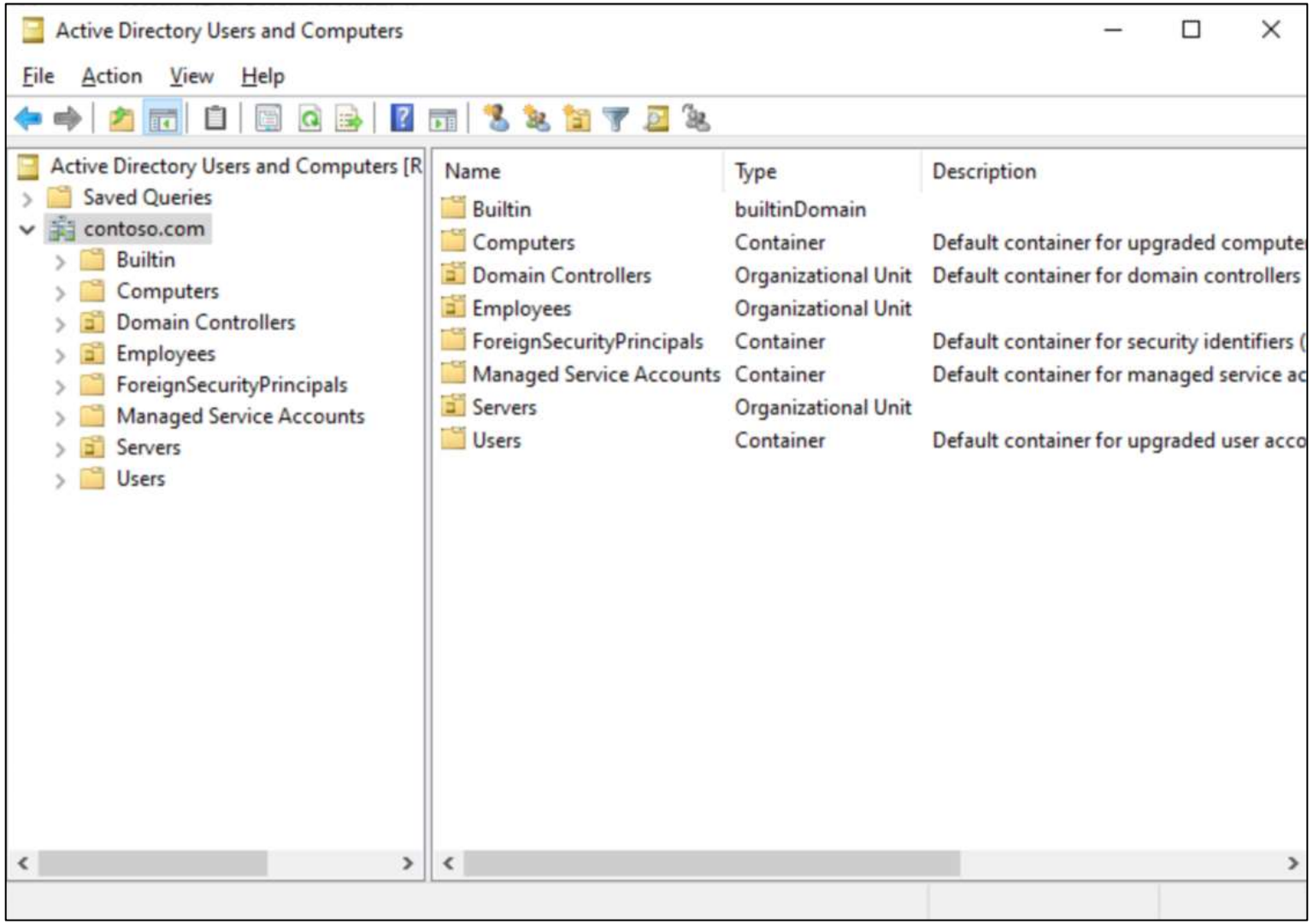
Active Directory Is Not Dead

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

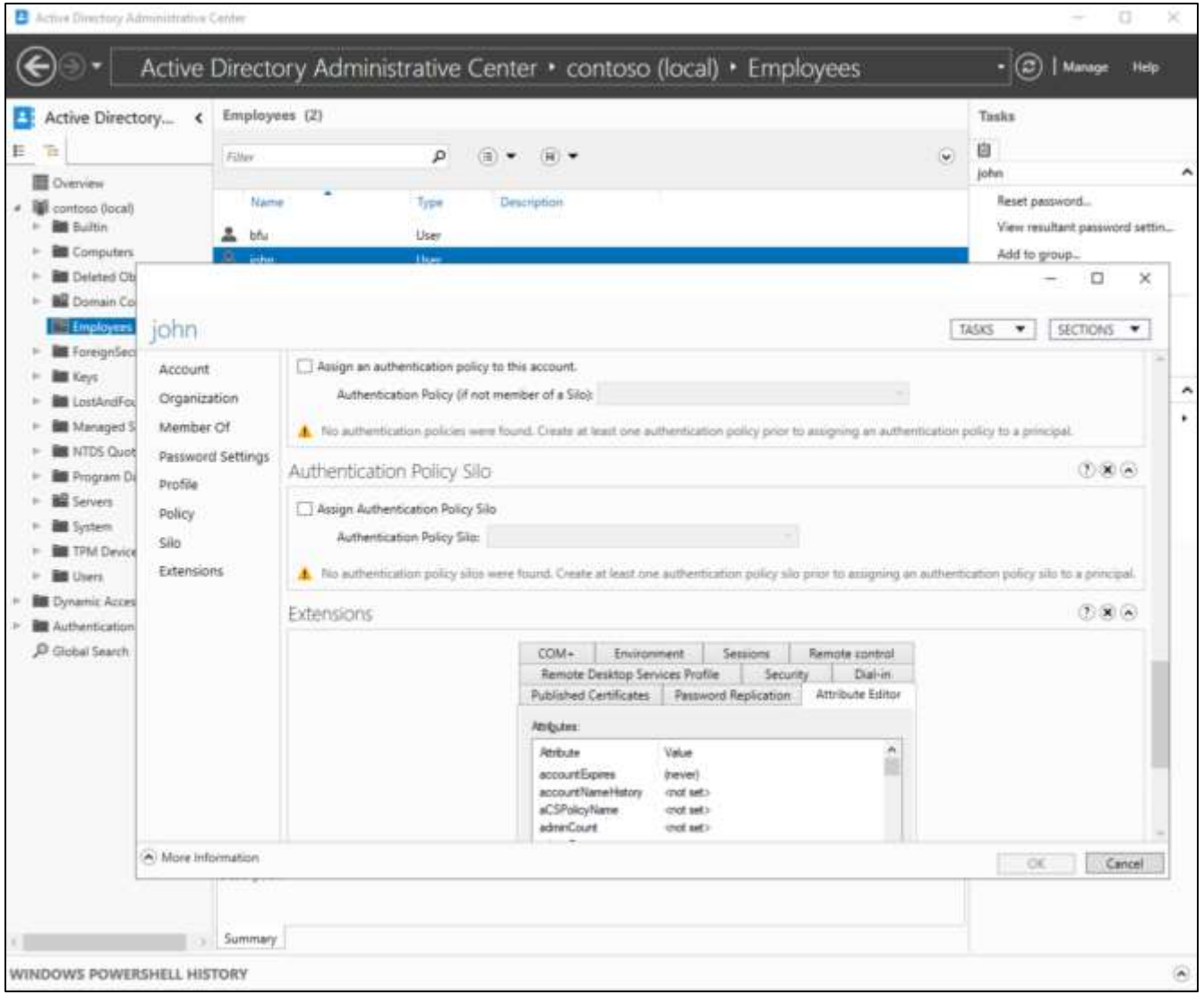
Mgr. Michael Grafnetter
MVP | MCT | CEI
www.dsinternals.com
@MGrafnetter

Is Active Directory Dead?

