 10 1607)
- Edge Profile Sync (Hybrid Identity)

New AD Features in Windows Server 2019



The screenshot displays the Windows Event Viewer interface. At the top, the 'Directory Service' log is selected, showing 215 events. The event list is filtered to show errors, with the selected event being 'Error' at 8/30/2018 12:40:06 PM, source 'NTDS ISAM'. The event details pane shows 'Event 623, NTDS ISAM'. The 'General' tab is active, displaying the following message:

NTDS (572,D,23) NTDSA: The version store for this instance (0) has reached its maximum size of 399Mb. It is likely that a long-running transaction is preventing cleanup of the version store and causing it to build in size. Updates will be rejected until the long-running transaction has been completely committed or rolled back.

Possible long-running transaction:

- SessionId: 0x000001AD71621320:0x25c20
- Session-context: 0x00000000
- Session-context ThreadId: 0x000000000000002D0
- Cleanup: 1
- Session-trace:
 - 45861@12:40:06 PM
 - 57573@12:36:59 PM

New AD Features in Windows Server 2022

Active Directory Domain Functional Levels

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 Server Native
- Windows 2000 Server Mixed

Active Directory Forest Functional Levels

- **Windows Server 2016**
- Windows Server 2012 R2*
- Windows Server 2012*
- **Windows Server 2008 R2**
- Windows Server 2008*
- **Windows Server 2003**
- **Windows 2000 Server Native**
- Windows 2000 Server Mixed

* No new features

Active Directory Optional Features

Feature	OS
Recycle Bin	Windows Server 2008 R2
Privileged Access Management	Windows Server 2016

Microsoft Identity Manager 2016

Milestone	Date
Start Date	Sep 28, 2015
Mainstream End Date	Jan 12, 2021
Extended End Date (Original)	Jan 13, 2026
Extended End Date	Jan 9, 2029

AD vs Entra ID New Features

Learn / Microsoft Entra / Fundamentals /

What's new in Microsoft Entra ID?

Article • 02/01/2024 • 84 contributors [Feedback](#)

In this article

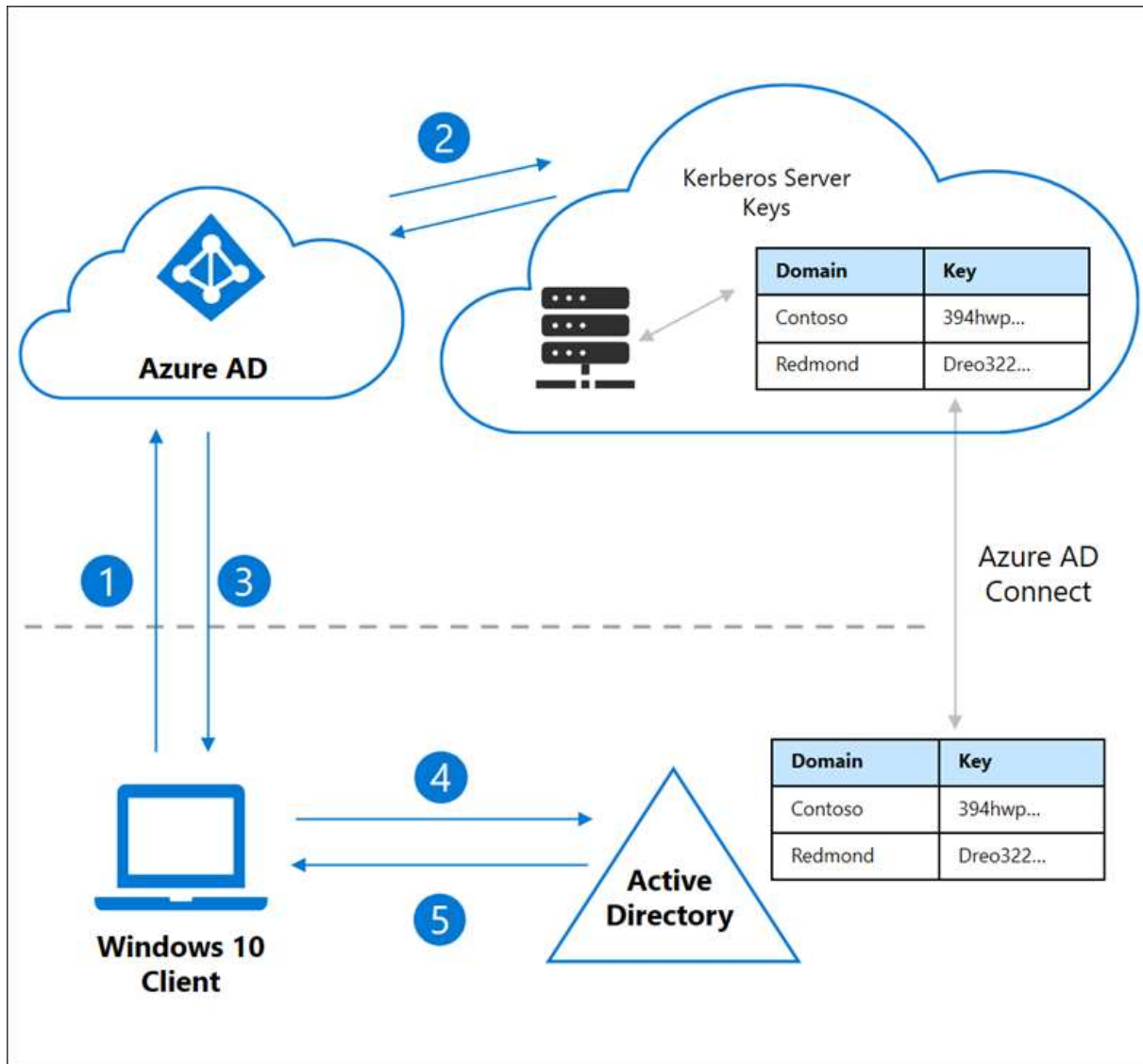
- January 2024
- December 2023
- November 2023
- October 2023
- September 2023

Get notified about when to revisit this page for updates by copying and pasting this URL: <https://learn.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us> into your  feed reader.

Microsoft Entra ID (previously known as Azure Active Directory) receives improvements on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about:

- The latest releases
- Known issues
- Bug fixes

PassKey Support (Cloud Kerberos Trust)



AD Certificate Services Web Enrollment

The screenshot shows a web browser window with the address bar displaying `https://gateway.contoso.com/certsrv/certrqma.asp`. The page title is "Microsoft Active Directory Certificate Services – Contoso Root CA". The main heading is "Advanced Certificate Request".

Certificate Template:
Web Server ▼

Key Options:
☒ Create new key set ☐ Use existing key set
CSP: Loading... ▼
Key Usage: ☒ Exchange ☐ Signature ☐ Both
Key Size: 0 Min: Max: (common key sizes:)
☒ Automatic key container name ☐ User specified key container name
☐ Mark keys as exportable
☐ Enable strong private key protection

Additional Options:
Request Format: ☒ CMC ☐ PKCS10
Hash Algorithm: ▼
Only used to sign request.
☐ Save request
Attributes:
Friendly Name:

Submit >

Active Directory Federation Services

Microsoft | Learn | Documentation | Training | Credentials | Q&A | Code Samples | Assessments | Shows

Windows Server | Get started | Failover clustering | Management | Identity and access | Networking | Troubleshooting | Related products

Filter by title

Learn / Windows Server /

AD FS Overview

Article • 02/13/2024 • 8 contributors

Feedback

Important

Instead of upgrading to the latest version of AD FS, Microsoft highly recommends migrating to Microsoft Entra ID. For more information, see [Resources for decommissioning AD FS](#)

Active Directory Federation Service (AD FS) enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries. AD FS extends the ability to use single sign-on functionality that is available within a single security or enterprise boundary to Internet-facing applications to enable customers, partners, and suppliers a streamlined user experience while accessing the web-based applications of an organization.

This document contains a list of all of the documentation overviews for AD FS for Windows Server. This includes the following:

- [What's New in AD FS for Windows Server 2019](#)
- [AD FS OpenID Connect/OAuth flows and Application Scenarios](#)

Left-hand navigation pane:

- Identity and Access
 - > Solutions and Scenario Guides
 - > Active Directory Domain Services
 - > Active Directory Federation Services
 - > AD FS Overview
 - AD FS Overview
 - What's new in Active Directory Federation Services
 - AD FS 2016 Requirements
 - > AD FS Design
 - > AD FS Deployment
 - > AD FS Development
 - > AD FS Operations
 - > AD FS Troubleshooting
 - > AD FS Technical Reference
 - AD FS 2016 FAQ
 - > AD FS Decommission
 - > Active Directory Rights Management Service
 - > Active Directory Certificate Services

AD Rights Management Services

The screenshot shows the Microsoft Learn website interface. The top navigation bar includes the Microsoft logo and links for Learn, Documentation, Training, Credentials, Q&A, Code Samples, Assessments, and Shows. The breadcrumb trail indicates the path: Windows Server 2012 R2 and Windows Server 2012 / Server Roles and Technologies / Active Directory / Active Directory Rights Management Services Overview. The left sidebar contains a search bar and a list of navigation links, with 'Active Directory Rights Management Services' highlighted. The main content area features the article title, a date, a list of topics covered in the article, and a section for related Azure information. The article text begins with an overview of AD RMS in Windows Server 2012.

Microsoft | Learn | Documentation | Training | Credentials | Q&A | Code Samples | Assessments | Shows

Filter by title

Windows Server 2012 R2 and Windows Server 2012

What's New in Windows Server

- > Technical Scenarios for Windows Server
- > Install and Deploy Windows Server
- > Migrate Roles and Features to Windows Server
- > Secure Windows Server
- > Manage Privacy
- > Support Windows Server
- > Server Roles and Technologies
 - Server Roles and Technologies
 - > Active Directory
 - Active Directory
 - What's New in Active Directory
 - > Active Directory Certificate Services
 - > Active Directory Domain Services
 - > Active Directory Federation Services
 - Active Directory Lightweight Directory Services
 - > Active Directory Rights Management Services
 - Active Directory Rights Management Services**
 - What's New in Active Directory Rights Management Services (AD RMS)
 - Test Lab Guide: Deploying an AD RMS Cluster
 - AD RMS Mobile Device Extension
 - Deploying AD RMS with AD FS
 - AD RMS Infrastructure Deployment Tips

Active Directory Rights Management Services Overview

Article • 08/31/2016

In this article

- Role description
- Practical applications
- New and changed functionality
- Server Manager information
- Show 2 more

Applies To: Windows Server 2012 R2, Windows Server 2012

Expand table

Did you know that Microsoft Azure provides similar functionality in the cloud? Learn more about [Microsoft Azure identity solutions](#).

Create a hybrid identity solution in Microsoft Azure:

- [Learn about Azure Rights Management](#)
- [Deploy the Azure Rights Management Connector](#)

This document provides an overview of Active Directory Rights Management Services (AD RMS) in Windows Server® 2012. AD RMS is the server role that provides you with management and development tools that work with industry security technologies—including encryption, certificates, and authentication—to help organizations create reliable information protection solutions.



Active Directory Is Not Dead

Windows Server Insiders Preview

The screenshot displays the Windows Server 2025 Standard desktop environment. The Task Manager application is open, showing the 'Processes' tab with a list of running processes. The 'Active Directory Users and Computers' console is also open, showing the 'Domain Controllers' folder. A PowerShell command prompt is running the `Get-ADUser -Filter *` command, displaying the properties of the 'Administrator' and 'Guest' users.

Task Manager - Processes

Name	Status	CPU	Memory	Disk	Network
Task Manager	Running	7.9%	47.8 MB	0 MB/s	0 MB/s
Service Host: Local System (14)	Running	2.9%	25.6 MB	0 MB/s	0 MB/s
Antimalware Service Executable	Running	2.0%	159.7 MB	0 MB/s	0 MB/s
termsvcs	Running	1.5%	40.0 MB	0 MB/s	0 MB/s
Windows Explorer	Running	1.3%	43.3 MB	0 MB/s	0 MB/s

Active Directory Users and Computers

Name	Type	DC Type	Site
AD2025-DC	Computer	GC	Default-First-Site-Name

PowerShell Command Prompt

```
PS C:\> Get-ADUser -Filter *
```

Administrator User Properties:

- DistinguishedName : CN=Administrator,CN=Users,DC=contoso,DC=com
- Enabled : True
- GivenName :
- Name : Administrator
- ObjectClass : user
- ObjectGUID : f040989a-a54b-47f5-ae73-a5dcdd53169c
- SamAccountName : Administrator
- SID : S-1-5-21-3926268688-3775052234-3212022108-500
- Surname :
- UserPrincipalName :

Guest User Properties:

- DistinguishedName : CN=Guest,CN=Users,DC=contoso,DC=com
- Enabled : False
- GivenName :
- Name : Guest
- ObjectClass : user
- ObjectGUID : 51c04f63-785f-4bc2-bcfb-a1e7ded3d4b2

Windows Server 2025 Standard
Evaluation copy. Build 26063.ge_release.240216-1326

#ADIsNotDead

Agenda

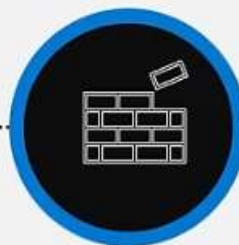


Improvements for Active Directory

Security



Scalability



Supportability



#ADIsNotDead



New Functional Levels

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the application icon and the text 'Active Directory Domain Services Configuration Wizard'. The window has standard Windows window controls (minimize, maximize, close) on the right. The main content area is titled 'Domain Controller Options' in a large blue font. In the top right corner, it says 'TARGET SERVER LTABDC1'. On the left side, there is a vertical navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (which is highlighted with a blue background), 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area on the right contains the following sections: 1. 'Select functional level of the new forest and root domain' with two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server vNEXT'. 2. 'Specify domain controller capabilities' with three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). 3. 'Type the Directory Services Restore Mode (DSRM) password' with two text boxes labeled 'Password:' and 'Confirm password:'. At the bottom of the main area is a blue hyperlink 'More about domain controller options'. The bottom of the window features a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
LTABDC1

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server vNEXT

Domain functional level: Windows Server vNEXT

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Schema Updates

adprep				
This PC > DVD Drive (D:) SSS_X64FRE_EN-US_DV9 > support > adprep >				
New [Icons] Sort View ...				
Name	Date modified	Type	Size	
en-us	2/17/2024 8:46 AM	File folder		
schupgrade	2/17/2024 8:44 AM	Security Catalog	25 KB	
sch91.ldf	2/17/2024 8:44 AM	LDF File	2 KB	
sch90.ldf	2/17/2024 8:44 AM	LDF File	3 KB	
sch89.ldf	2/17/2024 8:44 AM	LDF File	7 KB	
sch88.ldf	2/17/2024 8:44 AM	LDF File	2 KB	
sch87.ldf	2/17/2024 8:44 AM	LDF File	2 KB	
sch86.ldf	2/17/2024 8:44 AM	LDF File	3 KB	

32k Database Page Size Optional Feature

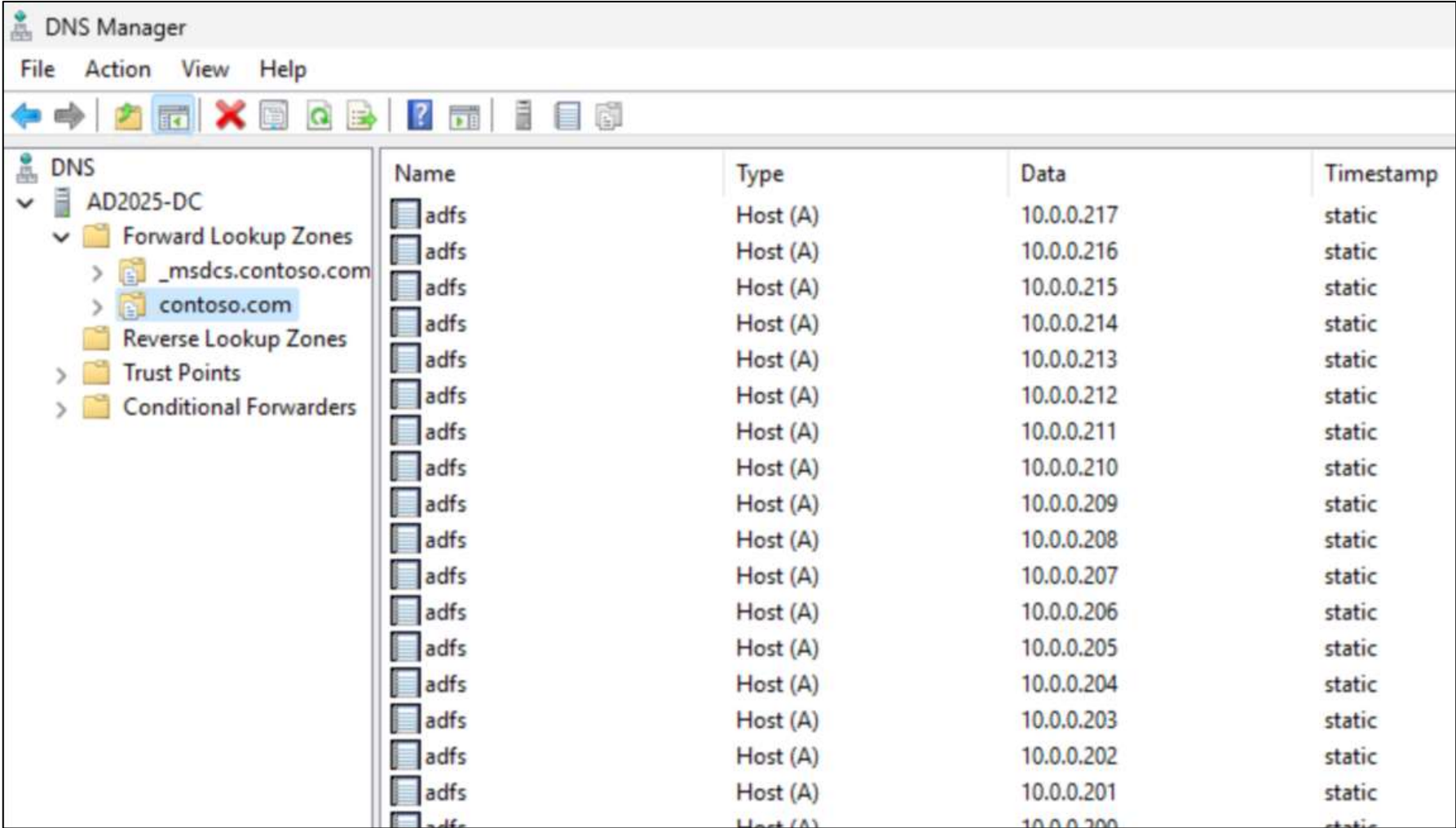
ms-Mcs-AdmPwdHistory

```
PS C:\Windows\system32> repadmin /replsum
Replication Summary Start Time: 2017-10-09 13:12:55

Beginning data collection for replication summary, this may take awhile:
.....

Destination DSA      largest delta      fails/total %%      error
-----
[Redacted]           27m:38s           0 / 15           0
[Redacted]           16m:16s           0 / 15           0
[Redacted]           26m:20s           0 / 15           0
[Redacted]           02m:13s           2 / 20          10 (8304) The maximum size of an object has been exceeded.
21d.01h:44m:09s       2 / 15           13 (8304) The maximum size of an object has been exceeded.
21d.01h:38m:28s       2 / 15           13 (8304) The maximum size of an object has been exceeded.
```

32k Database Page Size Optional Feature



The screenshot shows the Windows DNS Manager application. The left pane displays the hierarchy: DNS > AD2025-DC > Forward Lookup Zones > contoso.com. The right pane shows a list of Host (A) records for the contoso.com zone. The records are listed in descending order of IP address, from 10.0.0.217 down to 10.0.0.200. Each record has a Name of 'adfs', a Type of 'Host (A)', and a Timestamp of 'static'.