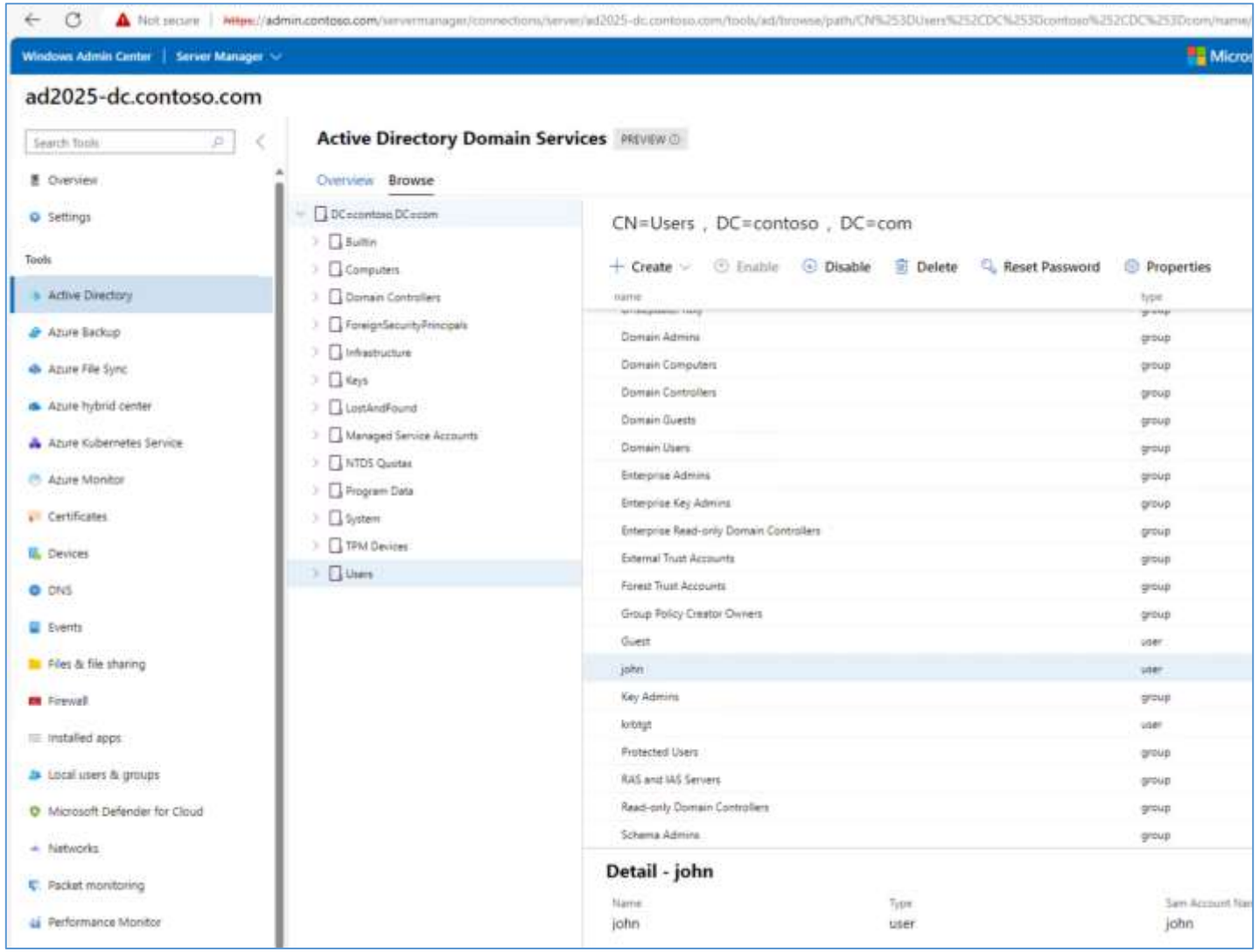
Active Directory Management Tools



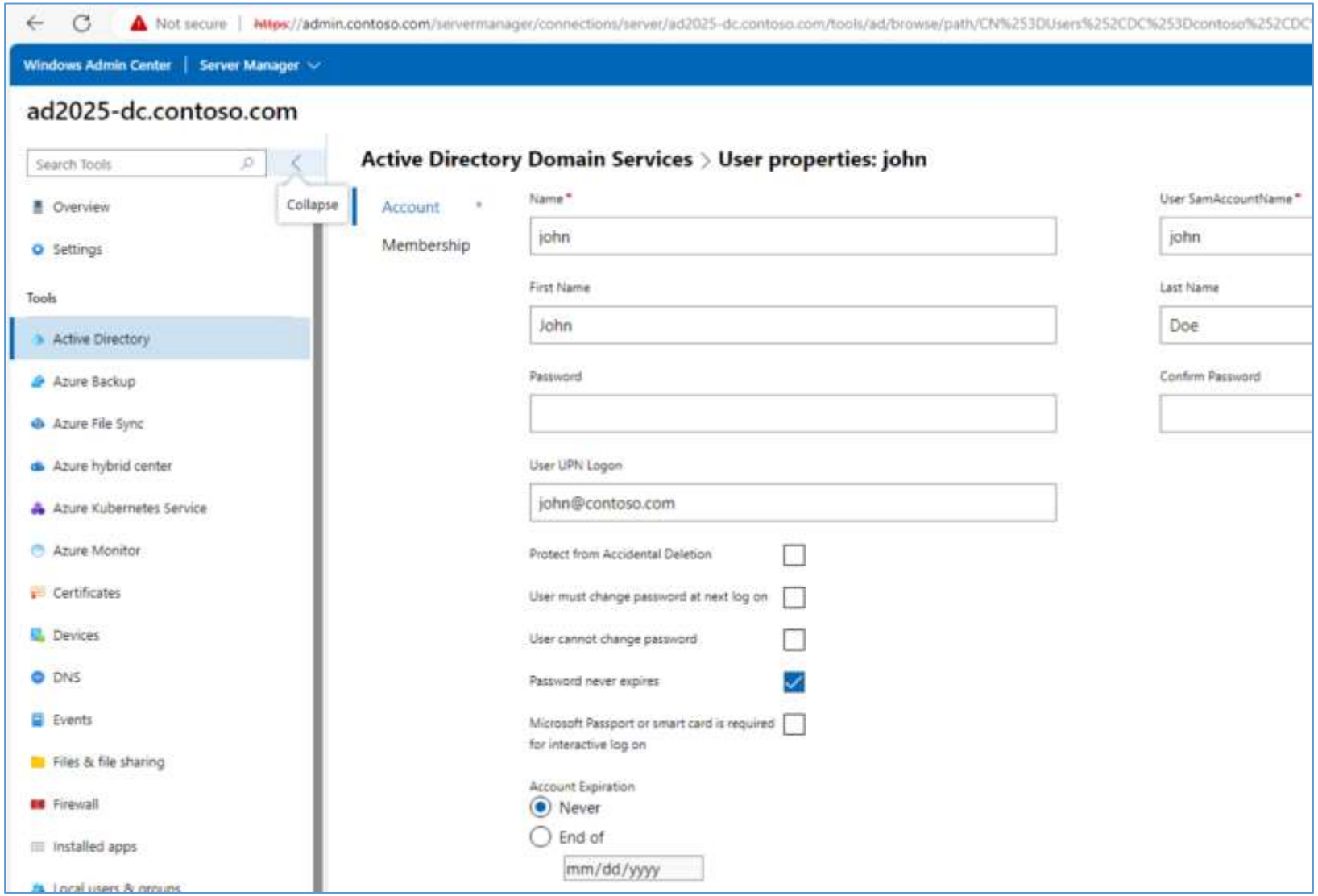
Active Directory Management Tools



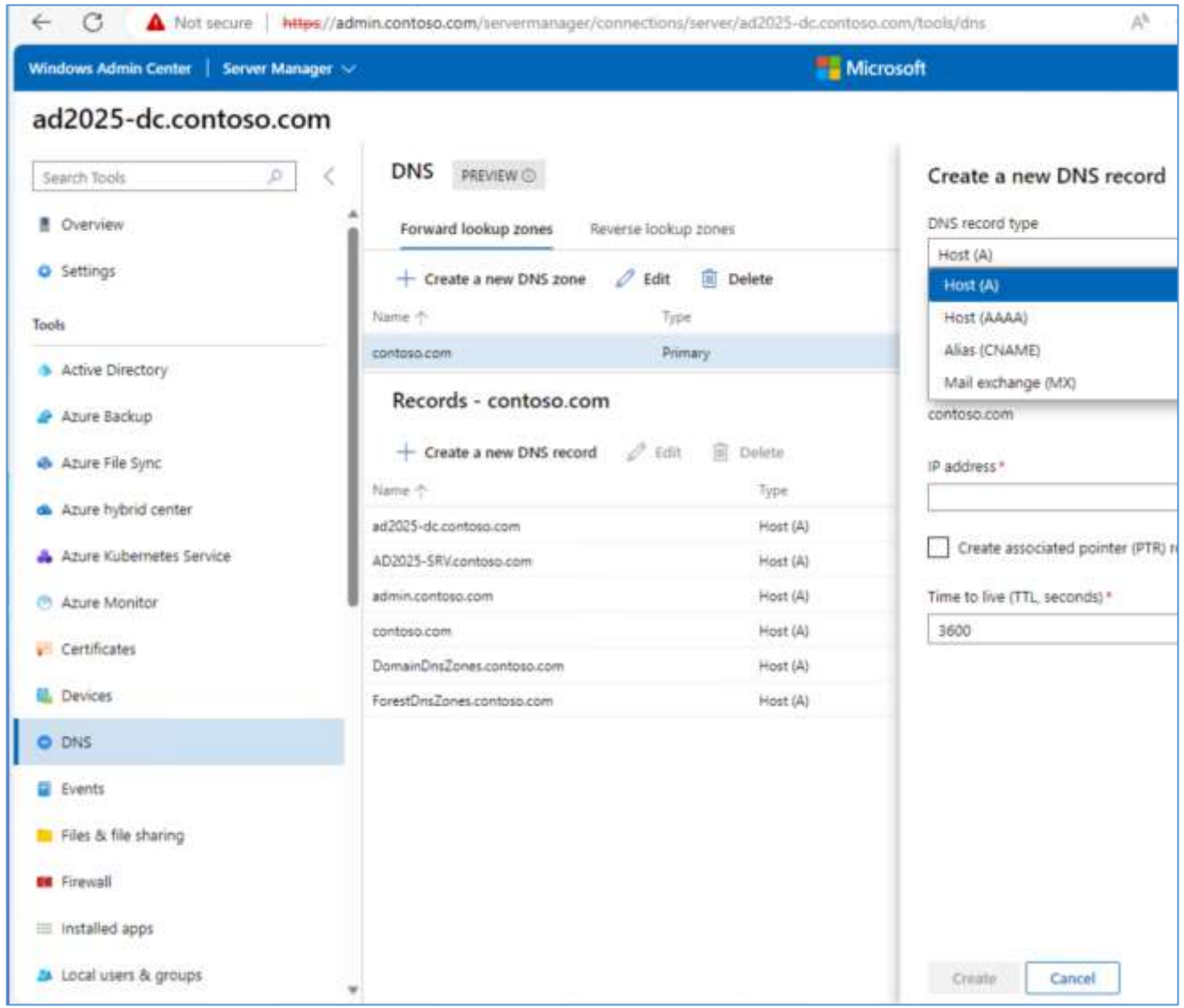
Active Directory Management Tools



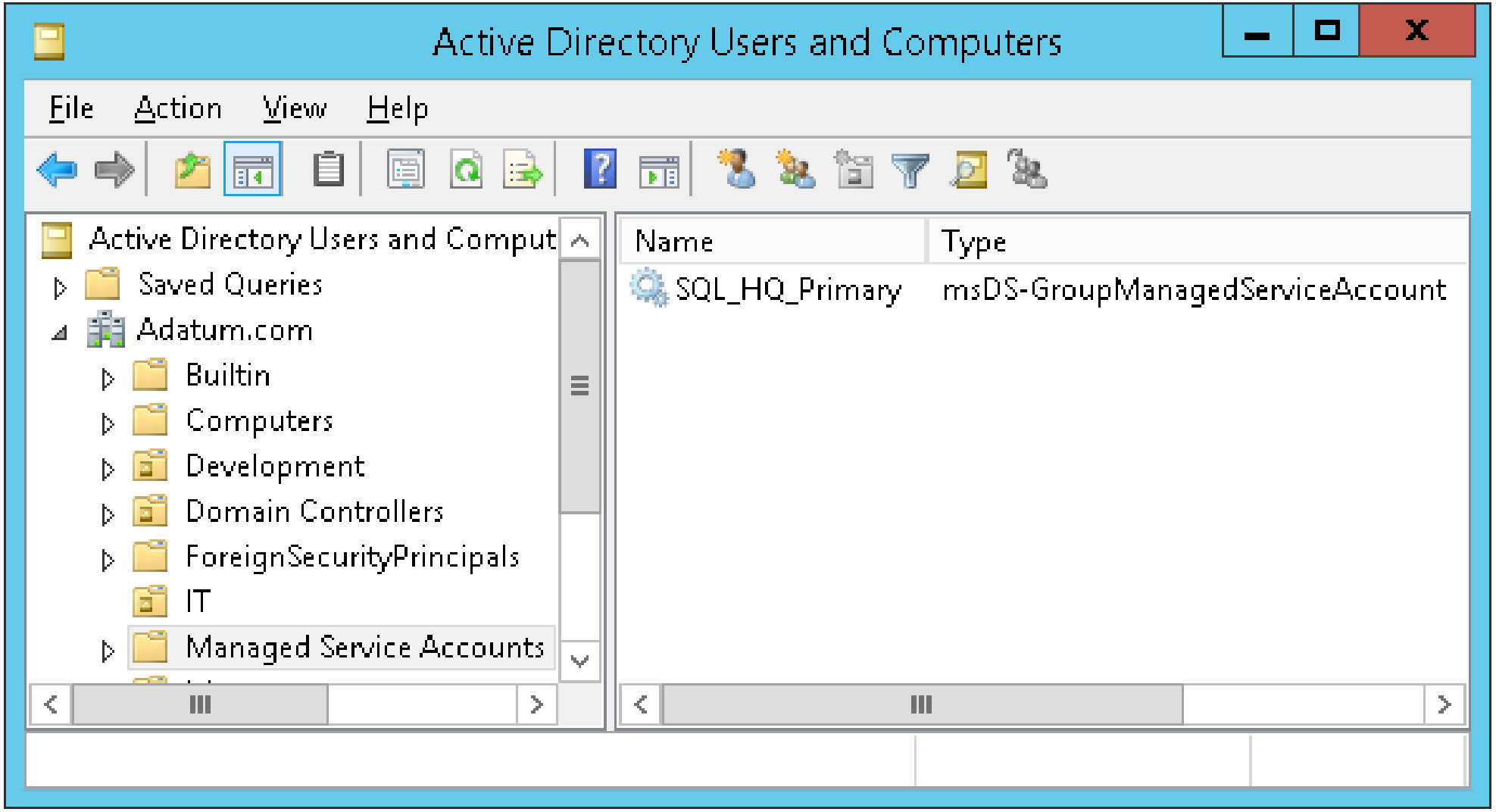
Active Directory Management Tools



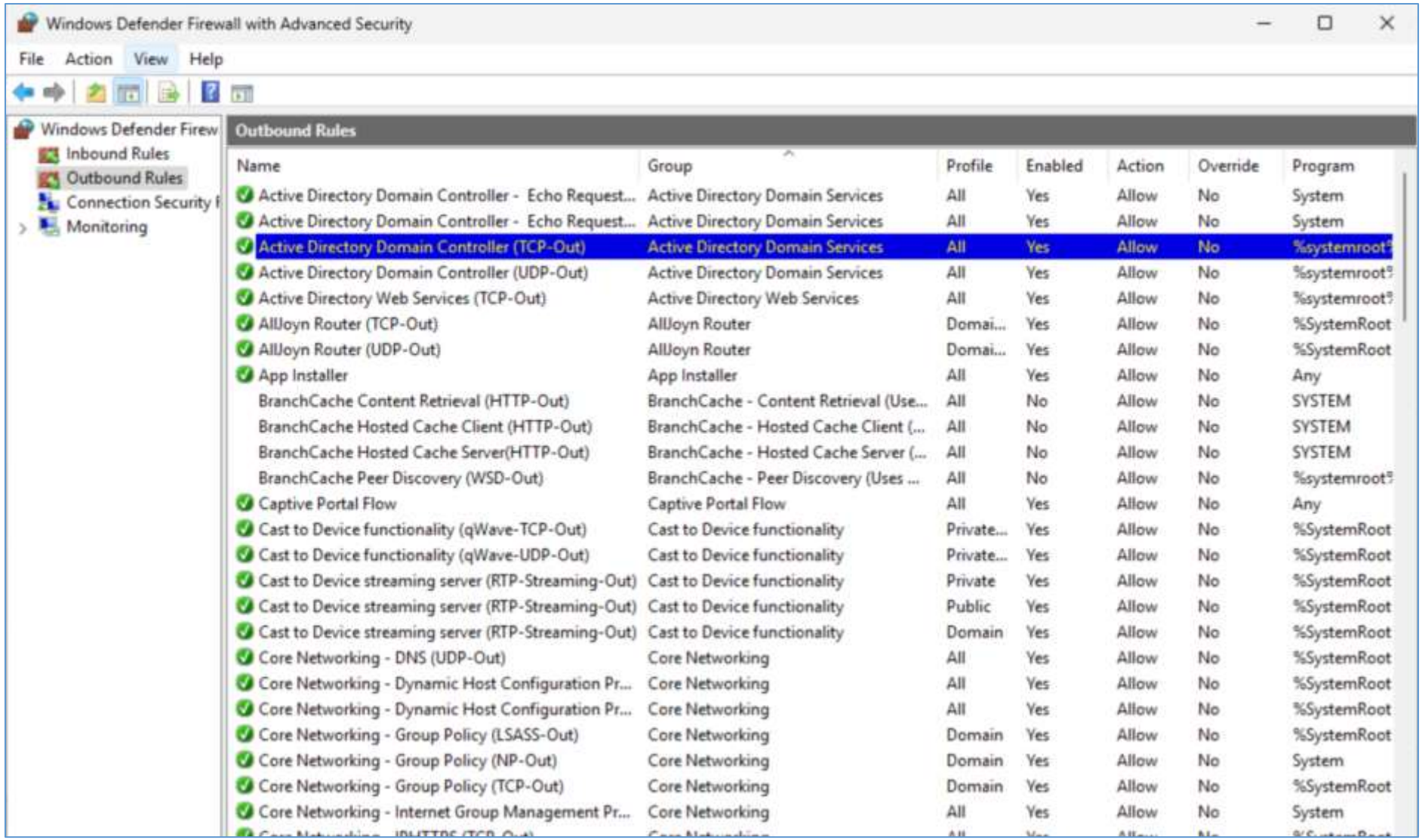
Active Directory Management Tools



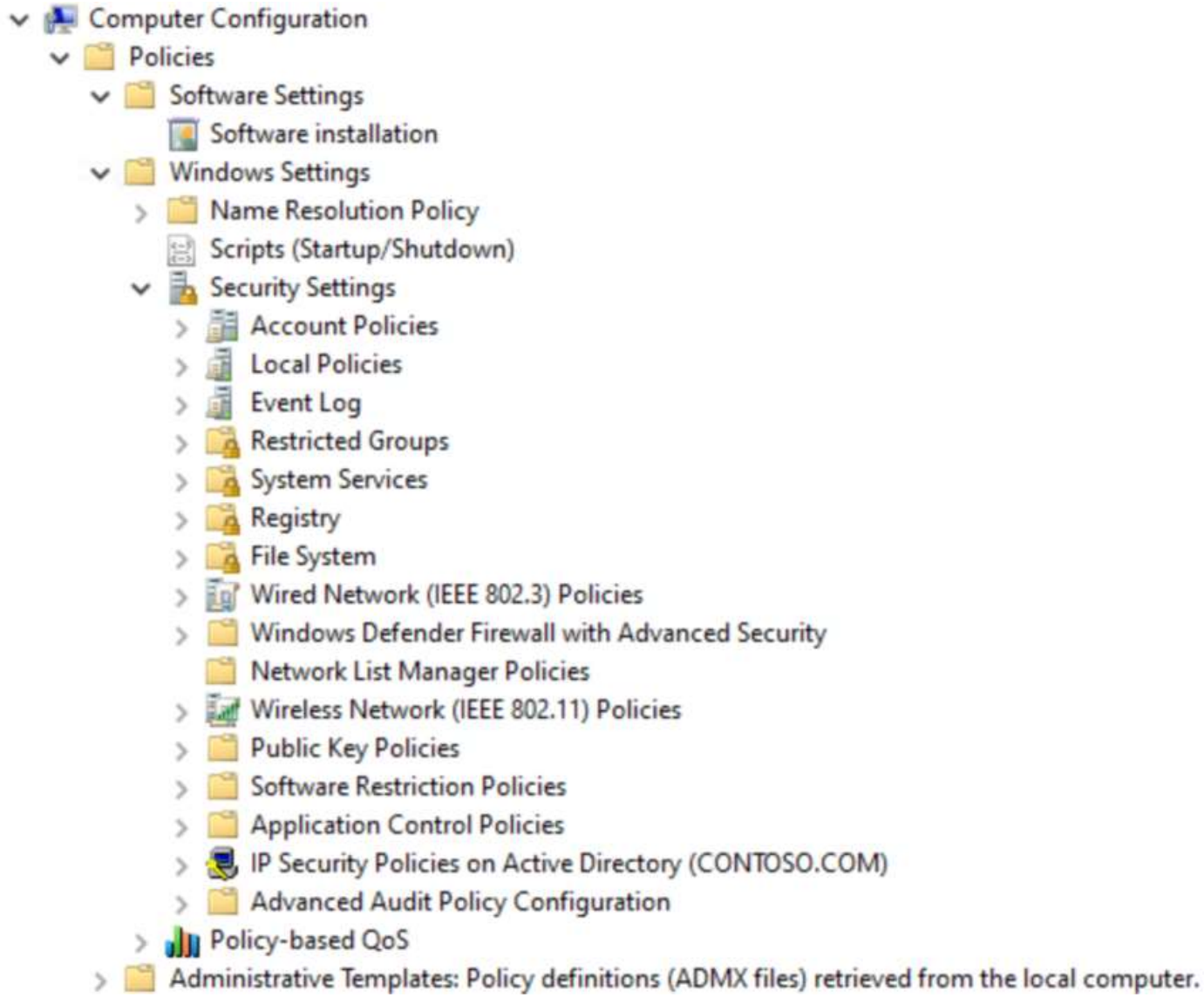