Name	Type	Data	Timestamp
adfs	Host (A)	10.0.0.217	static
adfs	Host (A)	10.0.0.216	static
adfs	Host (A)	10.0.0.215	static
adfs	Host (A)	10.0.0.214	static
adfs	Host (A)	10.0.0.213	static
adfs	Host (A)	10.0.0.212	static
adfs	Host (A)	10.0.0.211	static
adfs	Host (A)	10.0.0.210	static
adfs	Host (A)	10.0.0.209	static
adfs	Host (A)	10.0.0.208	static
adfs	Host (A)	10.0.0.207	static
adfs	Host (A)	10.0.0.206	static
adfs	Host (A)	10.0.0.205	static
adfs	Host (A)	10.0.0.204	static
adfs	Host (A)	10.0.0.203	static
adfs	Host (A)	10.0.0.202	static
adfs	Host (A)	10.0.0.201	static
adfs	Host (A)	10.0.0.200	static

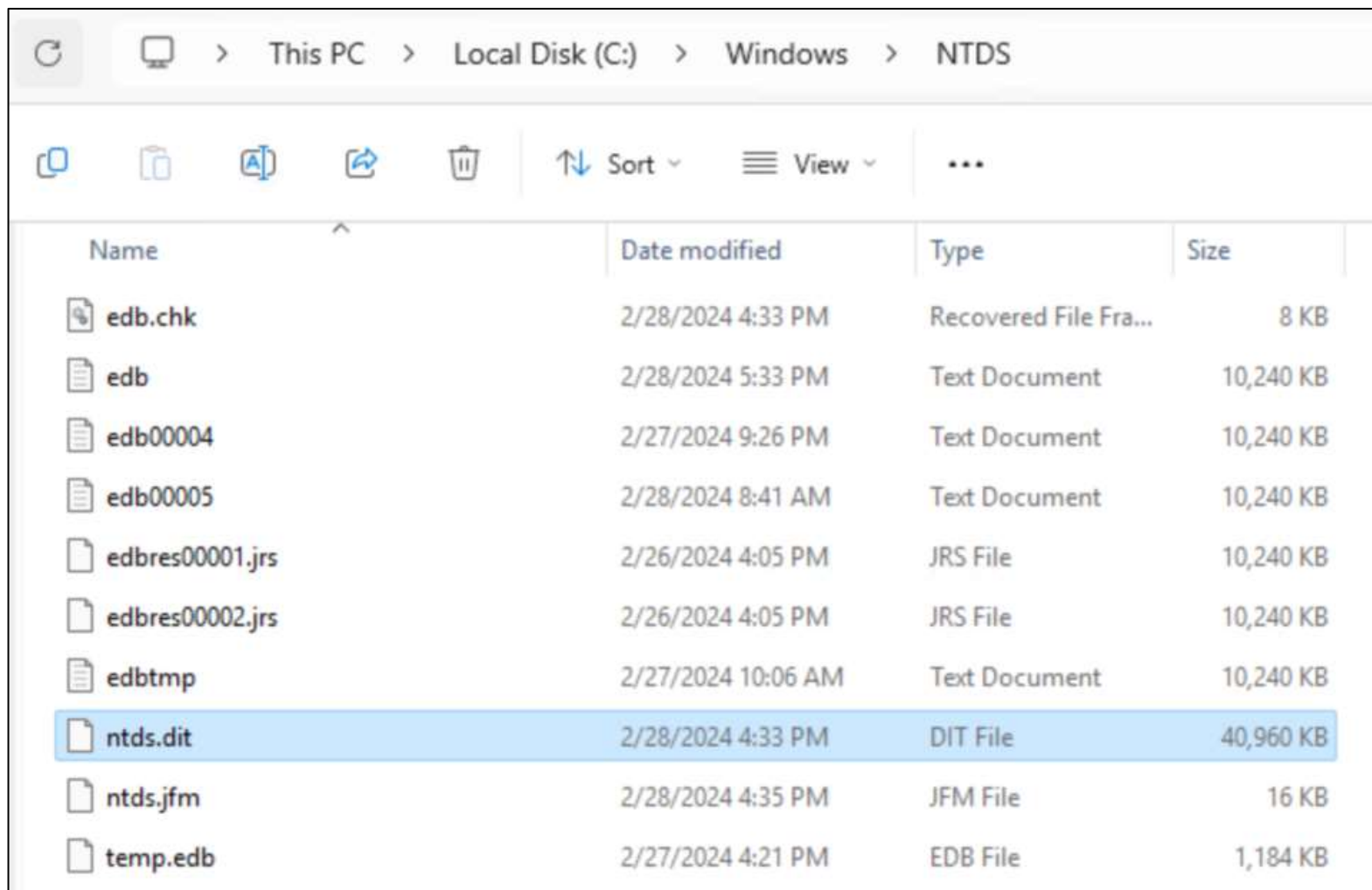
32k Database Page Size Optional Feature

Dn: DC=www4,DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com
dc: www4;
distinguishedName: DC=www4,DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com; |
dnsRecord (1275): wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 2144 dwTtlSeconds: 2693
wFlags: 0 dwSerial: 2144 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.5.9; wData
dwStartRefreshHr: 0 Data: 10.0.5.8; wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 2144
Version: 5 Rank: 240 wFlags: 0 dwSerial: 2144 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0
269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.5.5; wDataLength: 4 wType: 1; Version: 5 Rank: 240
wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 2144 dwTtlSeconds: 269352960 dwTimeo
2144 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.5.2; wDataLength: 4 wType: 1;
Data: 10.0.5.1; wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 2144 dwTtlSeconds: 2693
wFlags: 0 dwSerial: 2144 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.0.240; wD
dwStartRefreshHr: 0 Data: 10.0.0.239; wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 21
dNSTombstoned: FALSE;
dScorePropagationData (2): 2/28/2024 6:10:25 PM Central Europe Standard Time; 0x0 = ();
instanceType: 0x4 = (WRITE);
name: www4;
objectCategory: CN=Dns-Node,CN=Schema,CN=Configuration,DC=contoso,DC=com;
objectClass (2): top; dnsNode;
objectGUID: 086e9d74-bd24-4949-8990-7504ace1585c;

32k Database Page Size Optional Feature

```
Add-DnsServerResourceRecordA : Failed to create resource record www4 in zone contoso.com on server AD2025-DC.  
At line:5 char:9  
+ Add-DnsServerResourceRecordA -Name www4  
+ ~~~~~  
+ CategoryInfo          : NotSpecified: (www4:root/Microsoft/...ResourceRecordA) [Add-DnsServerResourceRecordA], C  
imException  
+ FullyQualifiedErrorId : WIN32 9005,Add-DnsServerResourceRecordA
```

32k Database Page Size Optional Feature



Name	Date modified	Type	Size
edb.chk	2/28/2024 4:33 PM	Recovered File Fra...	8 KB
edb	2/28/2024 5:33 PM	Text Document	10,240 KB
edb00004	2/27/2024 9:26 PM	Text Document	10,240 KB
edb00005	2/28/2024 8:41 AM	Text Document	10,240 KB
edbres00001.jrs	2/26/2024 4:05 PM	JRS File	10,240 KB
edbres00002.jrs	2/26/2024 4:05 PM	JRS File	10,240 KB
edbtmp	2/27/2024 10:06 AM	Text Document	10,240 KB
ntds.dit	2/28/2024 4:33 PM	DIT File	40,960 KB
ntds.jfm	2/28/2024 4:35 PM	JFM File	16 KB
temp.edb	2/27/2024 4:21 PM	EDB File	1,184 KB

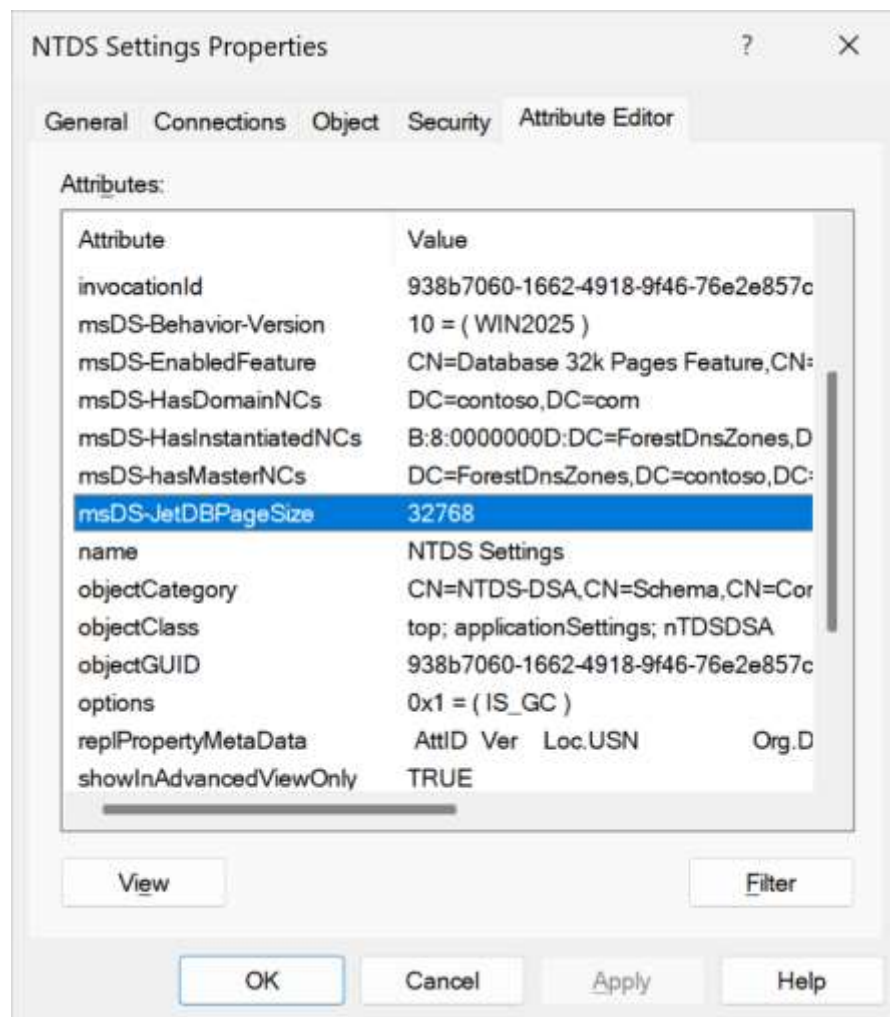
32k Database Page Size Optional Feature

```
msDS-JetGetRecordSize3      : <JetRecordSize3 version="1">
                             <cbData>5602</cbData>
                             <cbLongValueData>30780</cbLongValueData>
                             <cbOverhead>11320</cbOverhead>
                             <cbLongValueOverhead>35739</cbLongValueOverhead>
                             <cNonTaggedColumns>10</cNonTaggedColumns>
                             <cTaggedColumns>18</cTaggedColumns>
                             <cLongValues>1083</cLongValues>
                             <cMultiValues>1276</cMultiValues>
                             <cCompressedColumns>0</cCompressedColumns>
                             <cbDataCompressed>5602</cbDataCompressed>
                             <cbLongValueDataCompressed>30780</cbLongValueDataCompressed>
                             <cbIntrinsicLongValueData>5484</cbIntrinsicLongValueData>
                             <cbIntrinsicLongValueDataCompressed>5484</cbIntrinsicLongValueDataCompressed>
                             <cIntrinsicLongValues>198</cIntrinsicLongValues>
                             <cbKey>5</cbKey>
                             </JetRecordSize3>
Name                          : www4
```

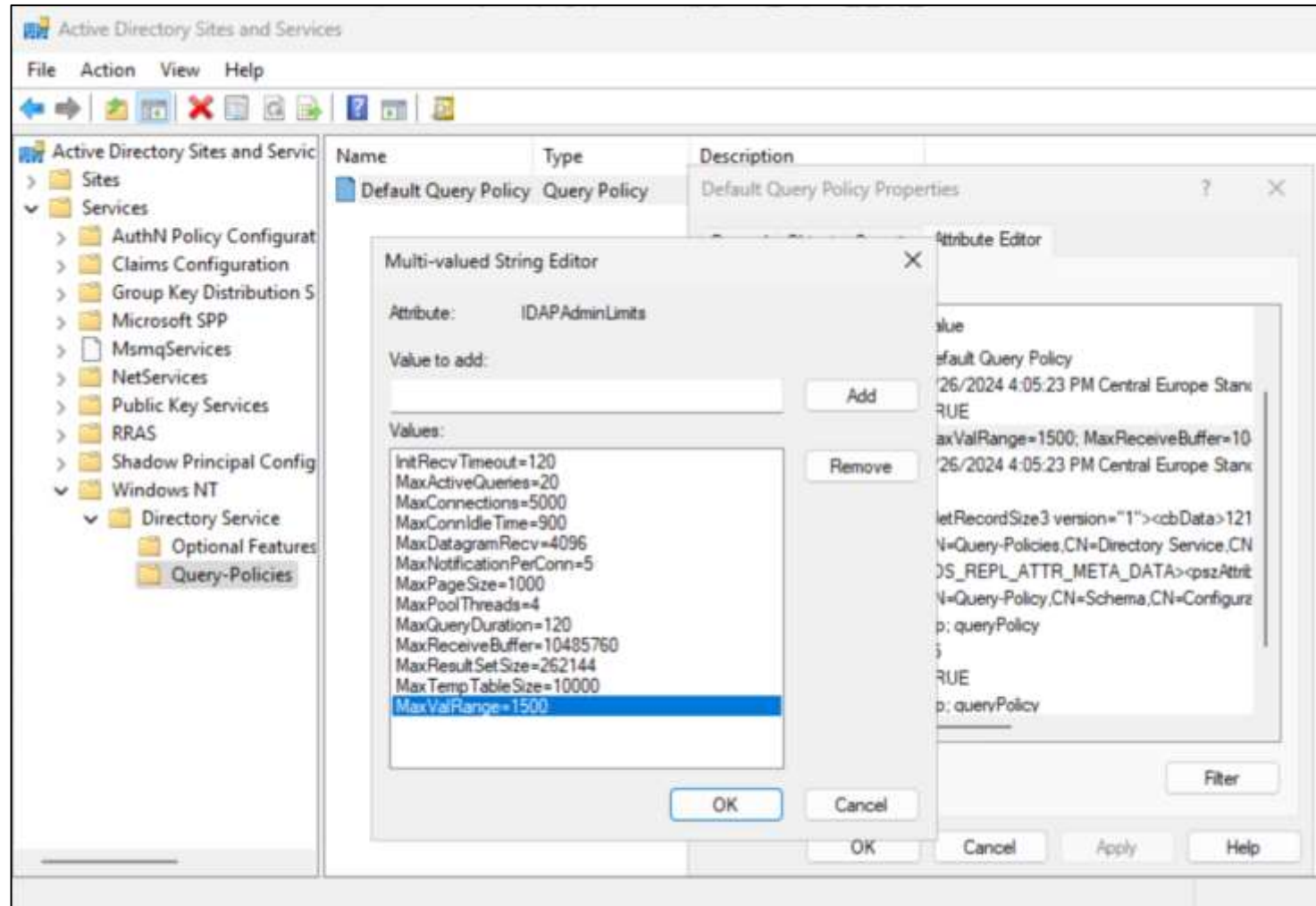
32k Database Page Size Optional Feature

```
Administrator: Windows PowerShell
PS C:\> (Get-ADOptionalFeature -Filter *).Name
Recycle Bin Feature
Privileged Access Management Feature
Database 32k Pages Feature
PS C:\> Enable-ADOptionalFeature -Identity 'Database 32k Pages Feature' `
>> -Scope ForestOrConfigurationSet `
>> -Target contoso.com `
>> -Confirm:$false
WARNING: Enabling 'Database 32k Pages Feature' on 'CN=Partitions,CN=Configuration,DC=contoso,DC=com' is an irreversible action! You will not be able to disable 'Database 32k Pages Feature' on 'CN=Partitions,CN=Configuration,DC=contoso,DC=com' if you proceed.
```

32k Database Page Size Optional Feature



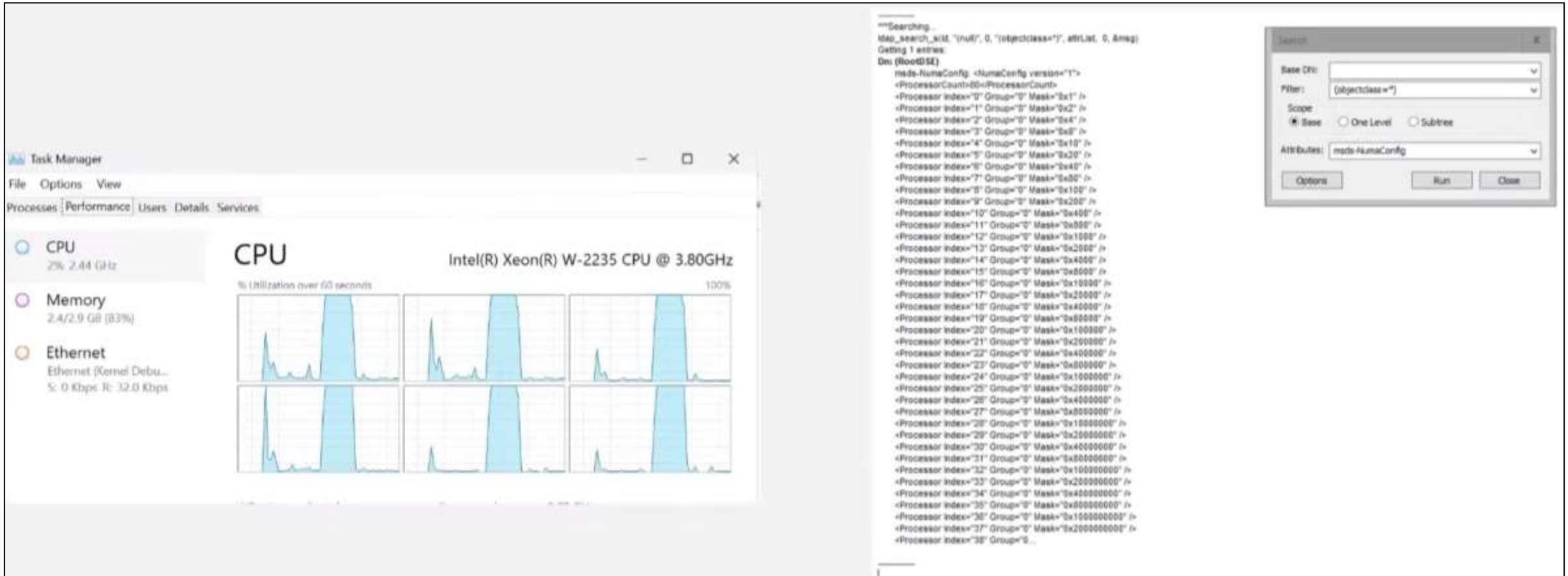
32k Database Page Size Optional Feature



32k Database Page Size Optional Feature