Configuring Managed Service Accounts

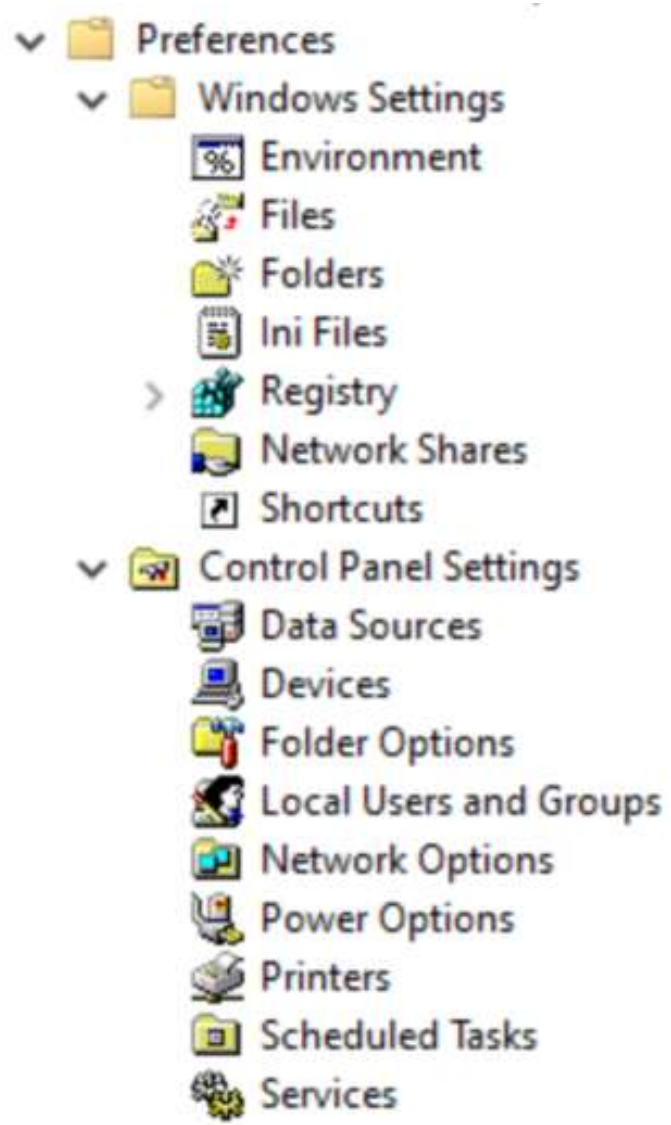


Domain Controller Firewall Outbound Rules

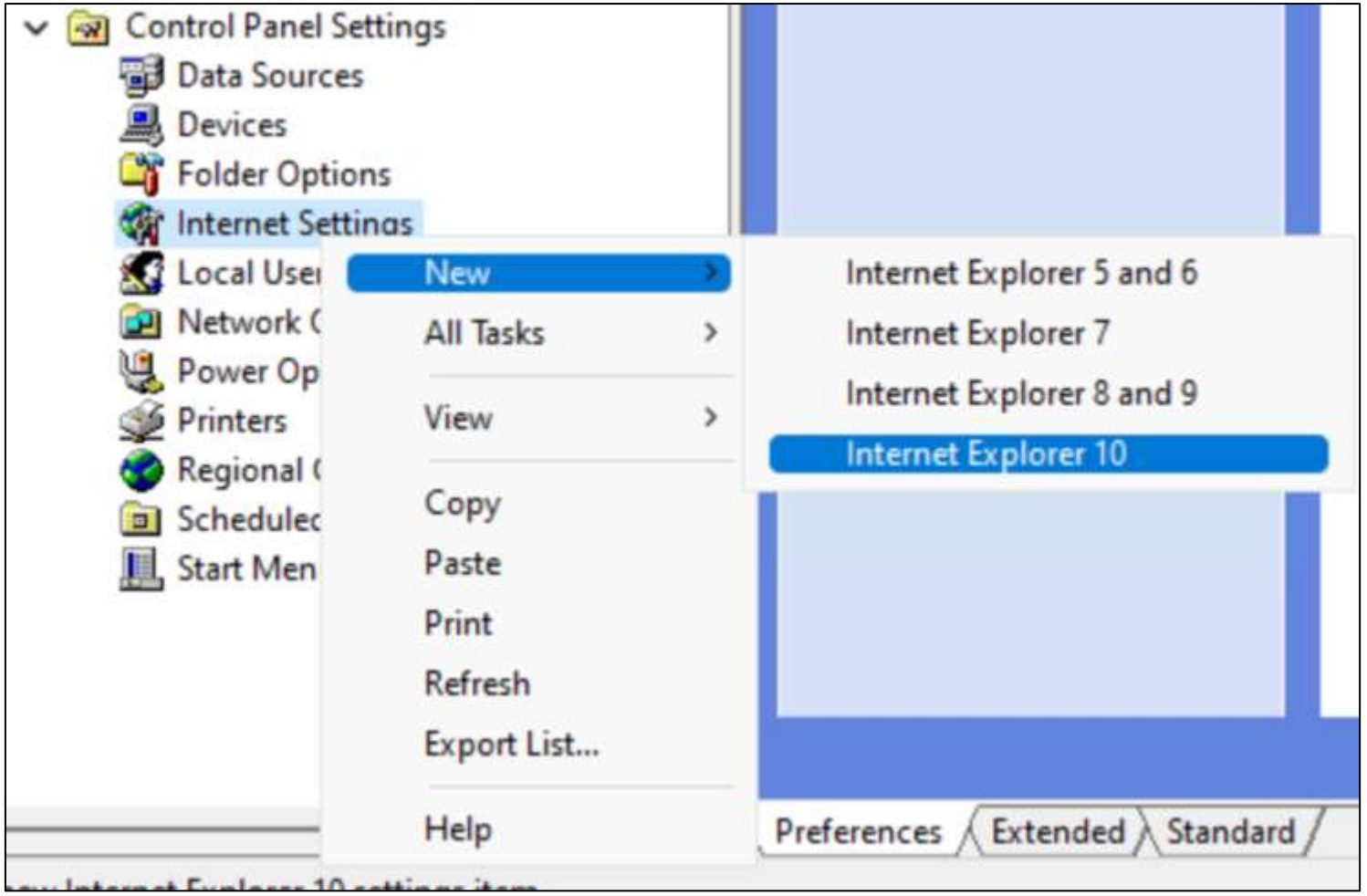


Endpoint Management