```
Getting 1 entries:
Dn: DC=www4,DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com
dc: www4;
distinguishedName: DC=www4,DC=contoso.com,CN=MicrosoftDNS,DC=DomainDnsZones,DC=contoso,DC=com;
dnsRecord (3240): wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 4115 dwTtlSeconds: 269352960 dwTimeout:
dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.125; wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 4115 d
4115 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.102; wDataLength: 4 wType: 1; Version: 5 Rank
Rank: 240 wFlags: 0 dwSerial: 4115 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.100; wDataLeng
wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 4115 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefre
dwStartRefreshHr: 0 Data: 10.0.64.97; wDataLength: 4 wType: 1; Version: 5 Rank: 240 wFlags: 0 dwSerial: 4115 dwTtlSeconds: 2
dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.95; wDataLength: 4 wType: 1; Version: 5 Rank: 240 v
240 wFlags: 0 dwSerial: 4115 dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.93; wDataLength: 4 w
dNSTombstoned: FALSE;
dSCorePropagationData (2): 2/28/2024 6:10:25 PM Central Europe Standard Time; 0x0 = ( );
instanceType: 0x4 = ( WRITE );
msDS-JetGetRecordSize3: <JetRecordSize3 version="1">
<cbData>142</cbData>
<cbLongValueData>91260</cbLongValueData>
<cbOverhead>32530</cbOverhead>
<cbLongValueOverhead>107019</cbLongValueOverhead>
<cNonTaggedColumns>10</cNonTaggedColumns>
<cTaggedColumns>18</cTaggedColumns>
<cLongValues>3243</cLongValues>
<cMultiValues>3241</cMultiValues>
<cCompressedColumns>0</cCompressedColumns>
<cbDataCompressed>142</cbDataCompressed>
<cbLongValueDataCompressed>91260</cbLongValueDataCompressed>
<cbIntrinsicLongValueData>24</cbIntrinsicLongValueData>
<cbIntrinsicLongValueDataCompressed>24</cbIntrinsicLongValueDataCompressed>
<clntrinsicLongValues>3</clntrinsicLongValues>
<cbKey>5</cbKey>
</JetRecordSize3>;
name: www4;
objectCategory: CN=Dns-Node,CN=Schema,CN=Configuration,DC=contoso,DC=com;
objectClass (2): top; dnsNode;
```

NUMA Support (Backported to WS2022)



Delegated Managed Service Account

Administrator: Windows PowerShell

```
PS C:\> New-ADServiceAccount -CreateDelegatedServiceAccount -Name svc_test -DNSHostName test.contoso.com
```

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

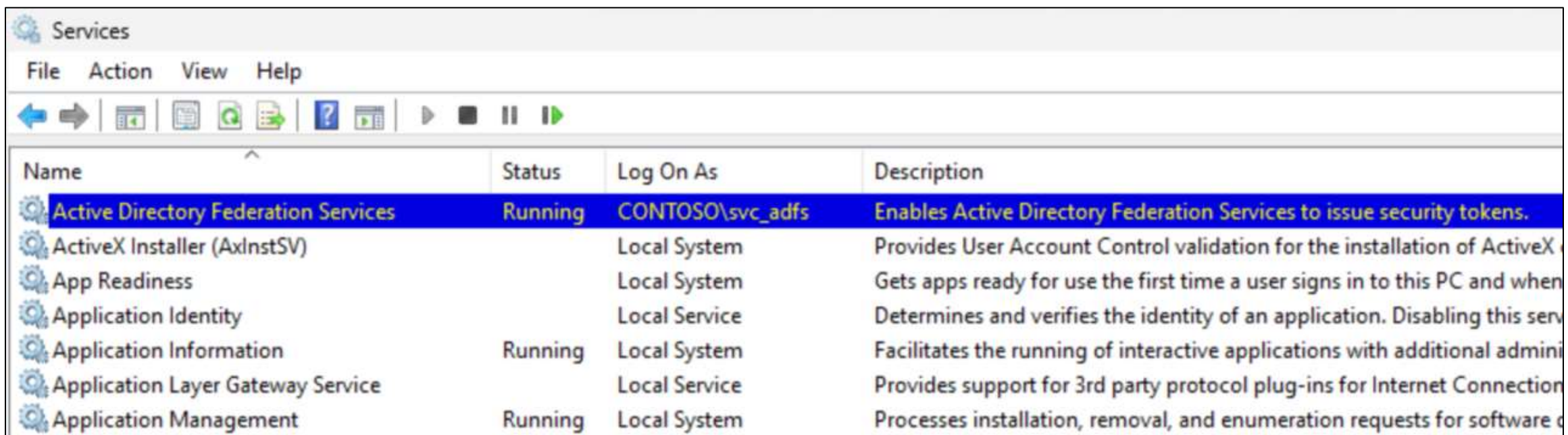
- Saved Queries
- contoso.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users

Name	Type
svc_test	msDS-DelegatedManagedServiceAccount
svc_sql_prod	msDS-GroupManagedServiceAccount
svc_gpo_backup	msDS-ManagedServiceAccount

Delegated Managed Service Account

- Uses Credential Guard (CG) to bind machine authentication
- Supports migration from existing standard service account
- Unconstrained delegation does not work with CG

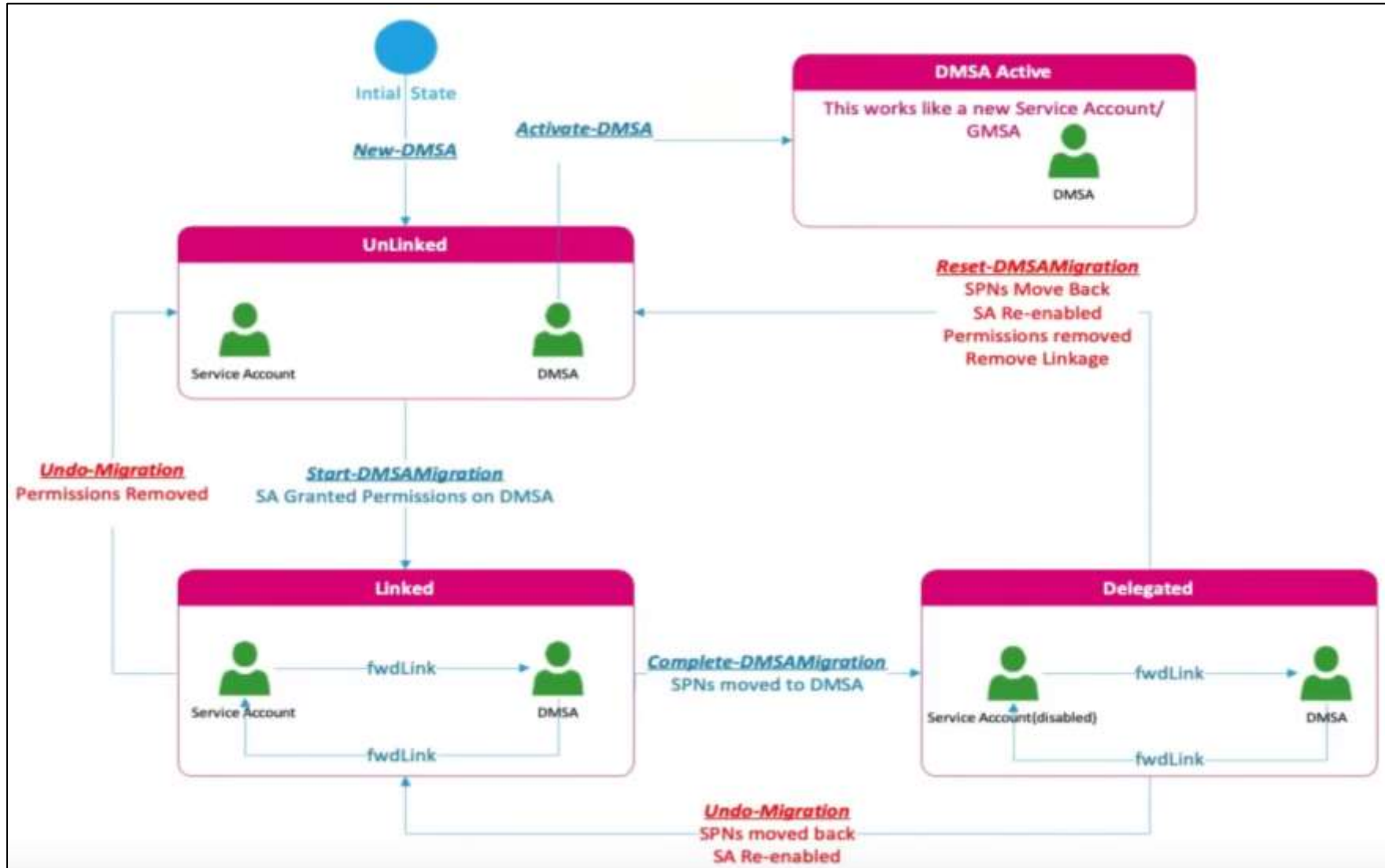
Delegated Managed Service Account



The screenshot shows the Windows Services console window. The title bar reads 'Services'. The menu bar includes 'File', 'Action', 'View', and 'Help'. The toolbar contains icons for navigation and service control. The main area displays a table of services. The 'Active Directory Federation Services' service is highlighted, showing it is running under the 'CONTOSO\svc_adfs' account. Other services listed include 'ActiveX Installer (AxInstSV)', 'App Readiness', 'Application Identity', 'Application Information', 'Application Layer Gateway Service', and 'Application Management'.

Name	Status	Log On As	Description
Active Directory Federation Services	Running	CONTOSO\svc_adfs	Enables Active Directory Federation Services to issue security tokens.
ActiveX Installer (AxInstSV)		Local System	Provides User Account Control validation for the installation of ActiveX
App Readiness		Local System	Gets apps ready for use the first time a user signs in to this PC and when
Application Identity		Local Service	Determines and verifies the identity of an application. Disabling this serv
Application Information	Running	Local System	Facilitates the running of interactive applications with additional admini
Application Layer Gateway Service		Local Service	Provides support for 3rd party protocol plug-ins for Internet Connection
Application Management	Running	Local System	Processes installation, removal, and enumeration requests for software d

Delegated Managed Service Account



Delegated Managed Service Account

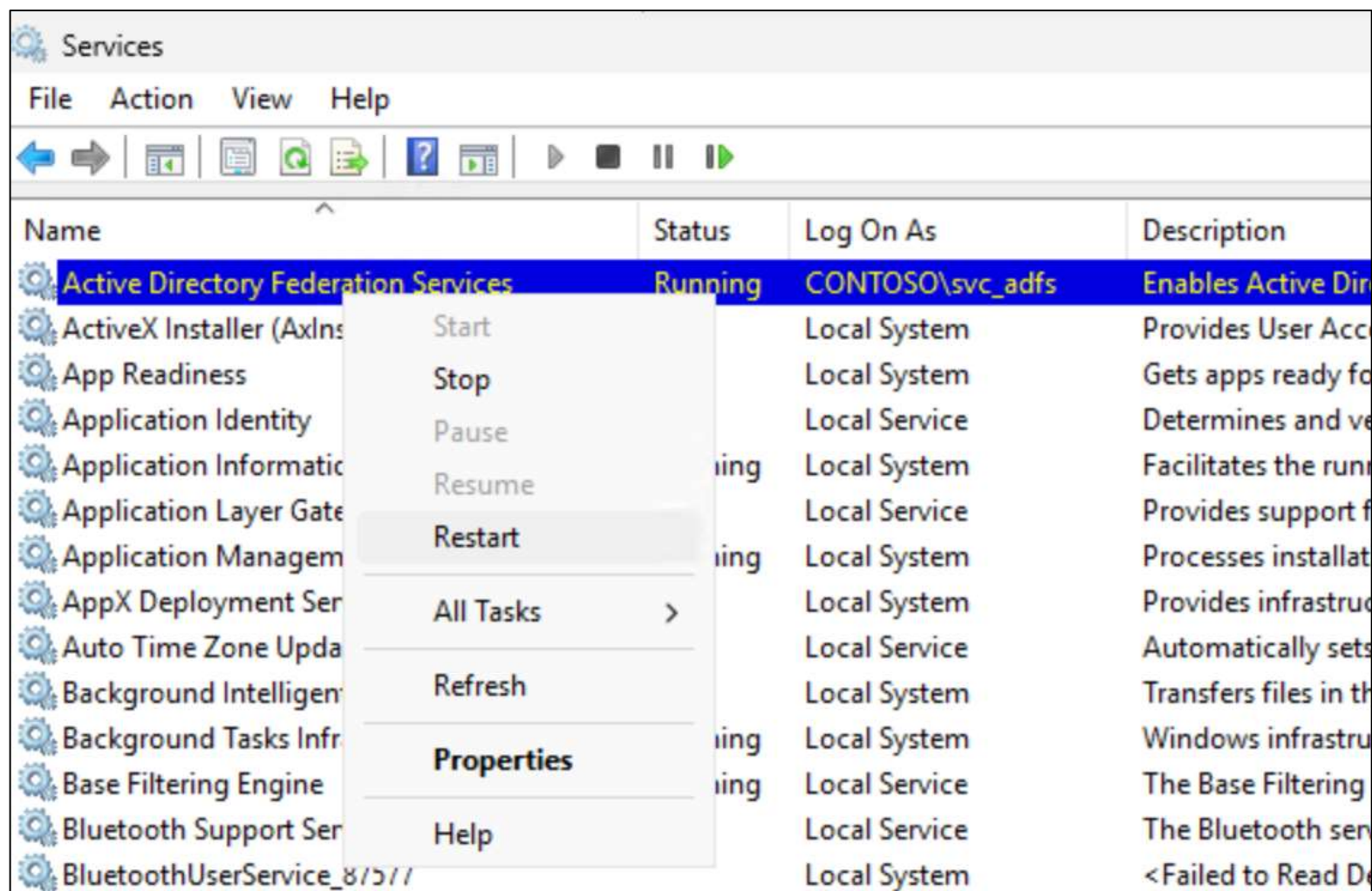
```
New-ADServiceAccount -CreateDelegatedServiceAccount `
    -Name svcd_adfs `
    -DNSHostName "login.$env:USERDNSDOMAIN" `
    -ManagedPasswordIntervalInDays 7 `
    -KerberosEncryptionType AES256

Start-ADServiceAccountMigration -Identity svcd_adfs `
    -SupersededAccount (Get-ADUser -Identity svc_adfs).DistinguishedName
```

Start-ADServiceAccountMigration

- The service account is granted Generic Read to all properties on the dMSA
- The service account is granted Write property to msDS-groupMSAMembership
- msDS-DelegatedMSAState is changed to 1
- msDS-ManagedAccountPrecededByLink is set to the service account
- msDS-SupersededAccountState is changed to 1
- msDS-SupersededManagedServiceAccountLink is set to the dMSA

Delegated Managed Service Account

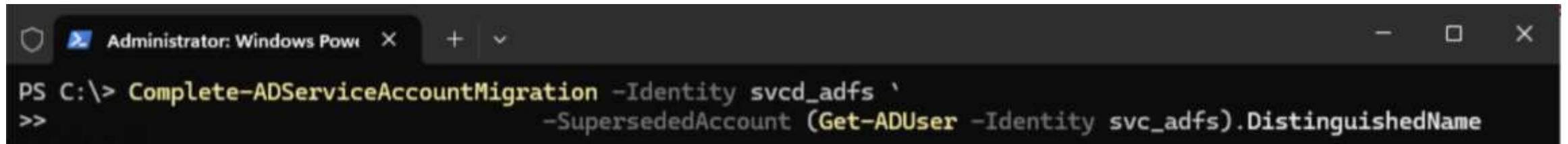


Delegated Managed Service Account

```
Administrator: Windows PowerShell
PS C:\> Get-ADServiceAccount -Identity svcd_adfs -Properties PrincipalsAllowedToRetrieveManagedPassword,
msDS-ManagedAccountPrecededByLink,msDS-DelegatedMSAState

DistinguishedName           : CN=svcd_adfs,CN=Managed Service Accounts,DC=contoso,DC=com
Enabled                     : True
msDS-DelegatedMSAState      : 1
msDS-ManagedAccountPrecededByLink : CN=svc_adfs,CN=Users,DC=contoso,DC=com
Name                        : svcd_adfs
ObjectClass                  : msDS-DelegatedManagedServiceAccount
ObjectGUID                   : 0a8b93c0-40ed-4617-a06c-70b94d0c34bd
PrincipalsAllowedToRetrieveManagedPassword : {CN=AD2025-SRV,CN=Computers,DC=contoso,DC=com}
SamAccountName               : svcd_adfs$
SID                          : S-1-5-21-3926268688-3775052234-3212022108-1107
UserPrincipalName            :
```

Delegated Managed Service Account



```
PS C:\> Complete-ADServiceAccountMigration -Identity svcd_adfs `
>> -SupersededAccount (Get-ADUser -Identity svc_adfs).DistinguishedName
```

Complete-ADServiceAccountMigration

- The service account is removed from Generic Read to all properties on the dMSA
- The service account is removed from Write property on the msDS-GroupMSAMembership attribute
- msDS-DelegatedMSAState is set to 2
- The Service Principal Names (SPN) are copied over from the service account to the dMSA account
- msDS-AllowedToDelegateTo is copied over if applicable
- msDS-AllowedToActOnBehalfOfOtherIdentity the security descriptor is copied over if applicable
- The assigned AuthN policy, msDS-AssignedAuthnPolicy, of the service account are copied over
- dMSA is added to any AuthN policy silos that the service account was a member of
- The trusted "Auth for Delegation" User Account Control (UAC) bit is copied over if it was set on the service account
- msDS-SupersededServiceAccountState is set to 2
- The service account is disabled via the UAC disable bit
- The SPN are removed from the account

Delegated Managed Service Account

```
Administrator: Windows Powe
PS C:\> Get-ADServiceAccount -Identity svcd_adfs -Properties PrincipalsAllowedToRetrieveManagedPassword,
msDS-ManagedAccountPrecededByLink,msDS-DelegatedMSAState,ServicePrincipalNames