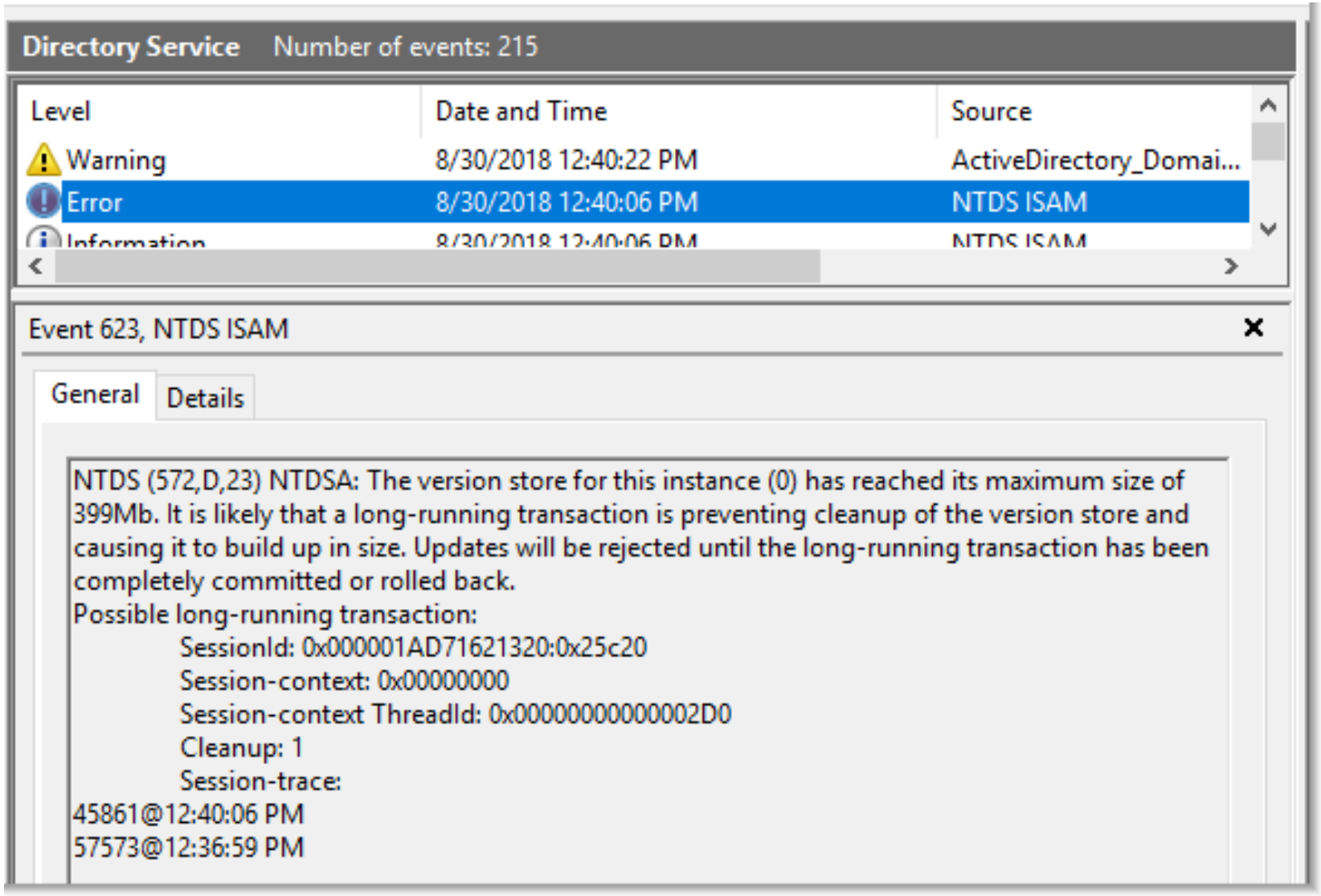
Endpoint Management



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



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

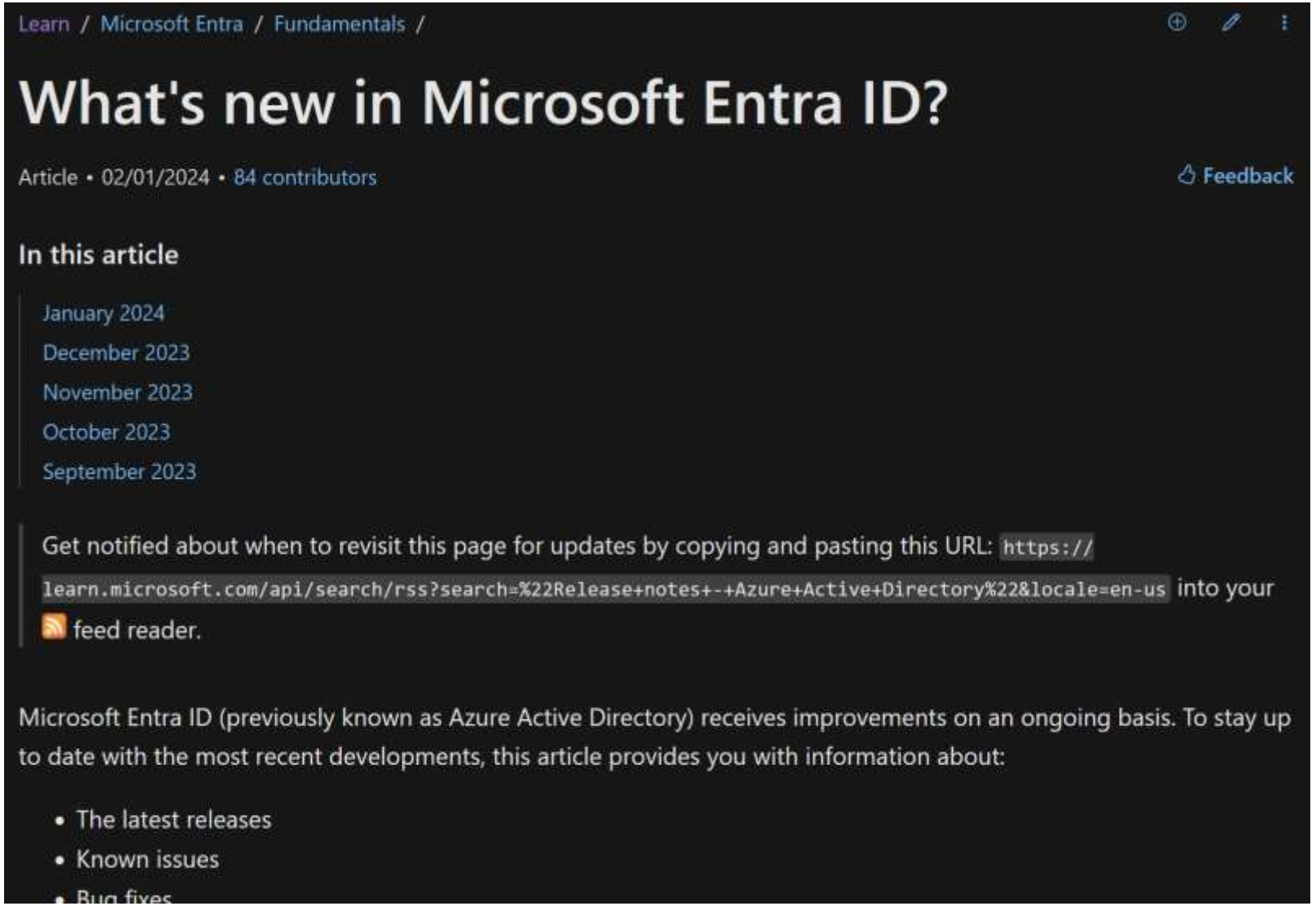