DistinguishedName           : CN=svcd_adfs,CN=Managed Service Accounts,DC=contoso,DC=com
Enabled                     : True
msDS-DelegatedMSAState      : 2
msDS-ManagedAccountPrecededByLink : CN=svc_adfs,CN=Users,DC=contoso,DC=com
Name                        : svcd_adfs
ObjectClass                 : msDS-DelegatedManagedServiceAccount
ObjectGUID                 : 0a8b93c0-40ed-4617-a06c-70b94d0c34bd
PrincipalsAllowedToRetrieveManagedPassword : {CN=AD2025-SRV,CN=Computers,DC=contoso,DC=com}
SamAccountName              : svcd_adfs$
ServicePrincipalNames       : {host/login.contoso.com, http/login.}
SID                         : S-1-5-21-3926268688-3775052234-3212022108-1107
UserPrincipalName           :
```

Delegated Managed Service Account

svc_adfs Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Organization

User logon name:
|

User logon name (pre-Windows 2000):
CONTOSO\ svc_adfs

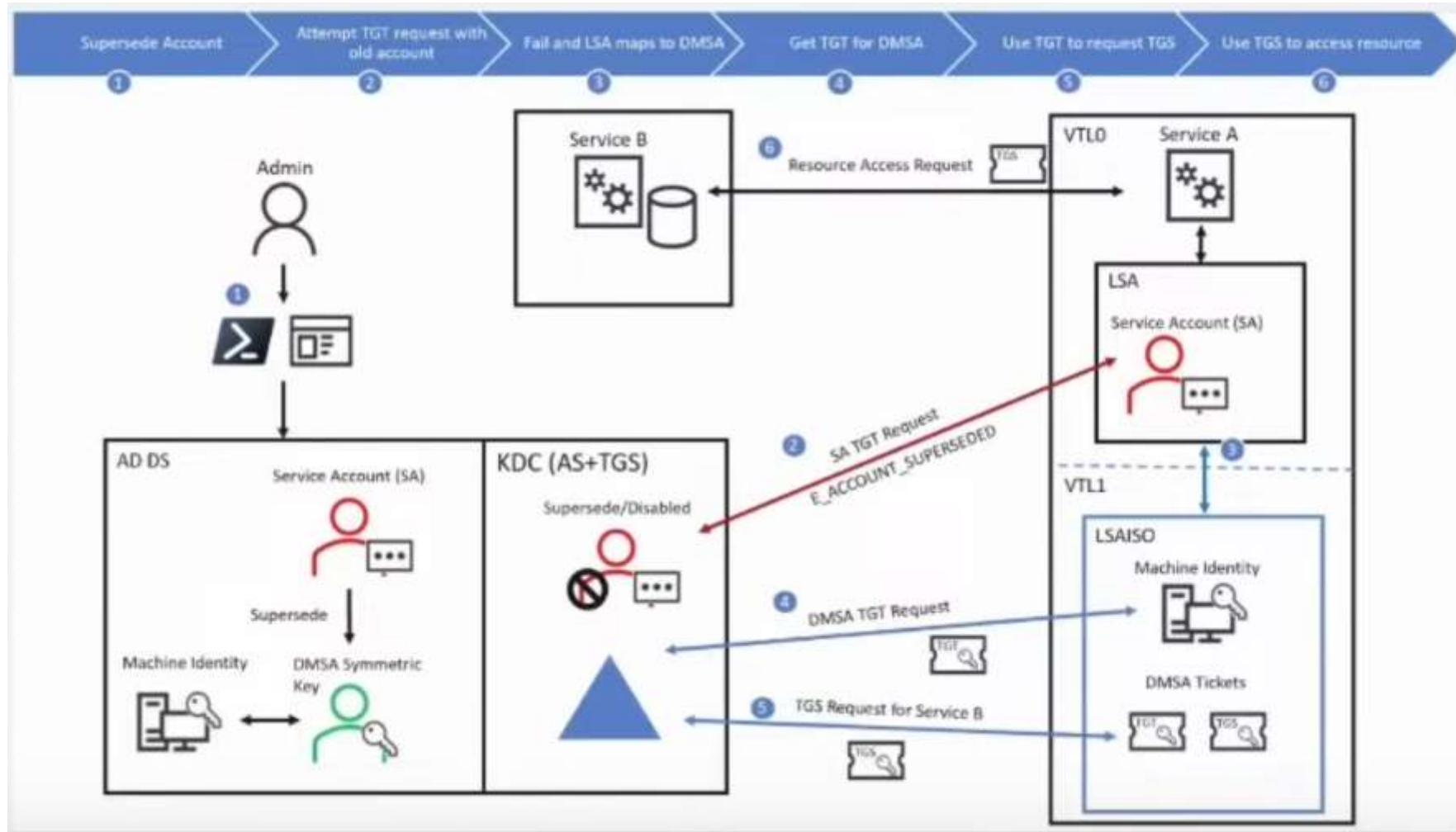
Logon Hours... Log On To...

☐ Unlock account

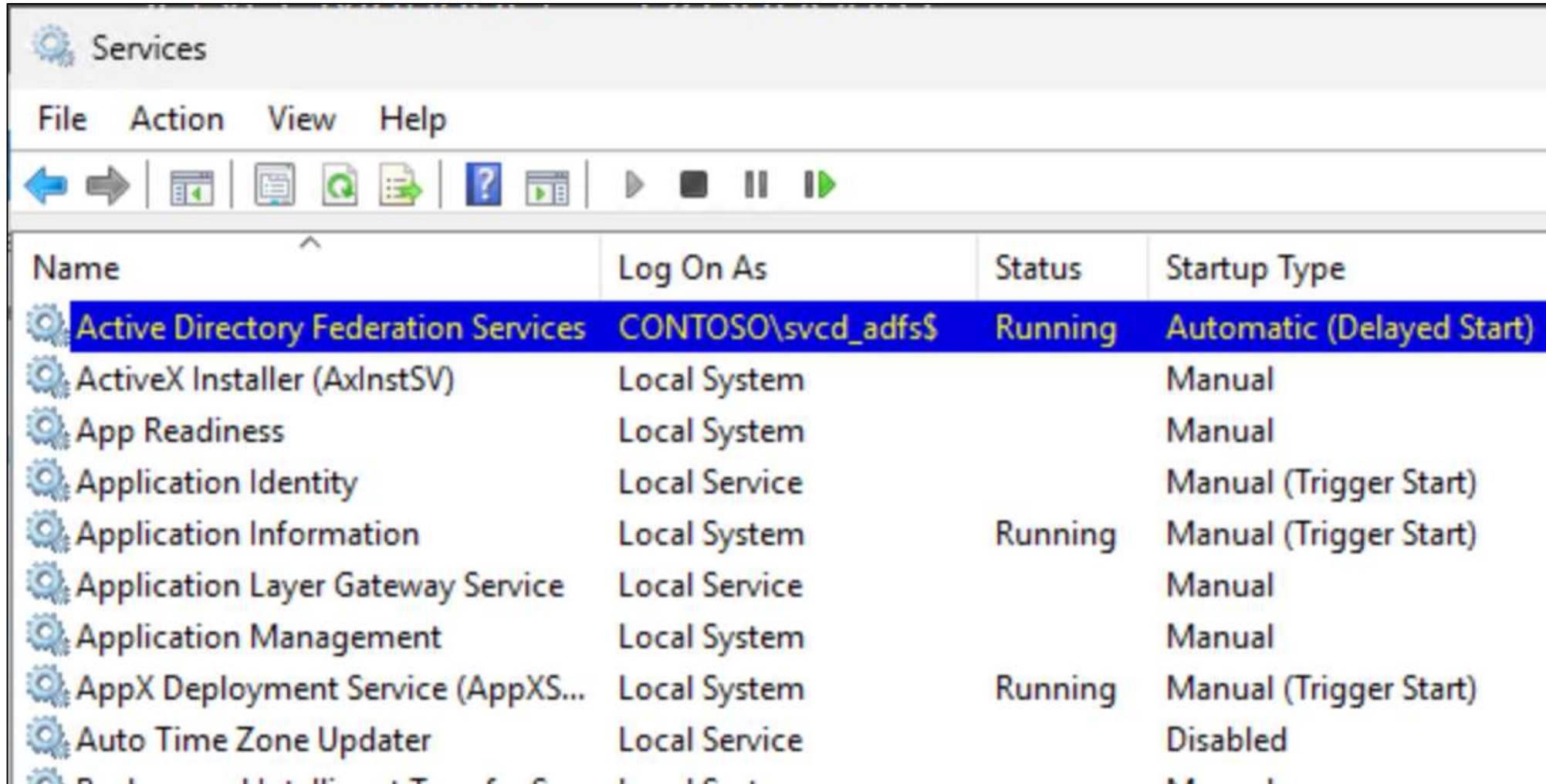
Account options:

- ☐ Store password using reversible encryption
- ☒ Account is disabled
- ☐ Smart card is required for interactive logon
- ☐ Account is sensitive and cannot be deleted

Delegated Managed Service Account



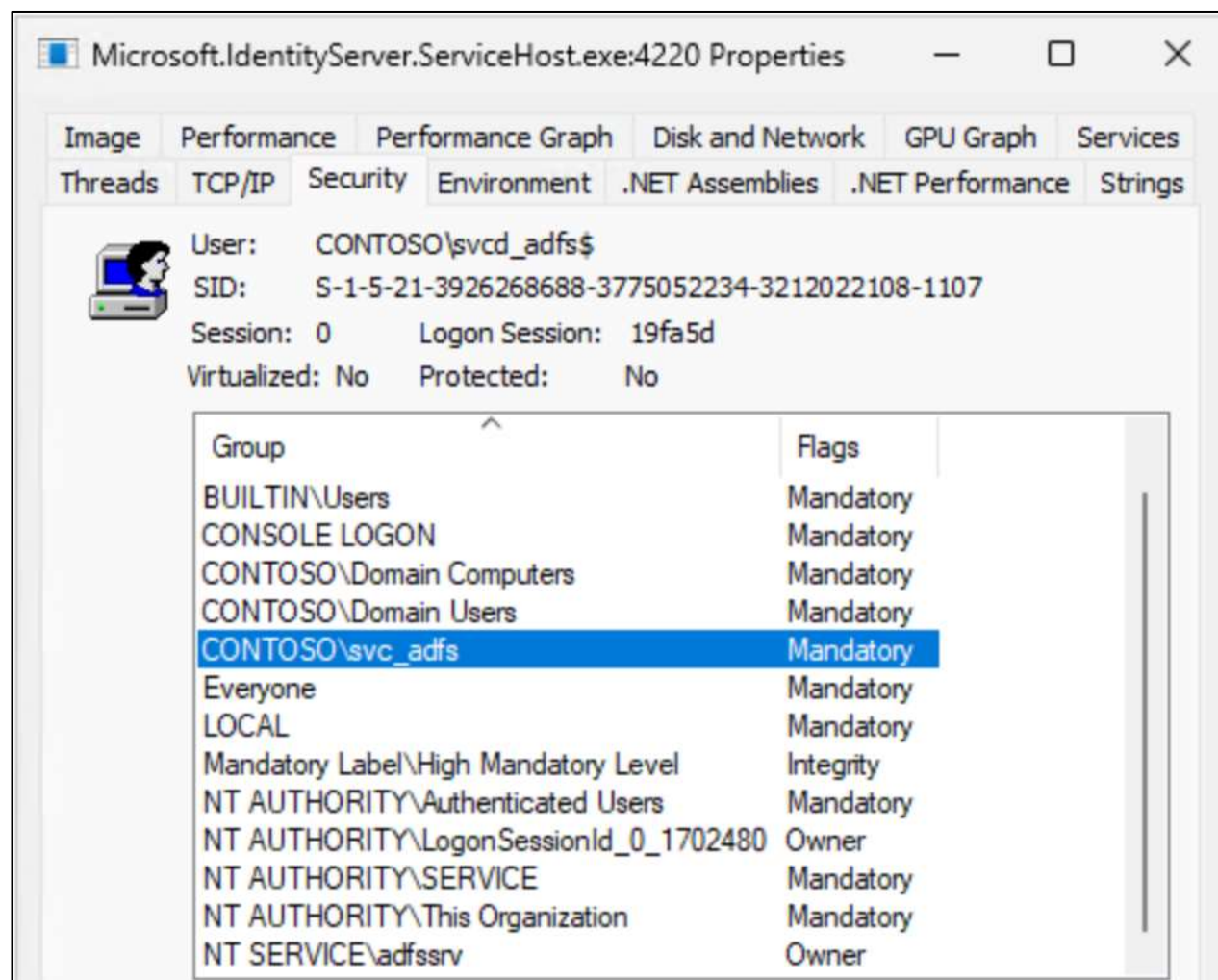
Delegated Managed Service Account



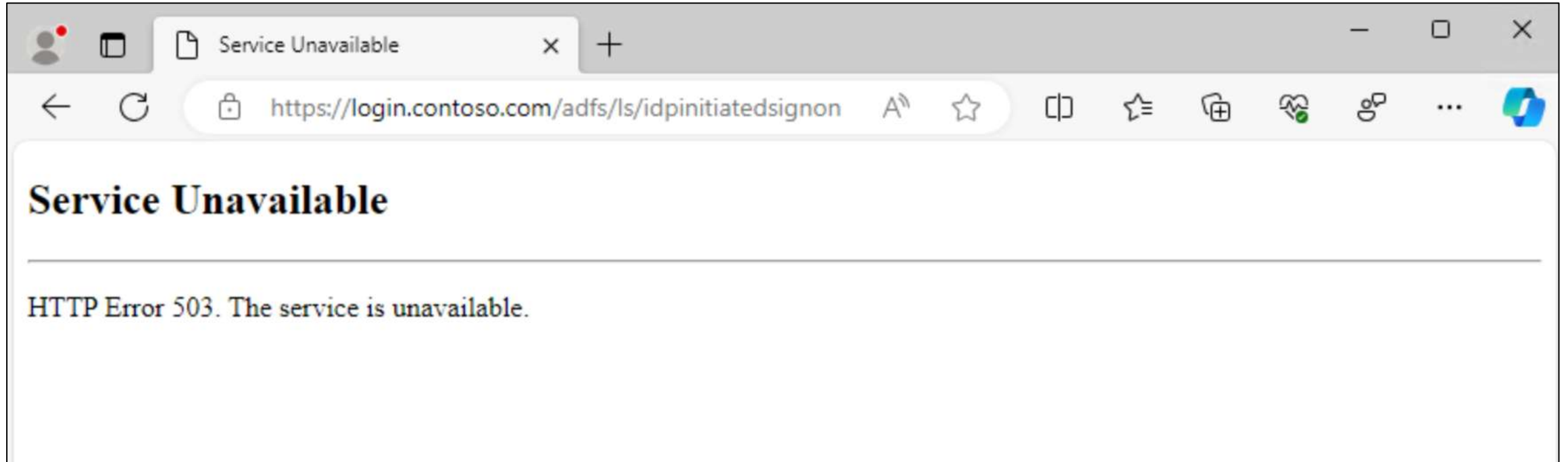
The screenshot shows the Windows Services console window. The title bar is 'Services'. The menu bar includes 'File', 'Action', 'View', and 'Help'. The toolbar contains various icons for navigation and service management. The main area is a table listing services. The first service, 'Active Directory Federation Services', is highlighted in blue. It is configured to log on as 'CONTOSO\svcd_adfs\$', is currently 'Running', and has a 'Startup Type' of 'Automatic (Delayed Start)'. Other services listed include 'ActiveX Installer (AxInstSV)', 'App Readiness', 'Application Identity', 'Application Information', 'Application Layer Gateway Service', 'Application Management', 'AppX Deployment Service (AppXS...)', and 'Auto Time Zone Updater'.

Name	Log On As	Status	Startup Type
Active Directory Federation Services	CONTOSO\svcd_adfs\$	Running	Automatic (Delayed Start)
ActiveX Installer (AxInstSV)	Local System		Manual
App Readiness	Local System		Manual
Application Identity	Local Service		Manual (Trigger Start)
Application Information	Local System	Running	Manual (Trigger Start)
Application Layer Gateway Service	Local Service		Manual
Application Management	Local System		Manual
AppX Deployment Service (AppXS...	Local System	Running	Manual (Trigger Start)
Auto Time Zone Updater	Local Service		Disabled

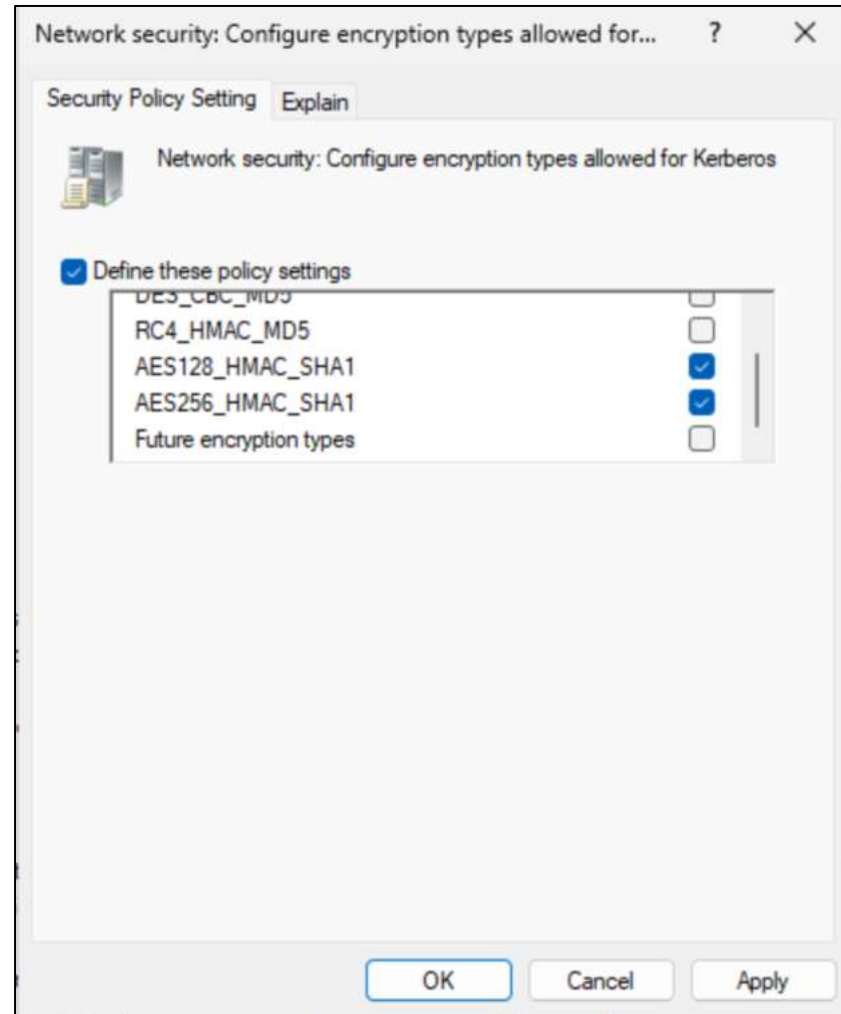
Delegated Managed Service Account



Delegated Managed Service Account



Kerberos AES SHA256 and SHA384 Support



Kerberos AES SHA256 and SHA384 Support

```
PS C:\> (Get-ADRepLAccount -SamAccountName john -Server localhost).SupplementalCredentials.KerberosNew.Credentials
```

```
AES256_CTS_HMAC_SHA384_192
```

```
Key: c72a343bef686e68b0a22378790cfc1112a4cbfef9a948e93dbe74b92eecda6d
```

```
Iterations: 4096
```

```
AES128_CTS_HMAC_SHA256_128
```

```
Key: 50175684ae022bf4c34656293277da46
```

```
Iterations: 4096
```

```
AES256_CTS_HMAC_SHA1_96
```

```
Key: 3c10ebb8bbdcc5984f76b383a4be5a017683104a6e7b455830ac8780bfbd943d
```

```
Iterations: 4096
```

```
AES128_CTS_HMAC_SHA1_96
```

```
Key: 84ae4ebcb1926532cd75282af3843f4d
```

```
Iterations: 4096
```

```
RC4_HMAC_NT
```

```
Key: 92937945b518814341de3f726500d4ff
```

```
Iterations: 4096
```

LDAP Support for TLS 1.3 (Backported to WS2022)

```
# nmap --script ssl-enum-ciphers -p 636 contoso-dc.contoso.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 22:06 CET
Nmap scan report for contoso-dc.contoso.com (10.213.0.3)
Host is up (0.0015s latency).
rDNS record for 10.213.0.3: CONTOSO-DC.contoso.com

PORT      STATE SERVICE
636/tcp   open  ldapssl
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|     cipher preference: server
|_  least strength: C
MAC Address: 00:17:FB:00:00:00 (FA)

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
```

LDAP Signing Enforced and CBT Enabled by Default

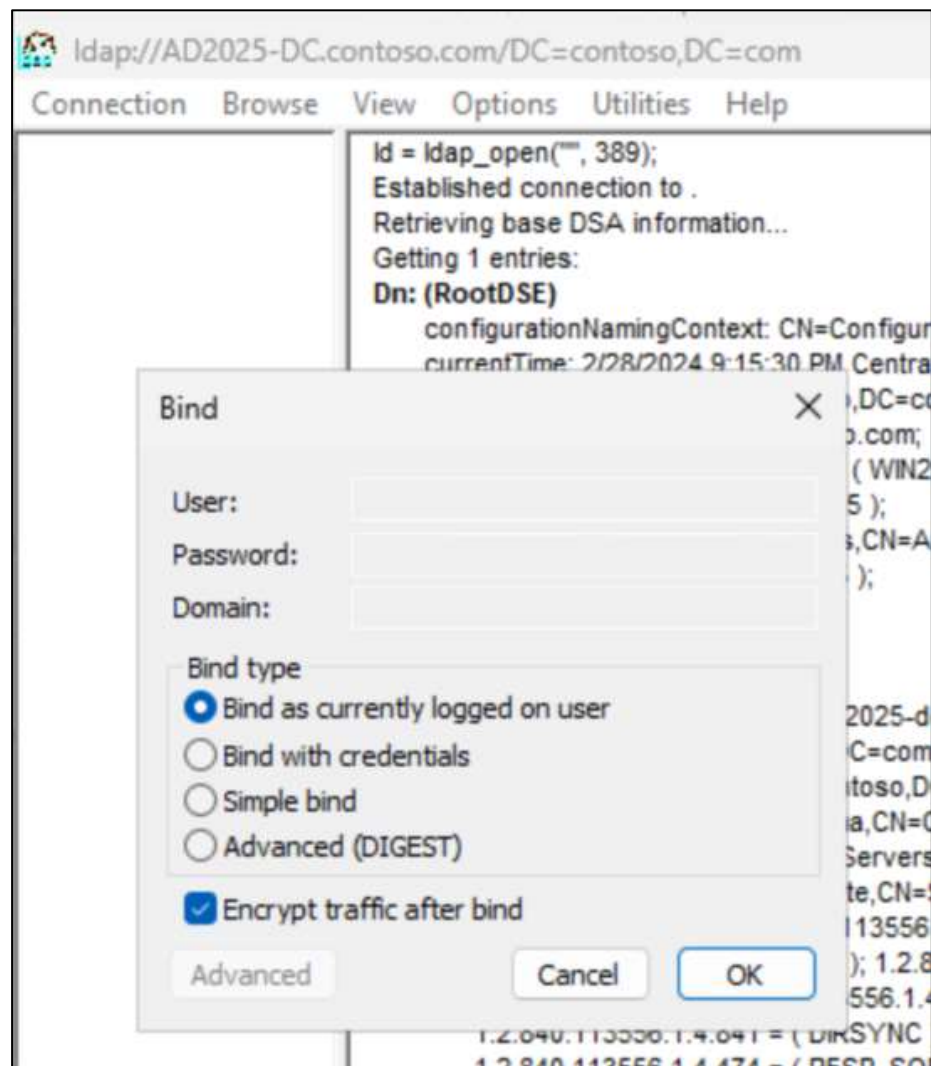
Policy	Policy Setting
 Domain controller: Allow computer account re-use during domain join	Not Defined
 Domain controller: Allow server operators to schedule tasks	Not Defined
 Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
 Domain controller: LDAP server channel binding token requirements	Not Defined
 Domain controller: LDAP server signing requirements	Not Defined
 Domain controller: LDAP server signing requirements Enforcement	Not Defined
 Domain controller: Refuse machine account password changes	Not Defined
 Domain controller: Refuse setting default machine account password	Not Defined

LDAP Channel Binding Audit Support (WS 2019+)

Domain controller: Allow computer account re-use during domain join	O:BAG:BAD:(A;;RC;;;BA)
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	Always
Domain controller: LDAP server signing requirements	Require signing
Domain controller: LDAP server signing requirements Enforcement	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain controller: Refuse setting default machine account password	Not Defined

- Event 3074: The following client performed an LDAP bind over SSL/TLS and would have failed the channel binding token validation if the directory server was configured to enforce validation of Channel Binding Tokens.
- Event 3075: The following client performed an LDAP bind over SSL/TLS and did not provide Channel Binding Information. When this directory server is configured to enforce validation of Channel Binding Tokens, this bind operation will be rejected.

LDAP Client Encryption by Default (SASL)

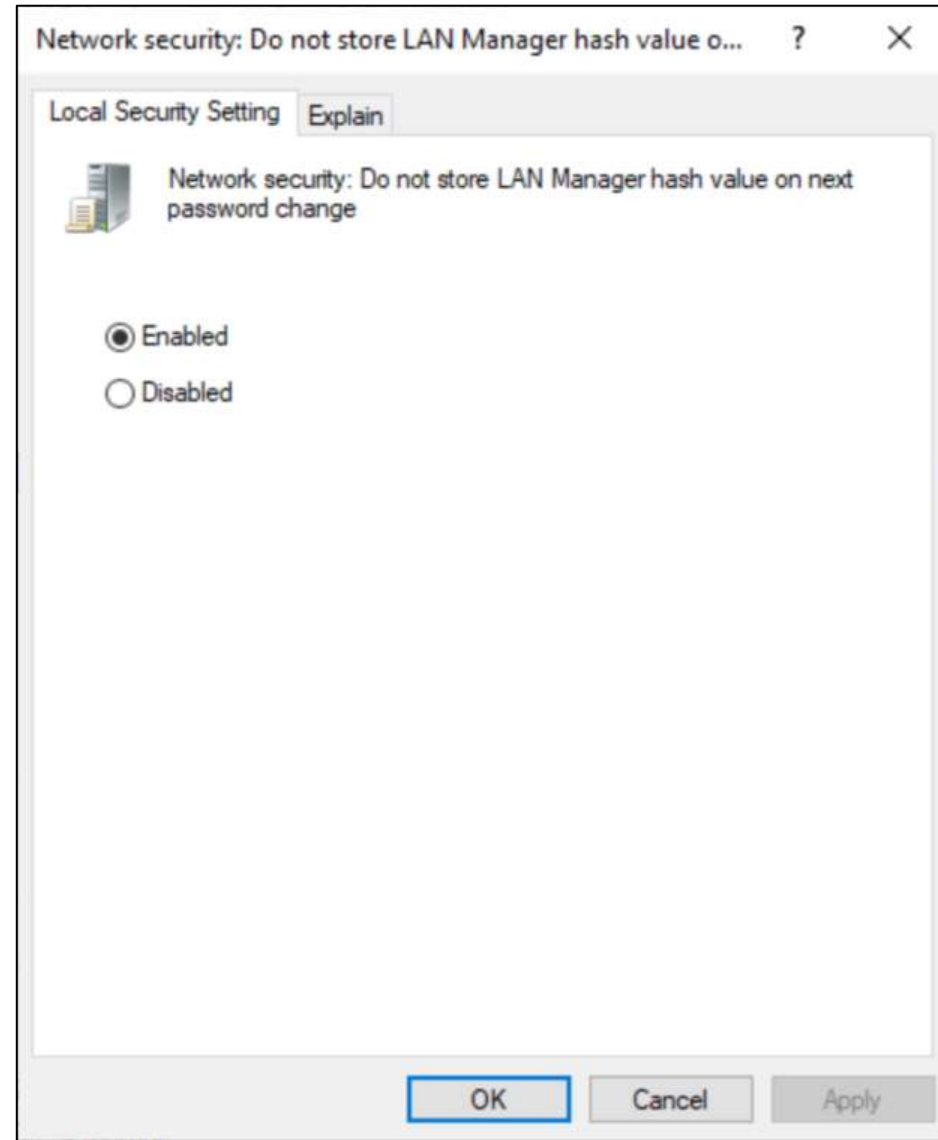


Confidential Attributes Require Encryption

```
Administrator: Windows Powe
PS C:\> Get-ADObject -Filter { objectClass -eq 'attributeSchema' -and searchFlags -band 128 } `
>> -SearchBase (Get-ADRootDSE).SchemaNamingContext -Properties LdapDisplayName |
>> Format-Wide -Property LdapDisplayName

msFVE-RecoveryPassword          msFVE-KeyPackage
msTPM-OwnerInformation          msPKI-CredentialRoamingTokens
msPKIRoamingTimeStamp          msPKIDPAPIMasterKeys
msPKIAccountCredentials        unixUserPassword
msTPM-OwnerInformationTemp      msKds-KDFAlgorithmID
msKds-KDFParam                 msKds-SecretAgreementAlgorithmID
msKds-SecretAgreementParam      msKds-PublicKeyLength
msKds-PrivateKeyLength         msKds-RootKeyData
msKds-Version                  msKds-DomainID
msKds-UseStartTime             msKds-CreateTime
msDS-TransformationRulesCompiled msDS-IssuerCertificates
msLAPS-Password                msLAPS-EncryptedPassword
msLAPS-EncryptedPasswordHistory msLAPS-EncryptedDSRMPassword
msLAPS-EncryptedDSRMPasswordHistory msLAPS-CurrentPasswordVersion
```

LAN Manager GPO Setting Removed

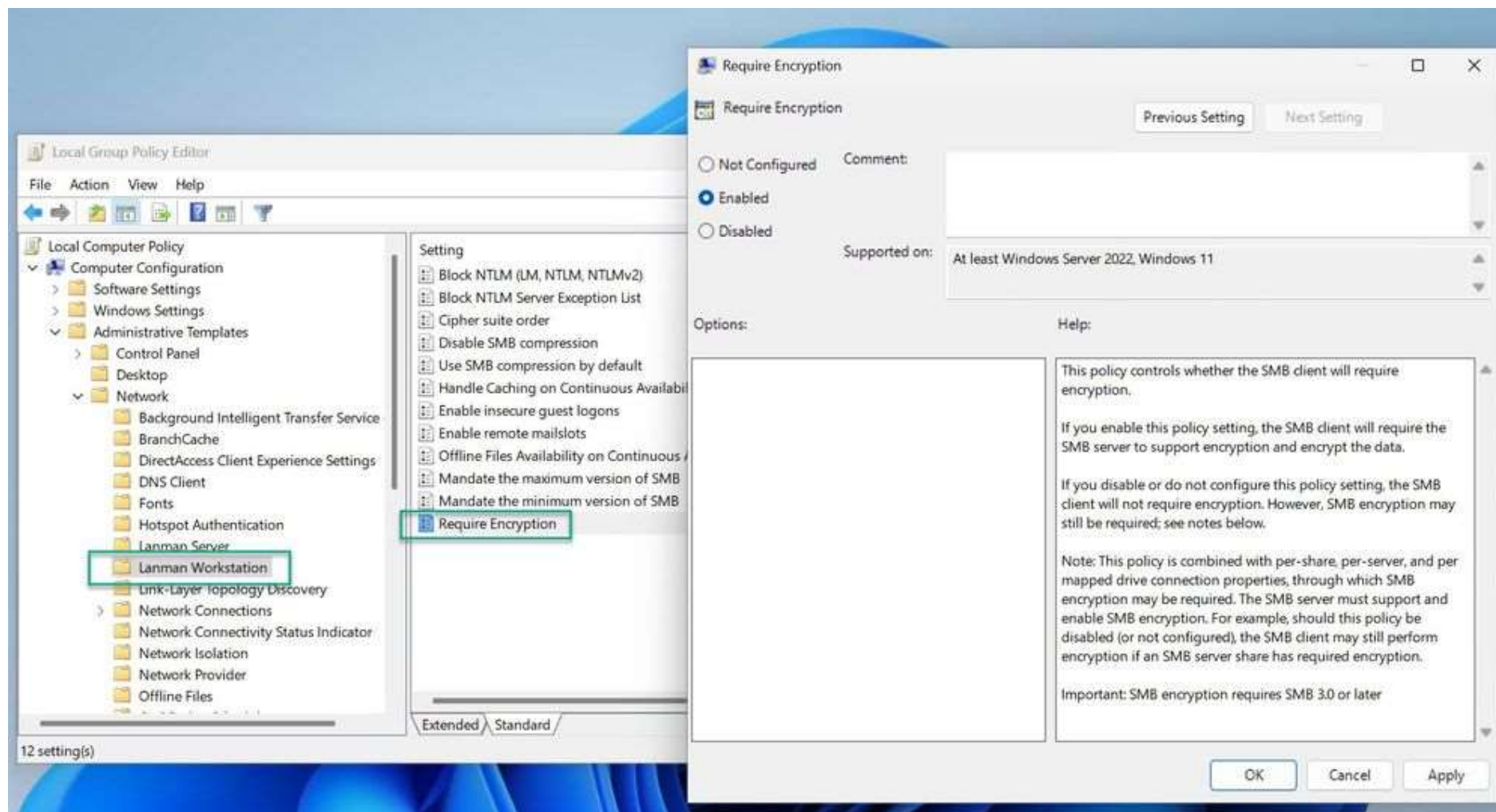


Kerberos PKINIT Support for Cryptographic Agility

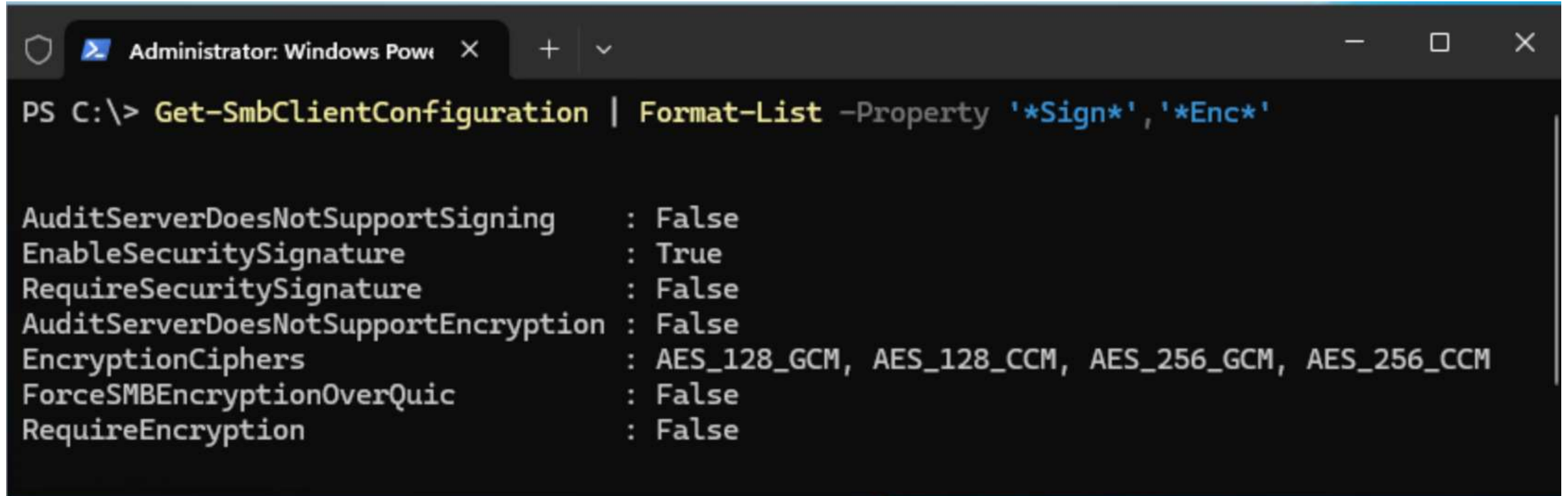
Currently supported algorithms:

- SHA1, SHA2
- RSA
- ECC (P-256 / P-384 / P-521)

Enforce SMB Encryption on Clients



Enforce SMB Encryption on Clients



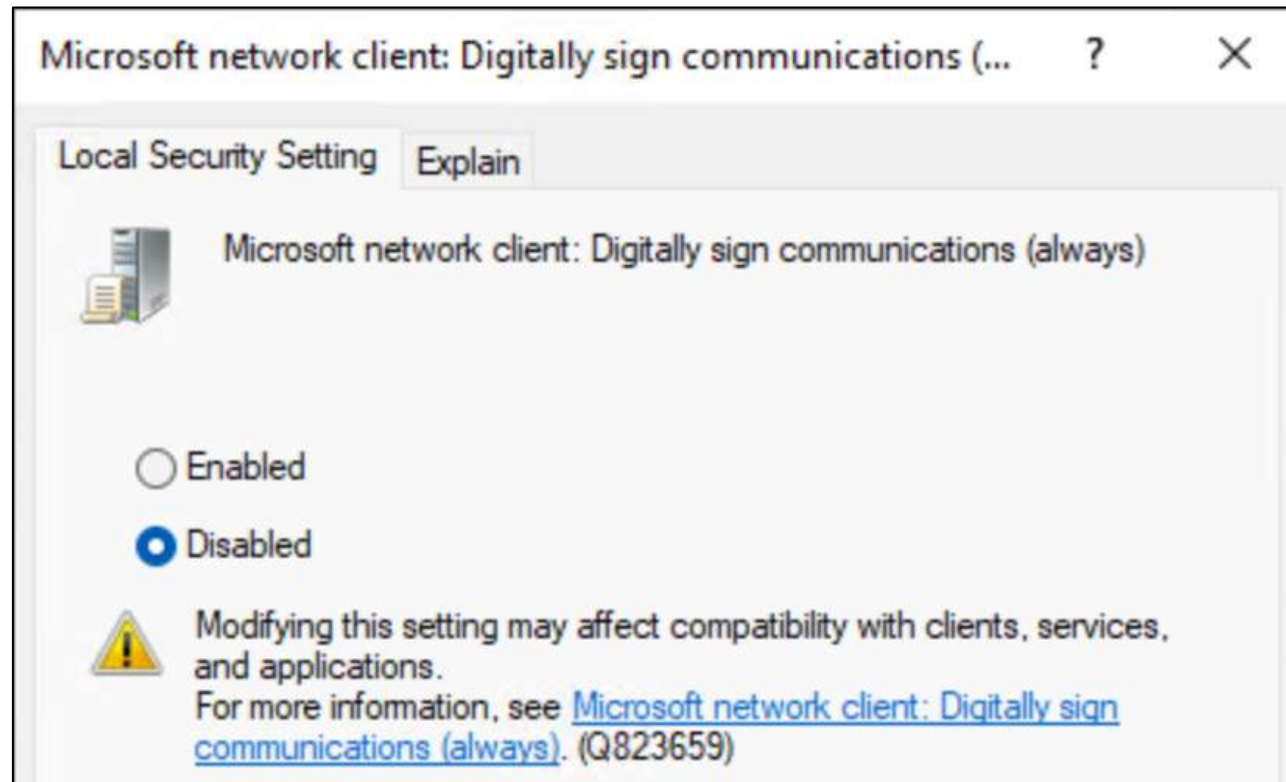
A screenshot of a Windows PowerShell terminal window. The title bar shows 'Administrator: Windows PowerShell' with standard window controls. The command prompt shows the command `Get-SmbClientConfiguration | Format-List -Property '*Sign*', '*Enc*'` being executed. The output lists several SMB-related settings and their values.

```
PS C:\> Get-SmbClientConfiguration | Format-List -Property '*Sign*', '*Enc*'