Active Directory Optional Features

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

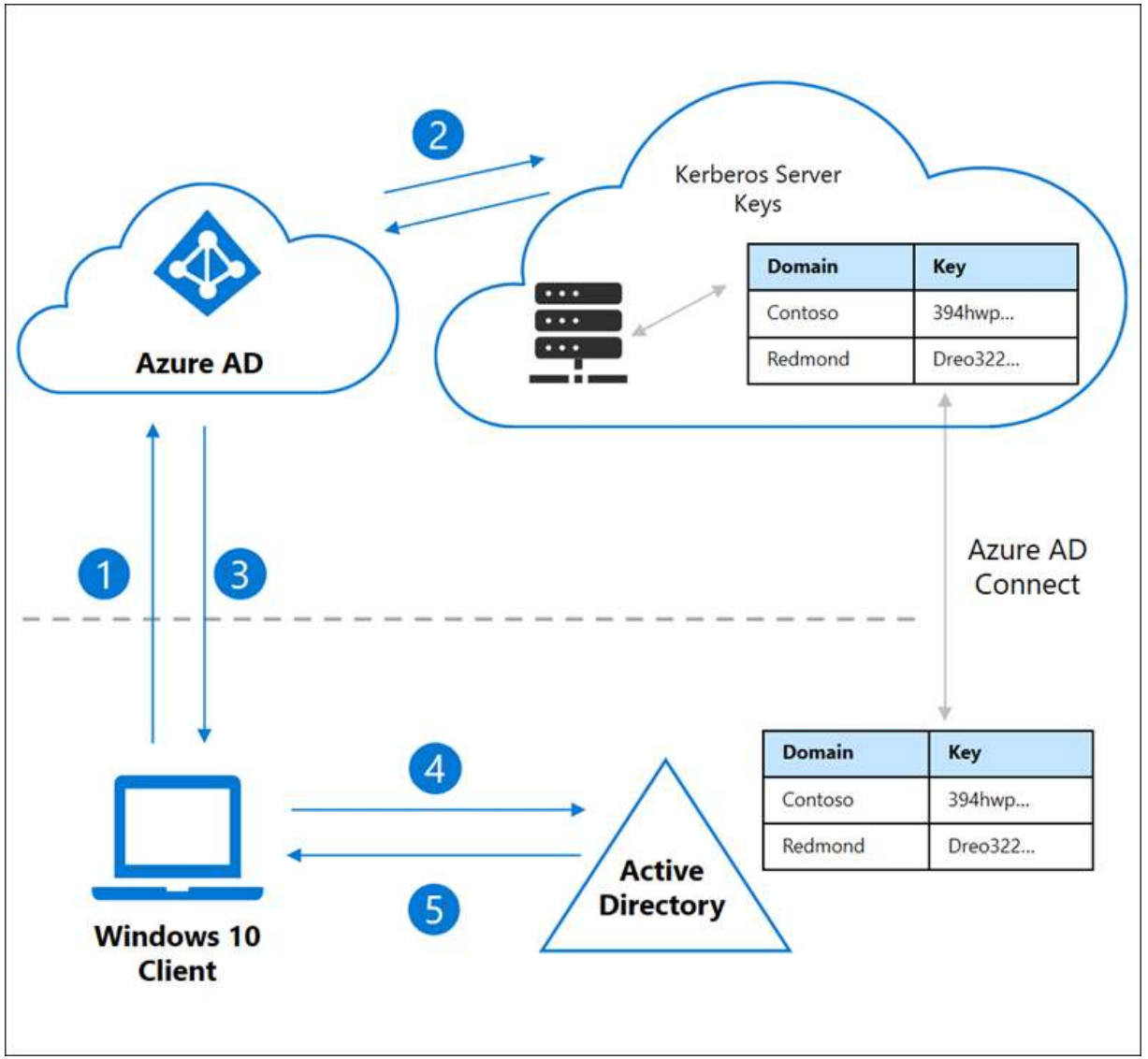
In this article

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.

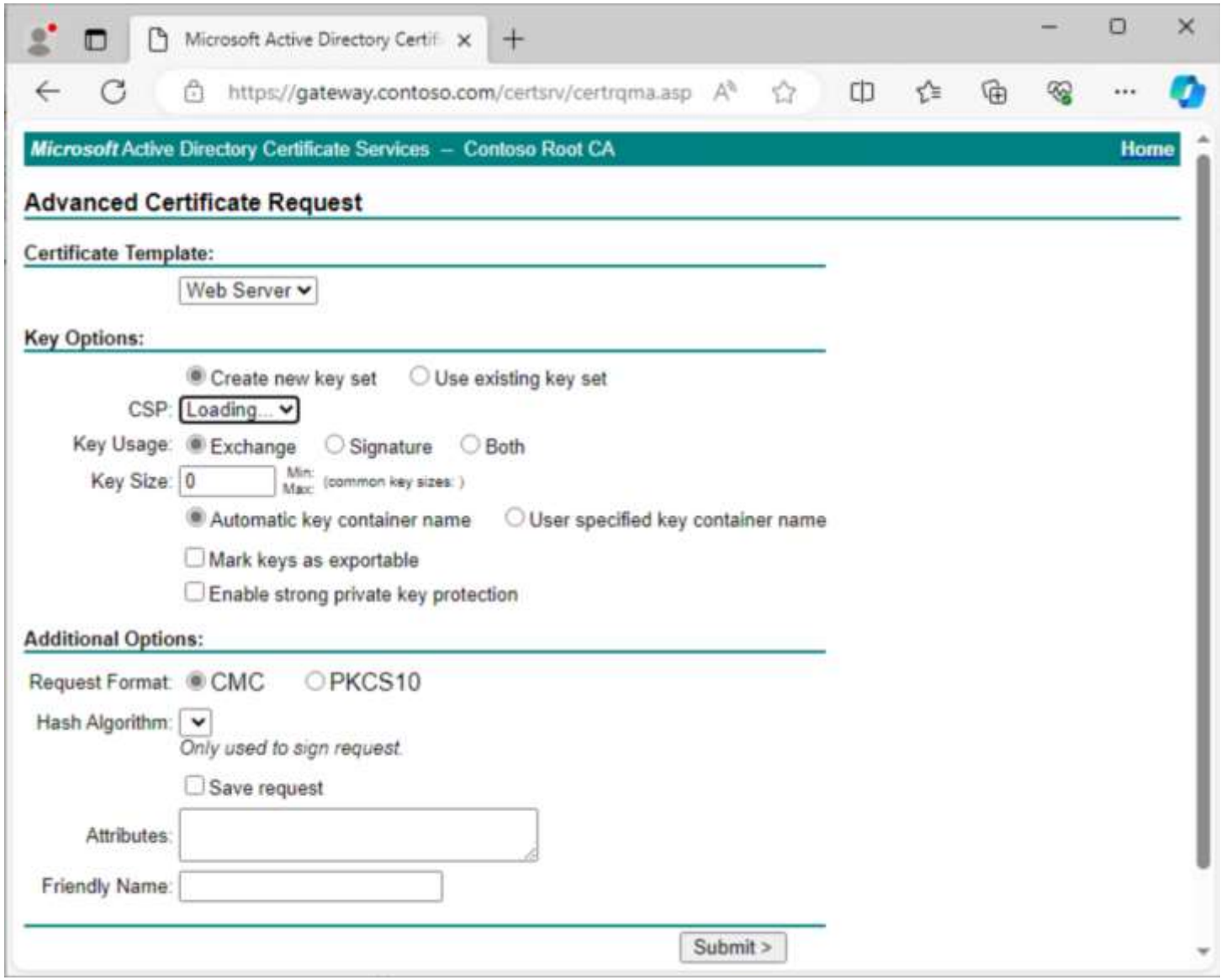
Microsoft Entra ID (previously known as Azure Active Directory) receives improvements on an ongoing basis. To stay up to date with the most recent developments, this article provides you with information about:

- The latest releases
- Known issues
- Bug fixes

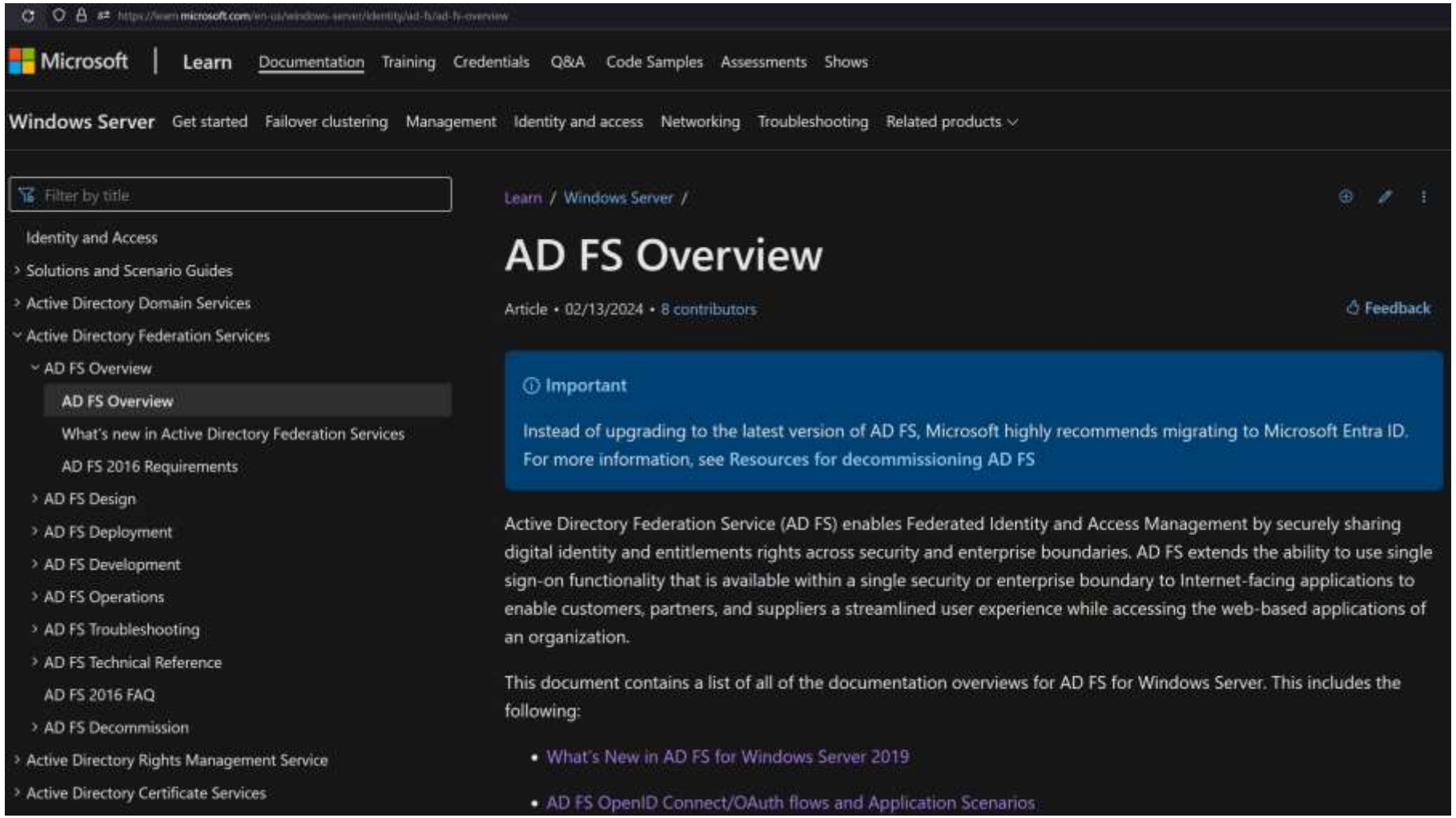
PassKey Support (Cloud Kerberos Trust)