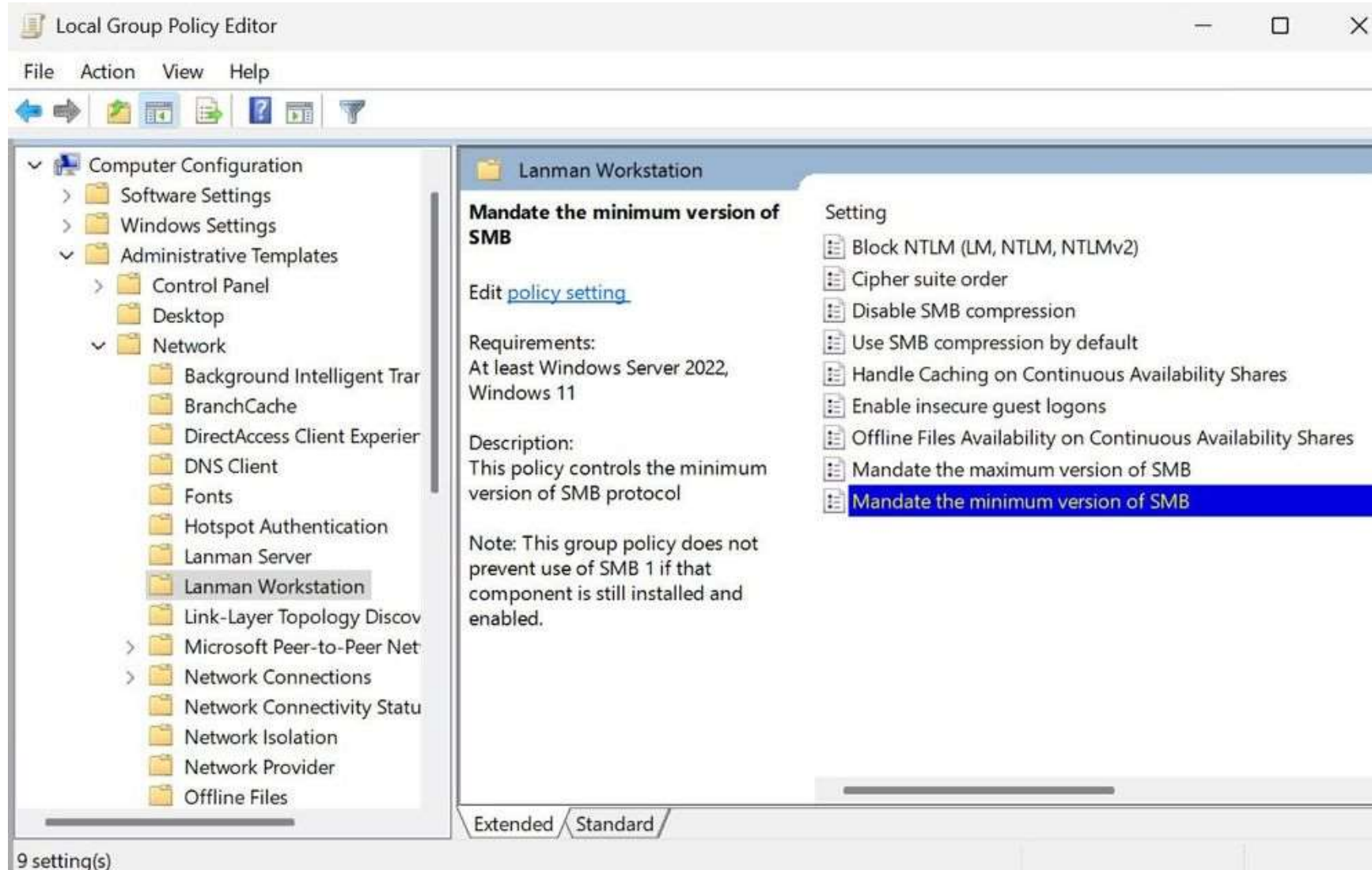
AuditServerDoesNotSupportSigning      : False
EnableSecuritySignature               : True
RequireSecuritySignature               : False
AuditServerDoesNotSupportEncryption  : False
EncryptionCiphers                     : AES_128_GCM, AES_128_CCM, AES_256_GCM, AES_256_CCM
ForceSMBEncryptionOverQuic           : False
RequireEncryption                     : False
```

SMB Client Signing Enabled by Default

SMB signing is now required by default for all SMB outbound connections where previously it was only required when connecting to shares named SYSVOL and NETLOGON on AD domain controllers.



SMB Dialect Management



SMB Dialect Management

The screenshot shows the 'Mandate the minimum version of SMB' Group Policy window. The title bar reads 'Mandate the minimum version of SMB'. Inside the window, there are navigation buttons 'Previous Setting' and 'Next Setting'. The policy is currently set to 'Enabled', indicated by a selected radio button. A 'Comment' text box is empty. The 'Supported on' section specifies 'At least Windows Server 2022, Windows 11'. Under the 'Options' section, the 'Select SMB version' dropdown menu is open, showing a list of versions: SMB 2.0.2, SMB 2.1.0, SMB 3.0.0, SMB 3.0.2, and SMB 3.1.1, with SMB 3.1.1 selected. The 'Help' section contains the text: 'This policy controls the minimum version of SMB protocol' and a note: 'Note: This group policy does not prevent use of SMB 1 if that component is still installed and enabled.' At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

Mandate the minimum version of SMB

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Windows Server 2022, Windows 11

Options:

Select SMB version:

Version: SMB 2.0.2 SMB 2.1.0 SMB 3.0.0 SMB 3.0.2 SMB 3.1.1

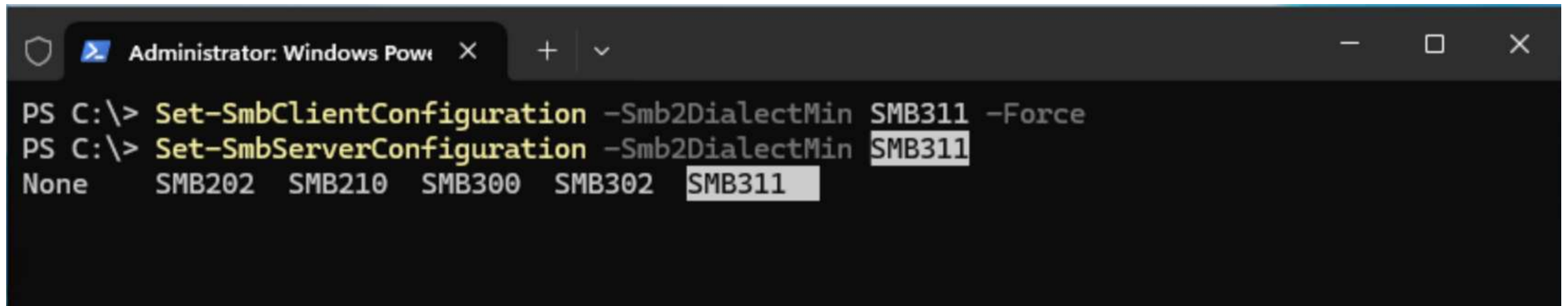
Help:

This policy controls the minimum version of SMB protocol

Note: This group policy does not prevent use of SMB 1 if that component is still installed and enabled.

OK Cancel Apply

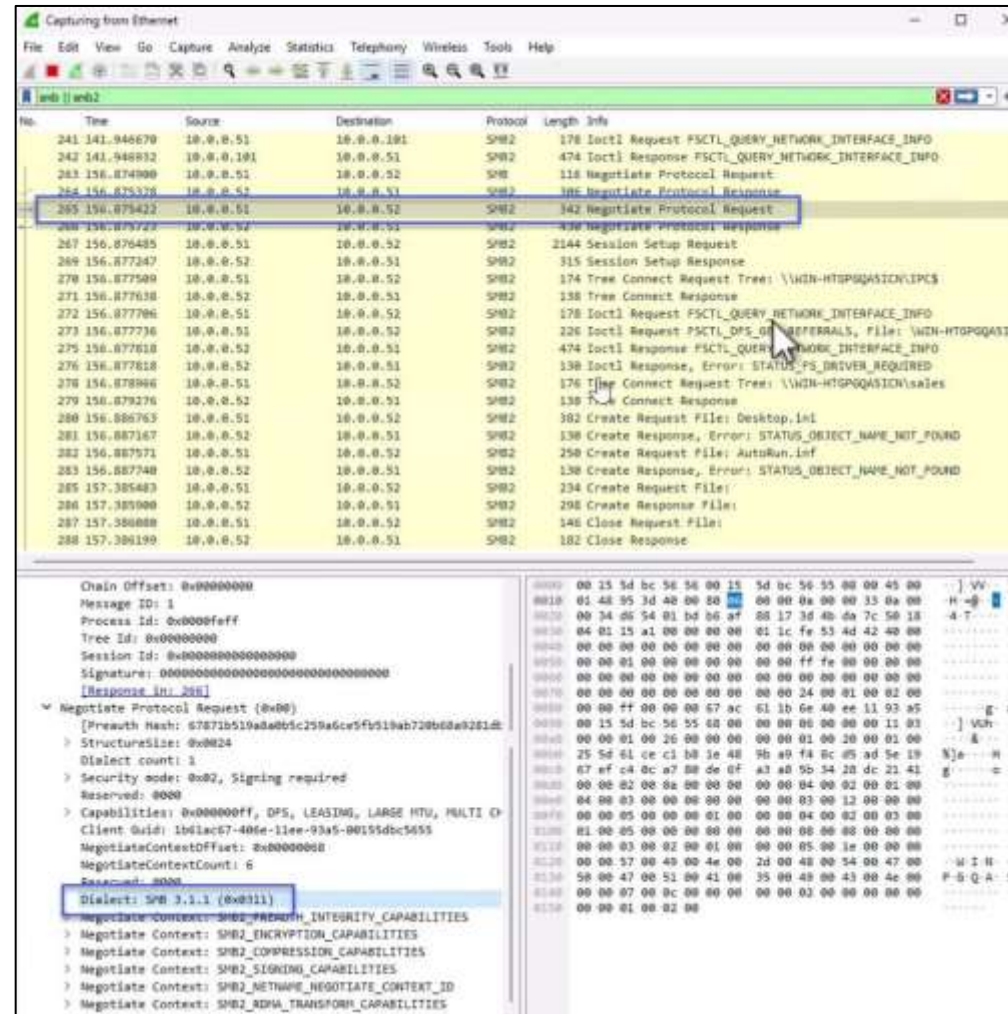
SMB Dialect Management



A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The window has a dark background and a light-colored title bar. The terminal shows two commands being executed in a PowerShell prompt (PS C:\>). The first command is `Set-SmbClientConfiguration -Smb2DialectMin SMB311 -Force`. The second command is `Set-SmbServerConfiguration -Smb2DialectMin SMB311`. Below the second command, the output of the `Get-SmbServerConfiguration` command is displayed, showing the current SMB dialect settings for the server. The output is a table with columns for the dialect name and its minimum supported version. The dialects listed are None, SMB202, SMB210, SMB300, SMB302, and SMB311. The minimum supported version for SMB311 is highlighted in a light gray box.

```
PS C:\> Set-SmbClientConfiguration -Smb2DialectMin SMB311 -Force
PS C:\> Set-SmbServerConfiguration -Smb2DialectMin SMB311
None      SMB202  SMB210  SMB300  SMB302  SMB311
```

SMB Dialect Management

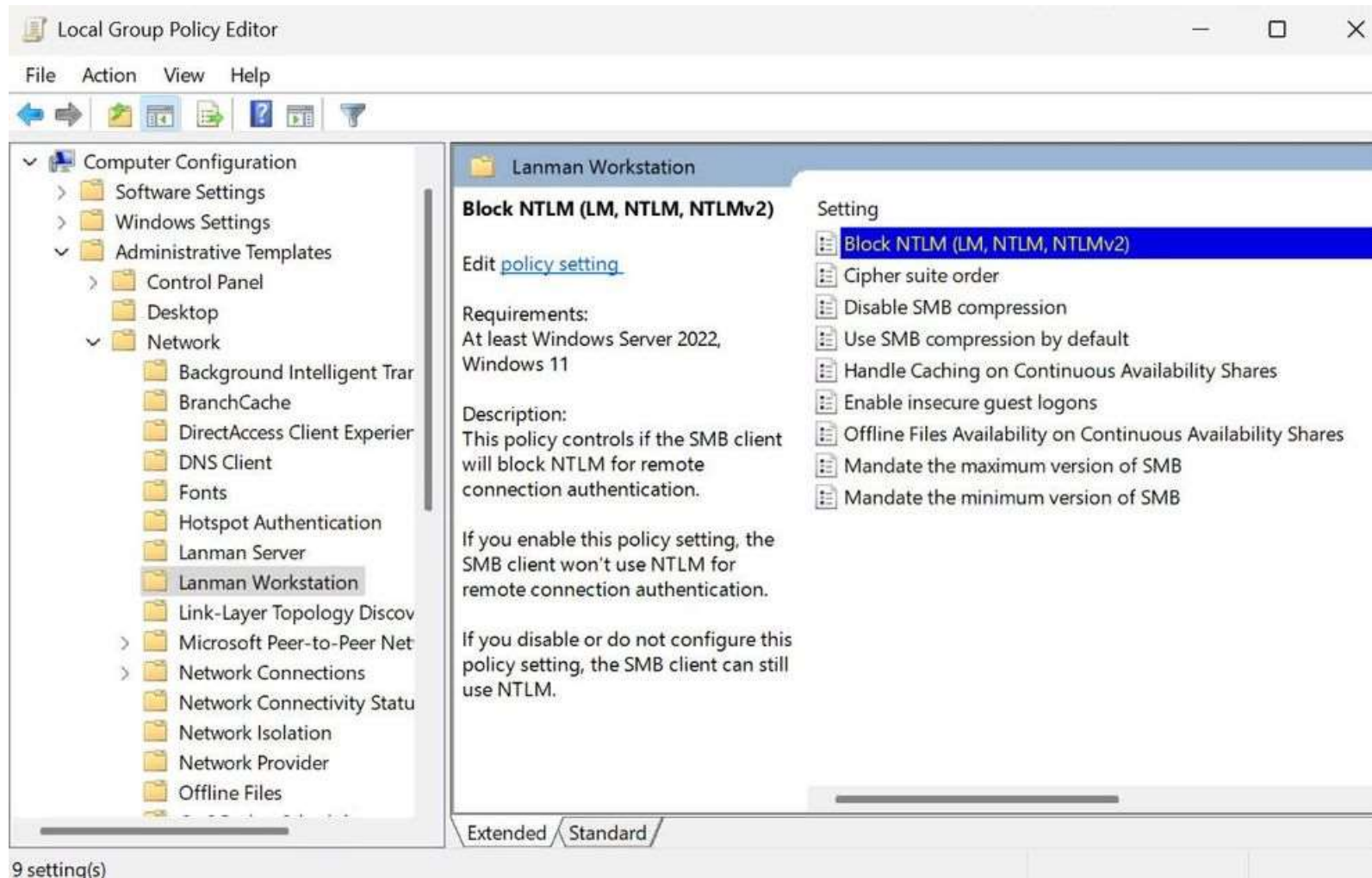


Chain Offset: 0x00000000
Message ID: 1
Process ID: 0x00000000
Tree ID: 0x00000000
Session ID: 0x0000000000000000
Signature: 00000000000000000000000000000000
[Response in 266]

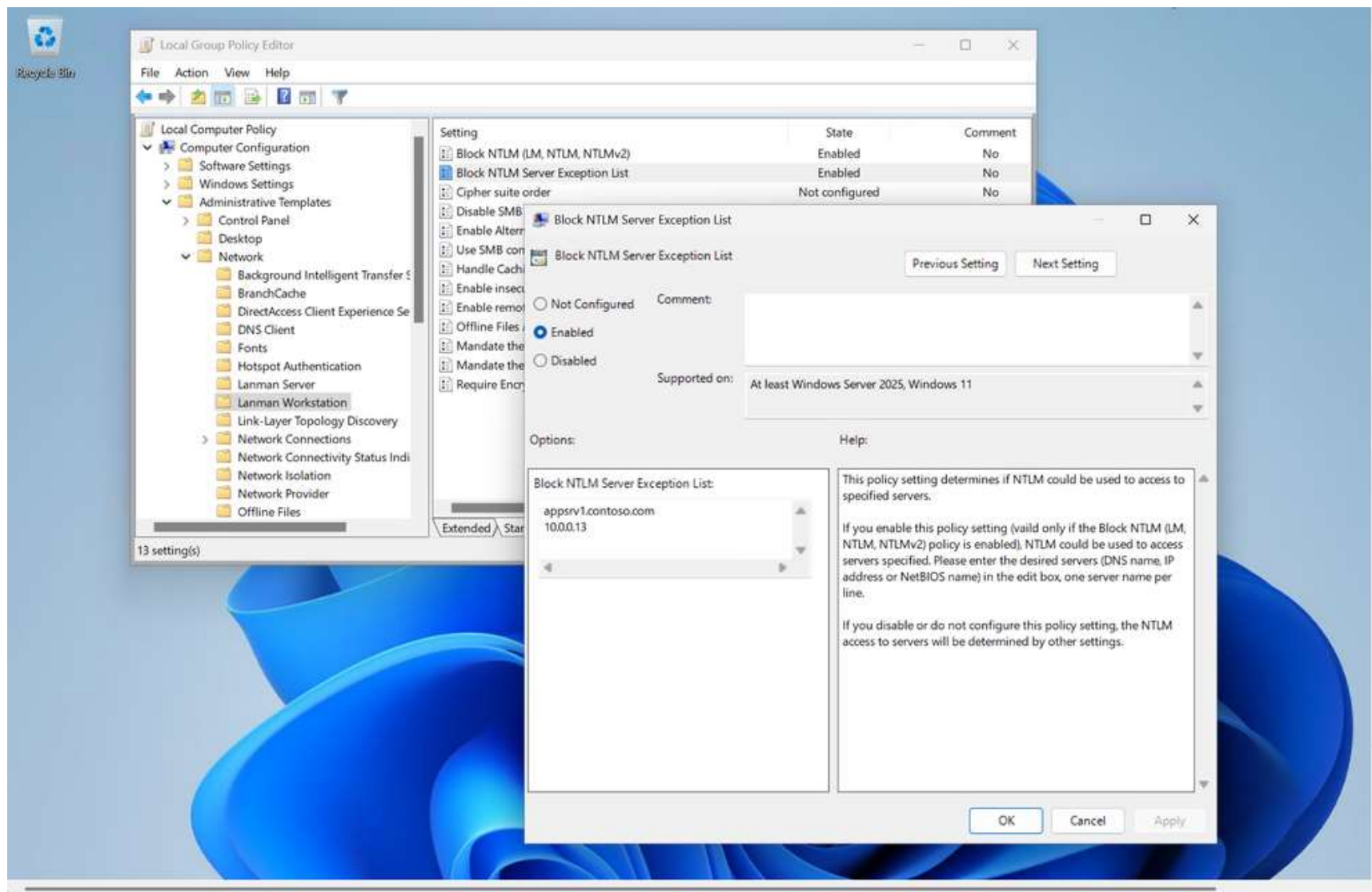
▼ Negotiate Protocol Request (0x00)
[Preamble Hash: 67871b519ada0b5c259a6ce5f519ab720b0da0281d8]
StructureSize: 0x0024
Dialect count: 1
Security mode: 0x02, Signing required
Reserved: 0000
Capabilities: 0x000000ff, DFS, LEASING, LARGE HTV, MULTI C
Client Guid: 1b1ac67-406e-11e1-9345-00155dc56555
NegotiateContextOffset: 0x00000000
NegotiateContextCount: 6
Reserved: 0000
Dialect: SMB 3.1.1 (0x0311)
Negotiate Context: SMB2_PREAMBLE_INTEGRITY_CAPABILITIES
Negotiate Context: SMB2_ENCRYPTION_CAPABILITIES
Negotiate Context: SMB2_COMPRESSION_CAPABILITIES
Negotiate Context: SMB2_SIGNING_CAPABILITIES
Negotiate Context: SMB2_NETWORK_NEGOTIATE_CONTEXT_ID
Negotiate Context: SMB2_REMOTE_TRANSFORM_CAPABILITIES

0000 00 15 5d bc 56 56 00 15 5d bc 56 55 00 00 45 00 ...
0010 01 48 95 3d 40 00 80 00 00 0a 00 00 33 0a 00 ...
0020 00 34 d6 54 01 bd b6 af 88 17 3d 4b da 7c 50 18 ...
0030 04 01 15 a1 00 00 00 00 01 1c fe 53 4d 42 40 00 ...
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0050 00 00 01 00 00 00 00 00 00 00 ff fe 00 00 00 ...
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
0070 00 00 00 00 00 00 00 00 00 00 24 01 00 02 00 ...
0080 00 00 ff 00 00 00 67 ac 61 1b 6e 40 ee 11 93 a5 ...
0090 00 15 5d bc 56 55 00 00 00 00 06 00 00 00 11 03 ...
00a0 00 00 01 00 26 00 00 00 00 01 00 20 00 01 00 ...
00b0 25 5d 61 ce c1 b0 1e 40 9b a9 f4 8c 05 ad 5e 19 ...
00c0 67 ef c4 0c a7 80 de 0f a3 a0 90 34 20 dc 21 41 ...
00d0 00 00 02 00 0a 00 00 00 00 04 00 02 00 01 00 ...
00e0 04 00 03 00 00 00 00 00 00 03 00 12 00 00 00 ...
00f0 00 00 05 00 00 00 01 00 00 04 00 02 00 03 00 ...
0100 01 00 05 00 00 00 00 00 00 00 05 00 00 00 00 ...
0110 00 00 03 00 02 00 01 00 00 00 05 00 1e 00 00 00 ...
0120 00 00 57 00 49 00 4e 00 2d 00 48 00 54 00 47 00 ...
0130 50 00 47 00 51 00 41 00 35 00 48 00 43 00 4e 00 ...
0140 00 00 07 00 0c 00 00 00 00 00 03 00 00 00 00 00 ...
0150 00 00 01 00 02 00

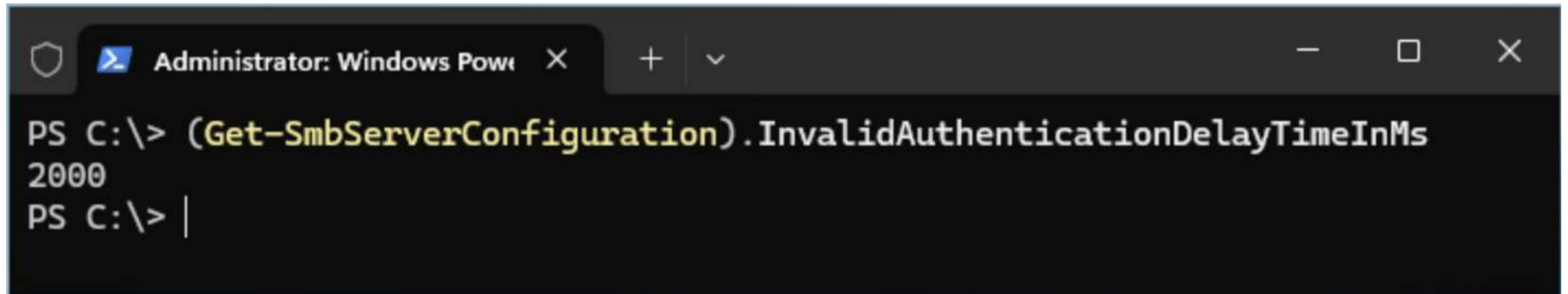
SMB Client NTLM Authentication Blocking



SMB Client NTLM Authentication Blocking



SMB Authentication Rate Limiter

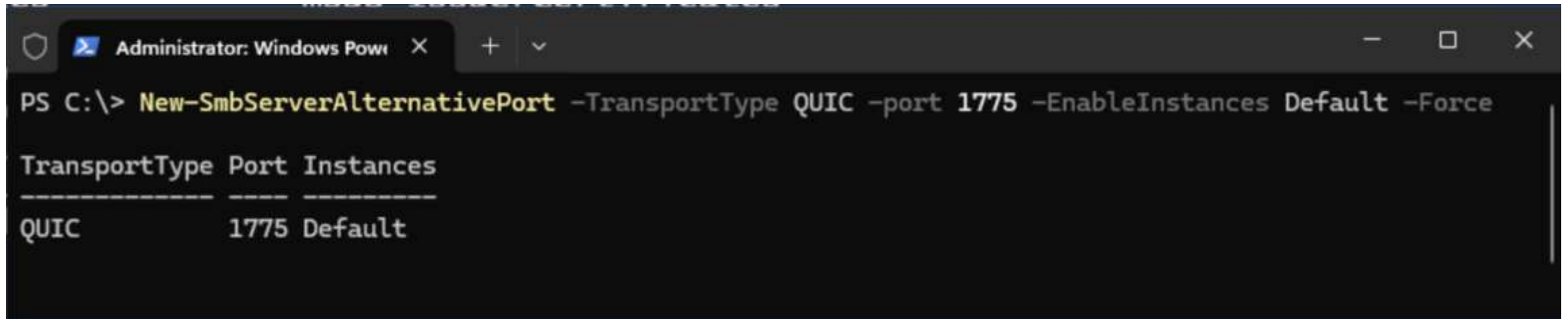


```
Administrator: Windows PowerShell
PS C:\> (Get-SmbServerConfiguration).InvalidAuthenticationDelayTimeInMs
2000
PS C:\> |
```

SMB Alternative Ports

Protocol	Default Port
SMB over NetBIOS	TCP/139
SMP over IP	TCP/445
SMB over QUIC	UDP/443
SMB Direct (RDMA)	TCP/5445

SMB Alternative Ports



A screenshot of a Windows PowerShell terminal window. The title bar shows 'Administrator: Windows PowerShell' with standard window controls. The command prompt shows the command: `New-SmbServerAlternativePort -TransportType QUIC -port 1775 -EnableInstances Default -Force`. The output is a table with three columns: TransportType, Port, and Instances. The table contains one row: QUIC, 1775, Default.

```
PS C:\> New-SmbServerAlternativePort -TransportType QUIC -port 1775 -EnableInstances Default -Force
```

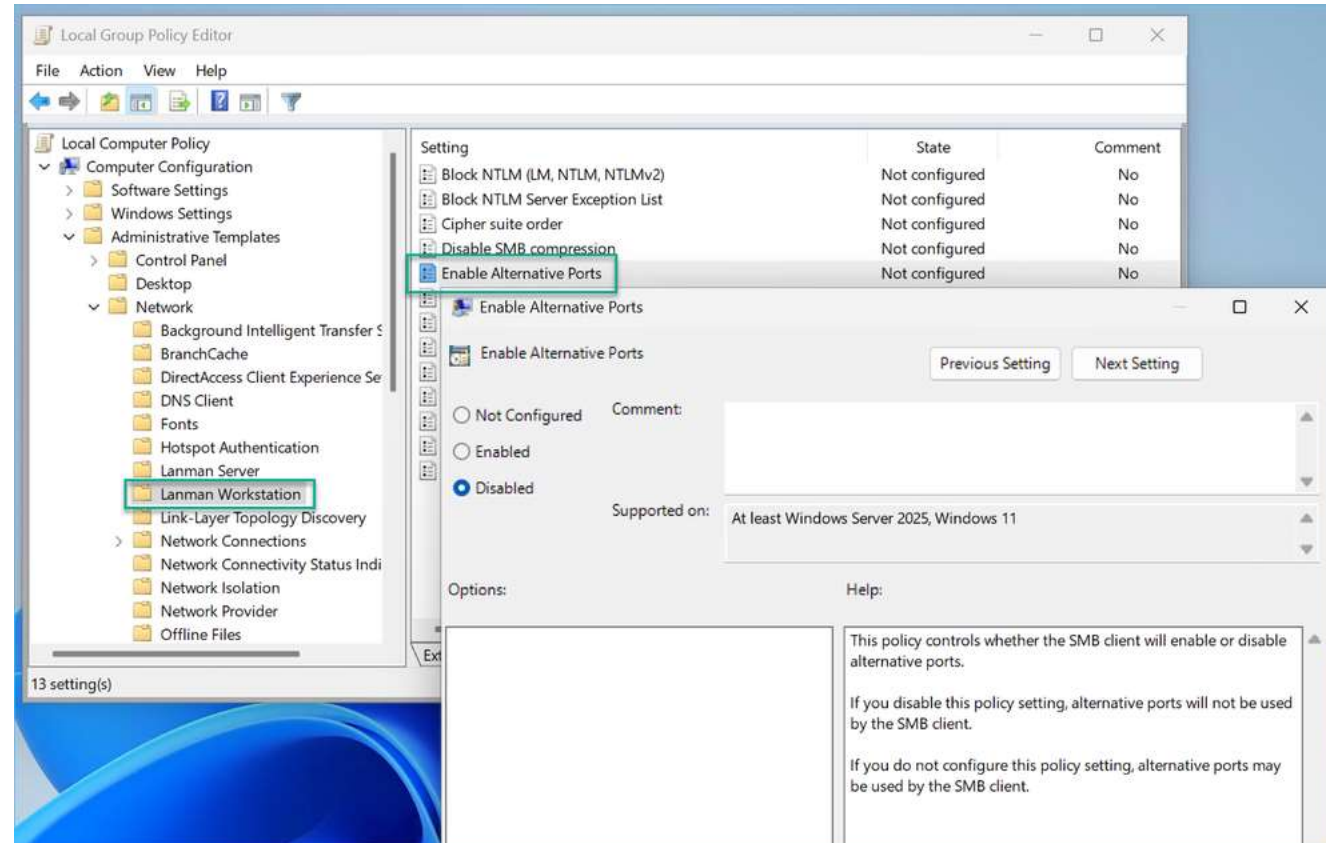
TransportType	Port	Instances
QUIC	1775	Default

SMB Alternative Ports

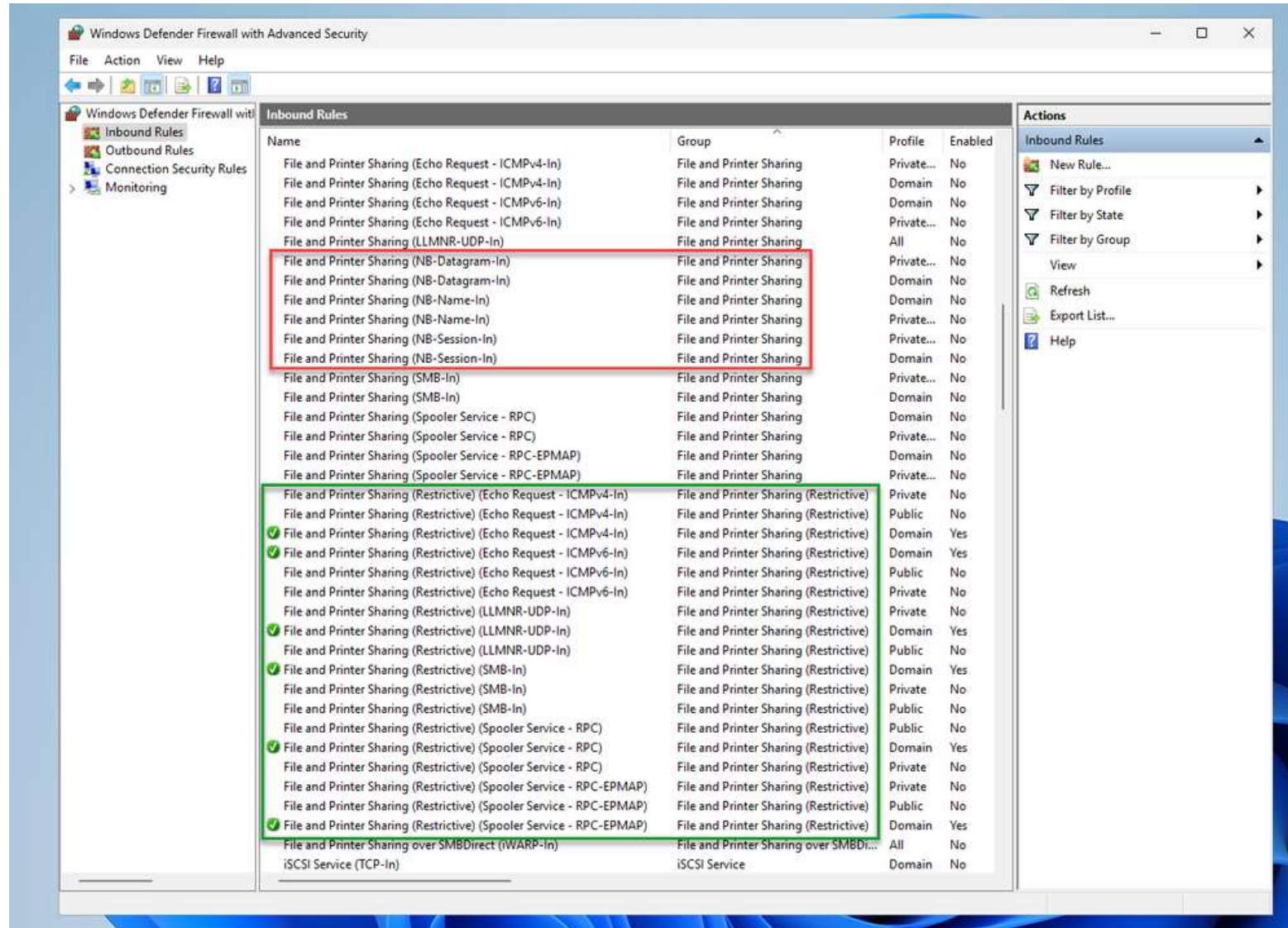
```
Administrator: Windows PowerShell
PS C:\> New-SmbMapping -LocalPath G \
>> -RemotePath \\ad2025-srv.contoso.com\data \
>> -TcpPort 1445 \
>> -QuicPort 2445 \
>> -RdmaPort 3445
```

```
Administrator: Command Prompt
C:\>NET USE \\ad2025-srv.contoso.com\data /TCP:1445 /QUIC:2445 /RDMA:3445
```

SMB Alternative Ports



File and Printer Sharing (Restrictive) FW Rules



Legacy SAM RPC Password Change Behavior

Remotely blocked RPC calls (DES-ECB-LM):

- SamrChangePasswordUser
- SamrOemChangePasswordUser2
- SamrUnicodeChangePasswordUser2

Members of the Protected Users group:

- SamrUnicodeChangePasswordUser4

Legacy SAM RPC Password Change Behavior

Configure SAM change password RPC methods policy

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled Supported on:

Options:

Options for Sam password change RPC method policy:

- Allow strong encryption change password RPC method
- Block all change password RPC methods
- Allow strong encryption change password RPC method only
- Allow all change password RPC methods

Help:

This policy enables an administrator to configure the remote usage of change user password RPC methods in security account manager(SAM).

When the policy is enabled, following options are supported:

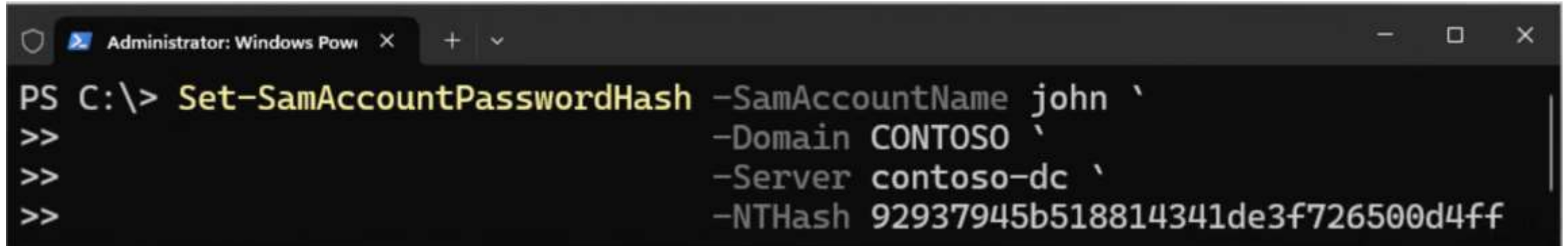
Block all change password RPC methods: block remote usage of all the security account manager(SAM) change password RPC methods.

Allow strong encryption change password RPC method: allow remote use of the change password RPC method which uses strong encryption and blocks remote use of weak encryption methods.

Allow all change password RPC methods: allows remote usage of all the change password RPC methods irrespective of the encryption.

Default policy: 1. Domain member computers - block all change password RPC methods.

Legacy SAM RPC Password Change Behavior

A screenshot of a Windows PowerShell terminal window. The title bar shows 'Administrator: Windows PowerShell' with a shield icon on the left and standard window controls on the right. The command prompt shows the command 'Set-SamAccountPasswordHash' being entered in yellow text, followed by four parameters: '-SamAccountName john', '-Domain CONTOSO', '-Server contoso-dc', and '-NTHash 92937945b518814341de3f726500d4ff'. The prompt is at 'PS C:\>'.

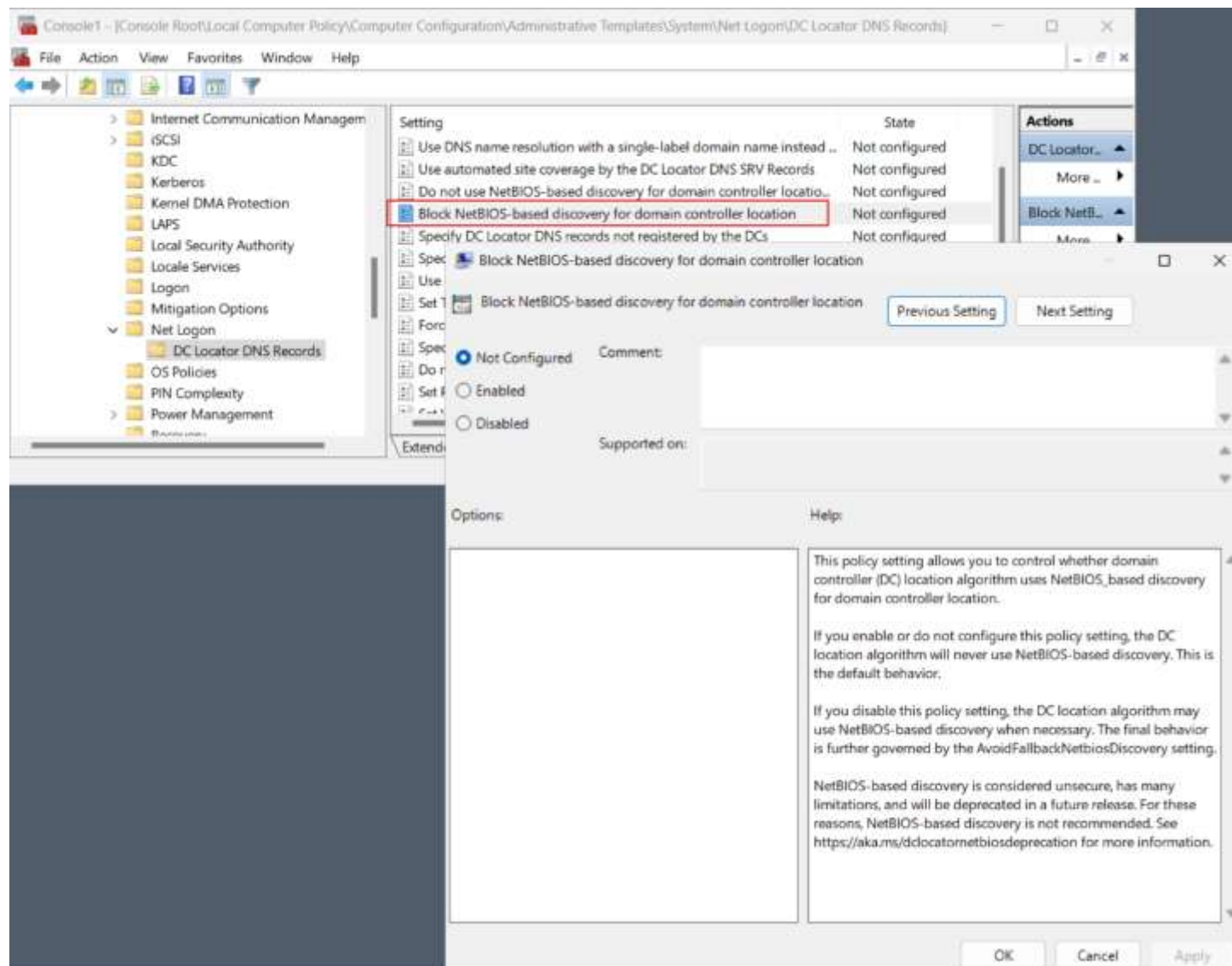
```
PS C:\> Set-SamAccountPasswordHash -SamAccountName john `
>>                                     -Domain CONTOSO `
>>                                     -Server contoso-dc `
>>                                     -NTHash 92937945b518814341de3f726500d4ff
```

SamrSetInformationUser(SAMPR_USER_INTERNAL1_INFORMATION)

DC Locator NetBIOS Deprecation



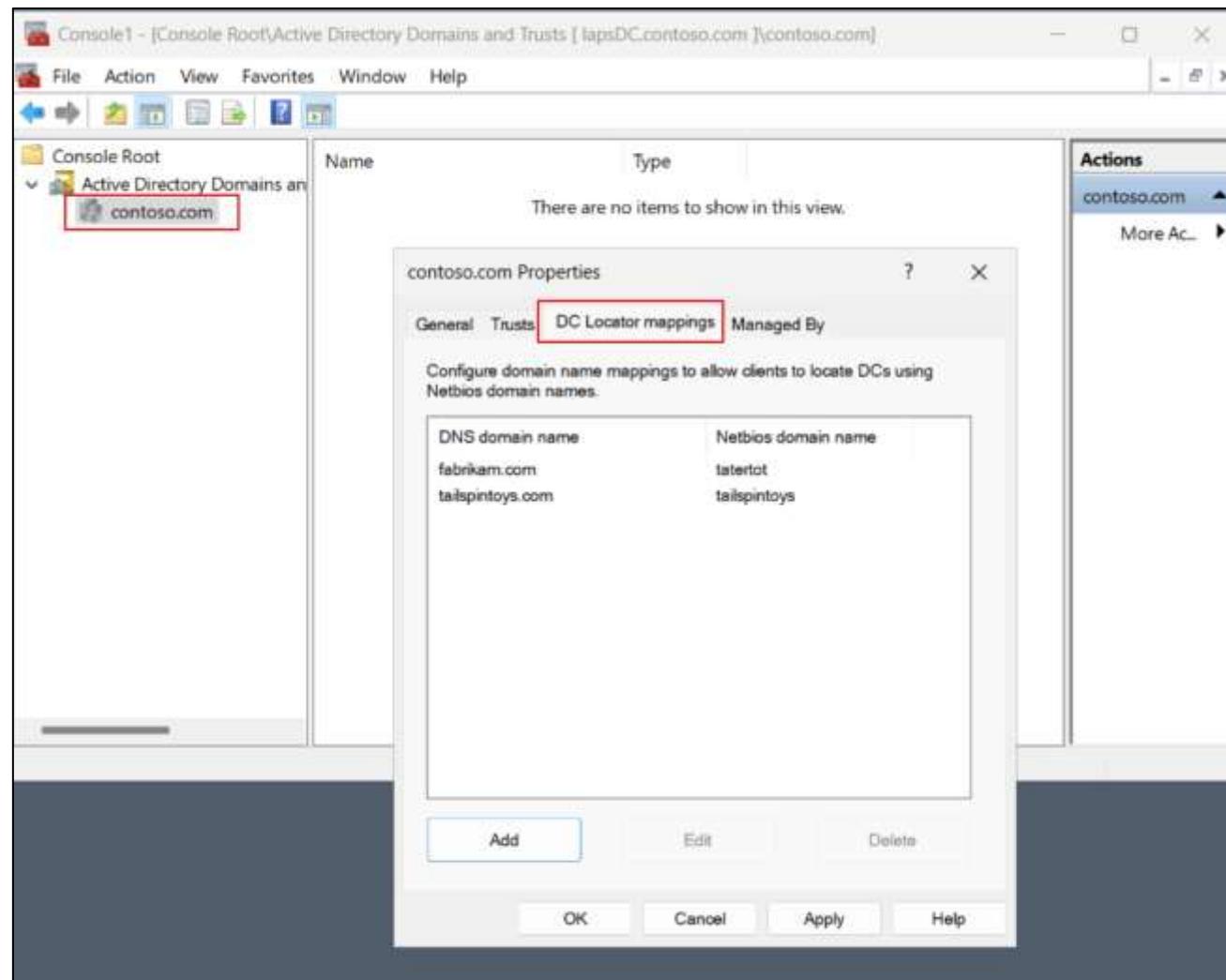
DC Locator NetBIOS Deprecation



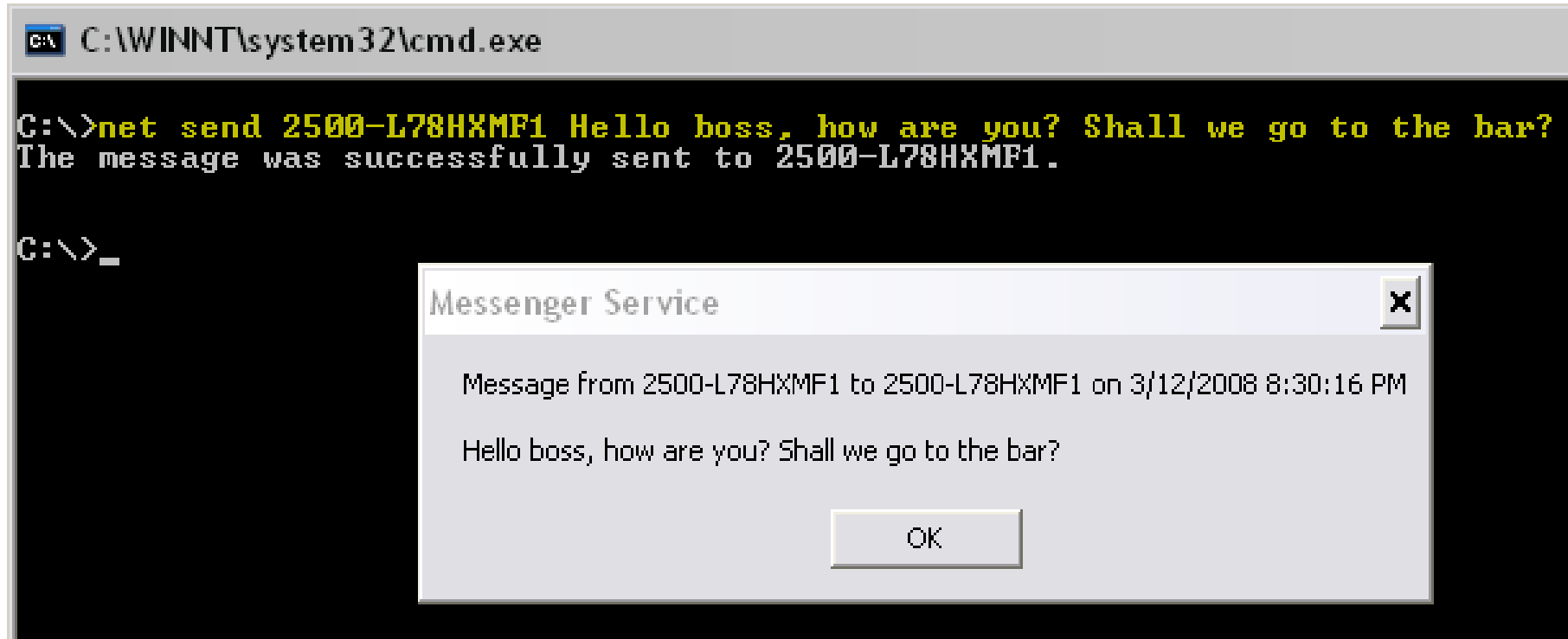
DC Locator NetBIOS Deprecation



DC Locator NetBIOS Deprecation



Deprecation of WINS and Remote Mailslots



Set-SmbClientConfiguration -EnableMailslots \$true

Replication Priority Order

AD now allows administrators to increase the system calculated replication priority with a particular replication partner for a particular naming context. This feature allows more flexibility in configuring the replication order to address specific scenarios.

DC Locator Performance Counters

Add Counters

Available counters

Select counters from computer:

<Local computer> Browse...

DC Locator (Client) ▼
DC Locator (DC) ▲

Pings: Active Mailslot Pings
Pings: Active UDP LDAP Pings
Pings: Average Mailslot Ping Latency (secs)
Pings: Average UDP LDAP Ping Latency (secs)
Pings: Mailslot Pings Received/sec
Pings: UDP LDAP Pings Received/sec

Instances of selected object:

Total
<All instances>
0
1
2
3
4
5

Search

Add >>

Added counters

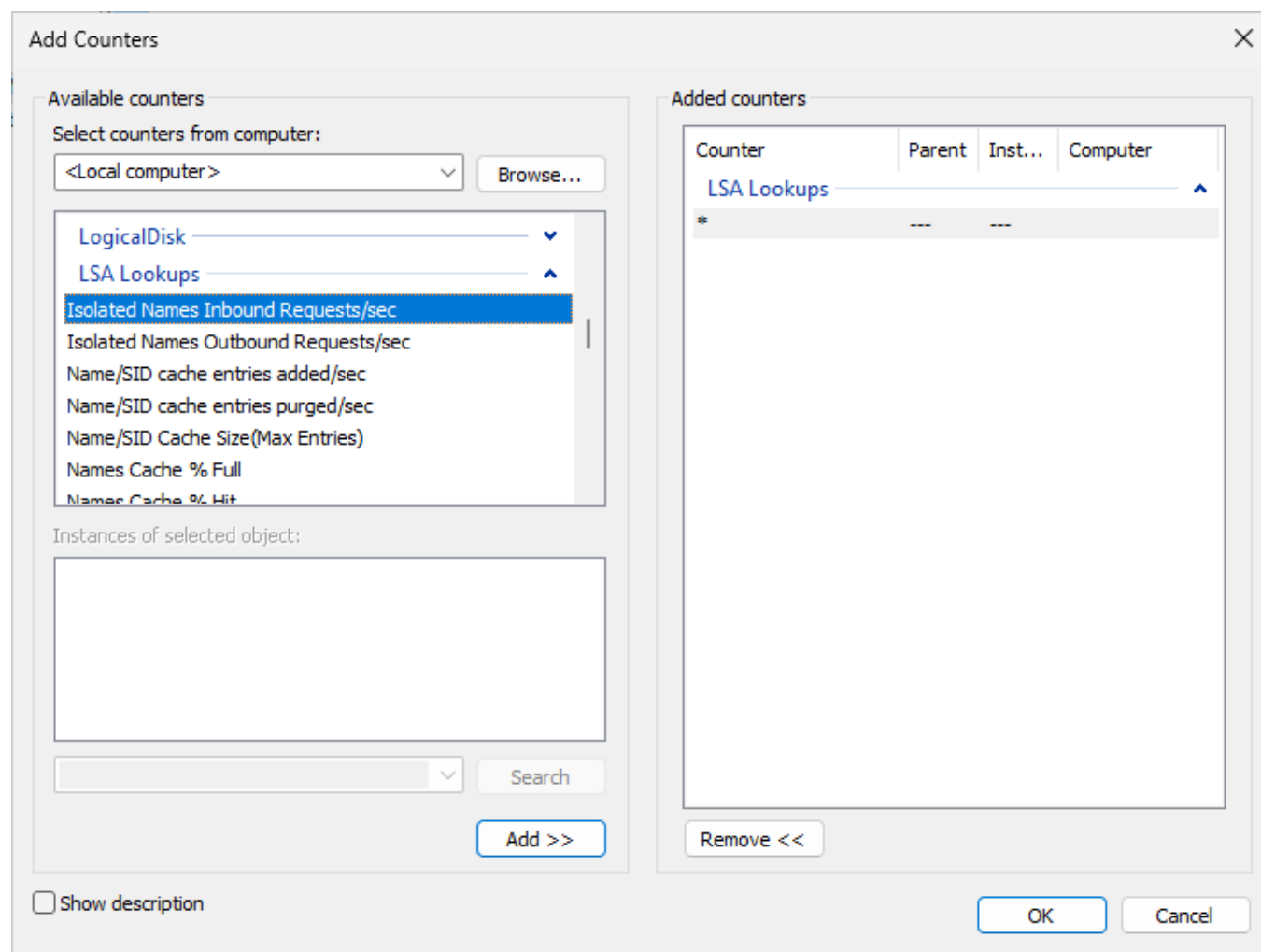
Counter	Parent	Inst...	Computer
---------	--------	---------	----------

Remove <<

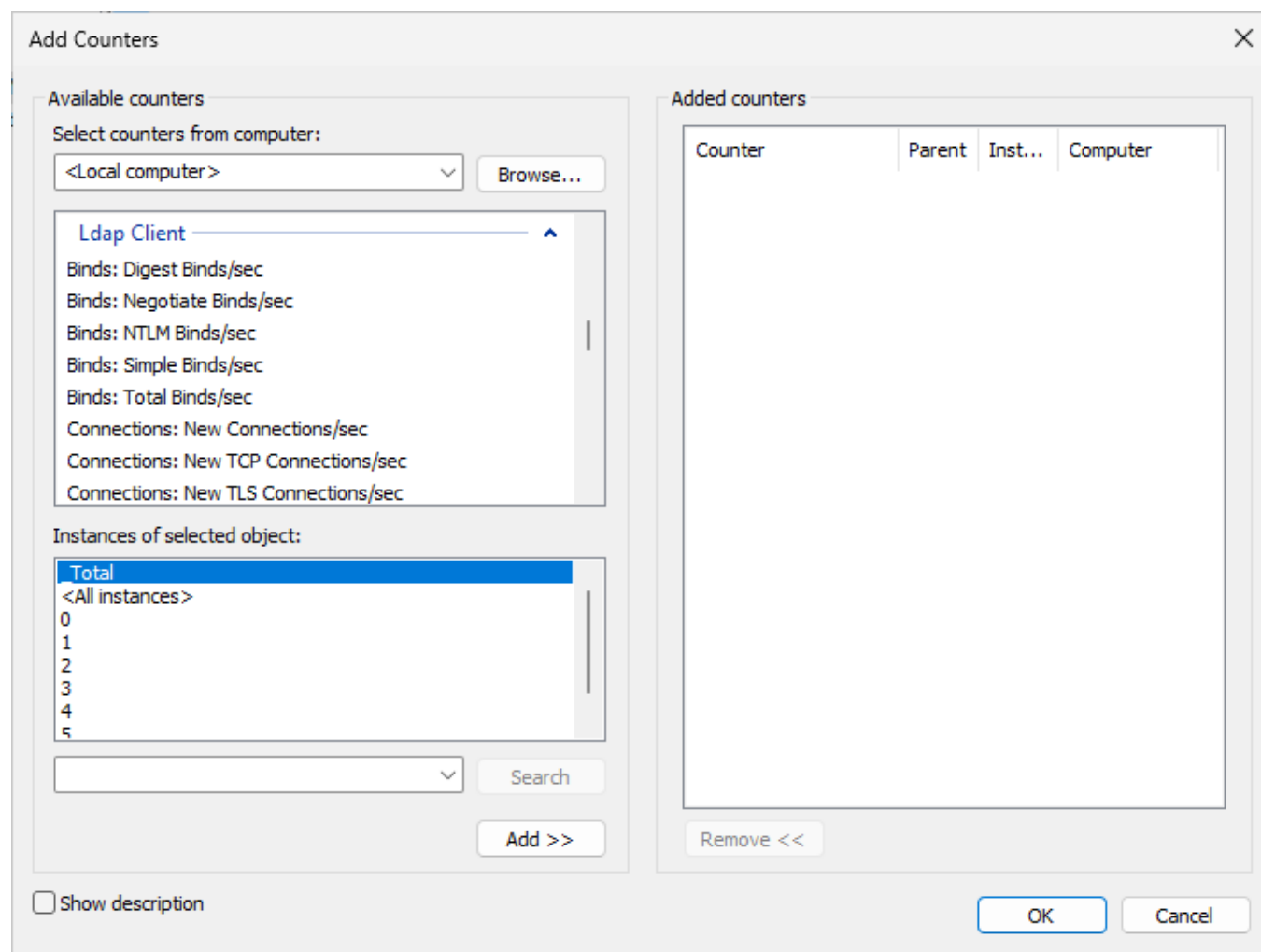
☐ Show description

OK Cancel

LSA Lookups Performance Counters



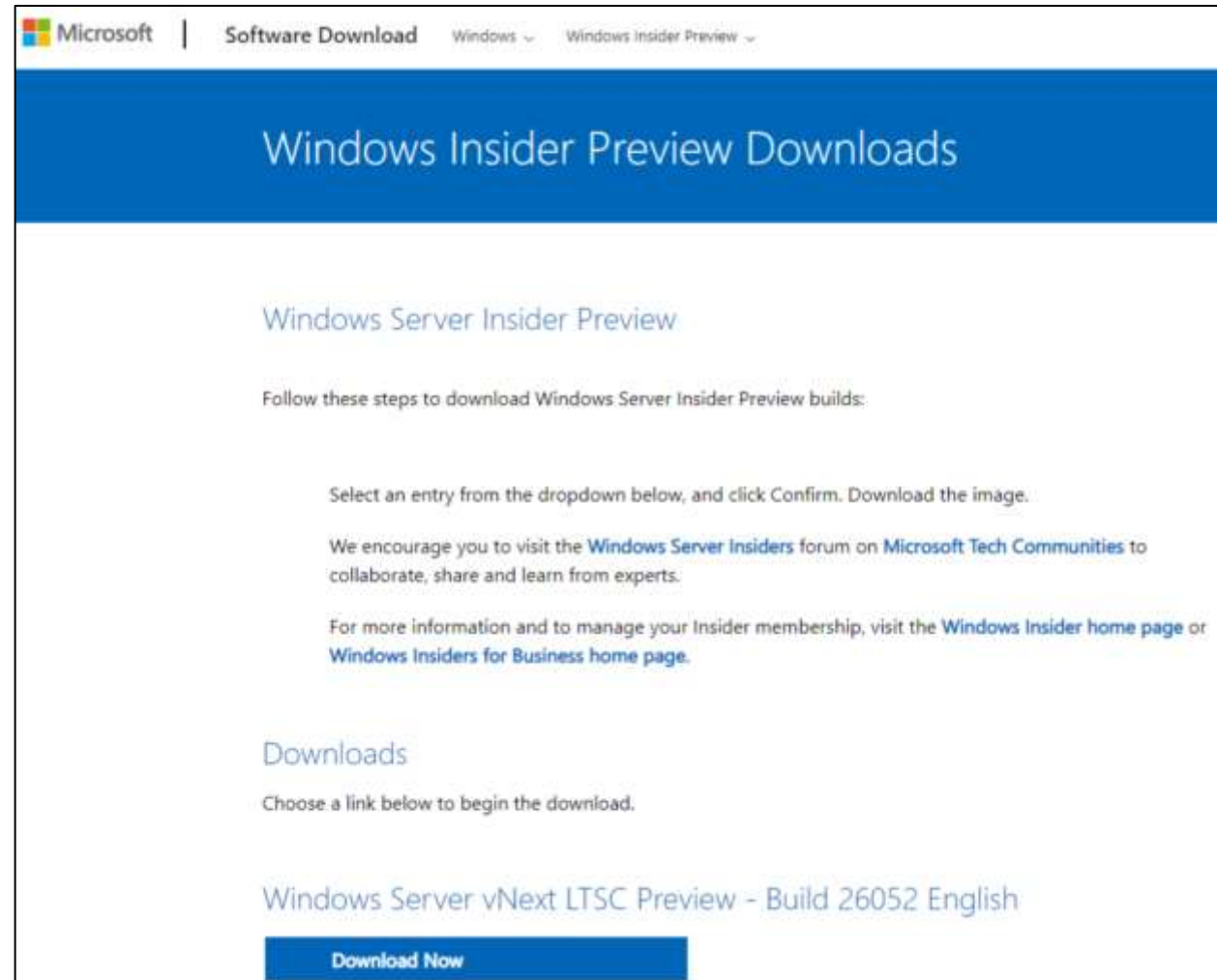
LDAP Client Performance Counters (WS2022+)



Summary: New AD and Security Features

- Delegated managed service accounts (dMSAs)
- LDAP, SMB, and Kerberos security improvements
- Slow deprecation of NetBIOS, NTLM, and SAM RPC
- Increased scalability
- Supportability improvements

Grab the ISO



Give Feedback

The screenshot shows the Windows Feedback Hub application window. On the left is a sidebar with navigation options: Home, Feedback (selected), Announcements, Quests, and Achievements. At the bottom of the sidebar is the user profile for Michael Grafnetter and a Settings icon. The main content area is titled 'All feedback' and 'My feedback' (underlined). Below the title is a search bar with the placeholder text 'Give us feedback to make Windows better' and a '+ Give new feedback' button. Filter options are displayed: Sort: Activity, Filter: Submitted by me, Upvoted by me, and Device: Server. Below these are Category: Windows Server and Subcategory: Management. The main feedback item is titled 'Problem' with a red icon, followed by the heading 'dMSA migration incompatible with ADFS'. The description reads: 'I tried the migration from a standard user account to a delegated managed service account (dMSA) with the Active Directory Federation Services (ADFS) component on WS2025 Insider Preview build 26063.1. After the migration, the service does not work properly, with many...'. It is marked as 'Submitted by me' and shows the category path 'Category Windows Server > Management'. The last activity is 'Submitted about an hour ago'. There are '0 comments' and an 'Add comment' link. At the bottom, it shows '1 upvotes' and a 'Give similar feedback' link with a speech bubble icon.

Feedback Hub

←

☰

Home

Feedback

Announcements

Quests

Achievements

Michael Grafnetter

Settings

All feedback My feedback

Give us feedback to make Windows better

+ Give new feedback

Sort: Activity Filter: Submitted by me, Upvoted by me Device: Server

Category: Windows Server Subcategory: Management

Problem

dMSA migration incompatible with ADFS

I tried the migration from a standard user account to a delegated managed service account (dMSA) with the Active Directory Federation Services (ADFS) component on WS2025 Insider Preview build 26063.1. After the migration, the service does not work properly, with many...

Submitted by me

Category Windows Server > Management

Last activity Submitted about an hour ago

comments 0 Add comment

1 upvotes Give similar feedback

Active Directory Is Not Dead

New AD and Security Features in Windows Server vNext LTSC Preview (2025?)

Mgr. Michael Grafnetter

MVP | MCT | CEI

www.dsinternals.com

 @MGrafnetter