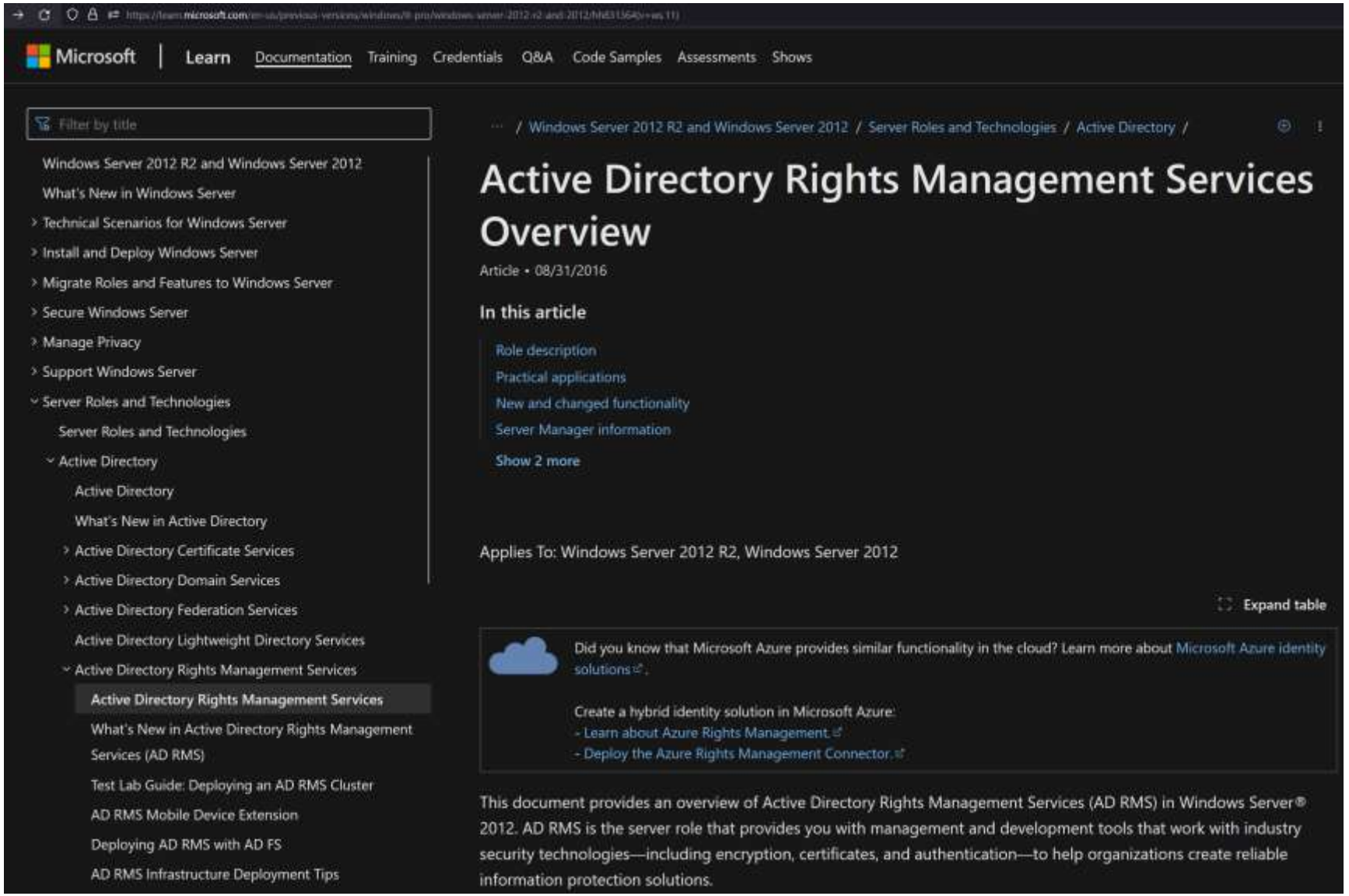
AD Certificate Services Web Enrollment



Active Directory Federation Services

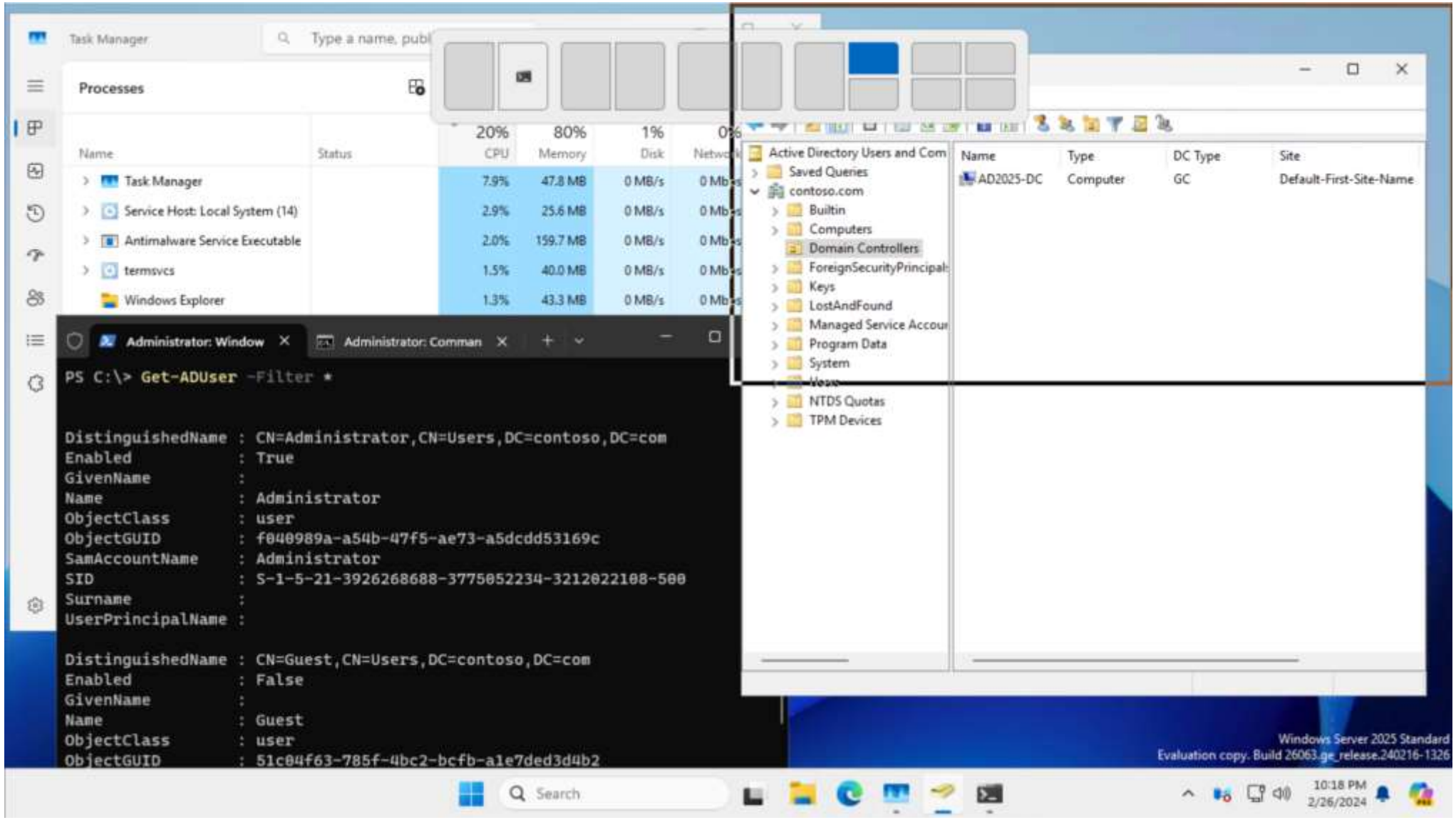


AD Rights Management Services

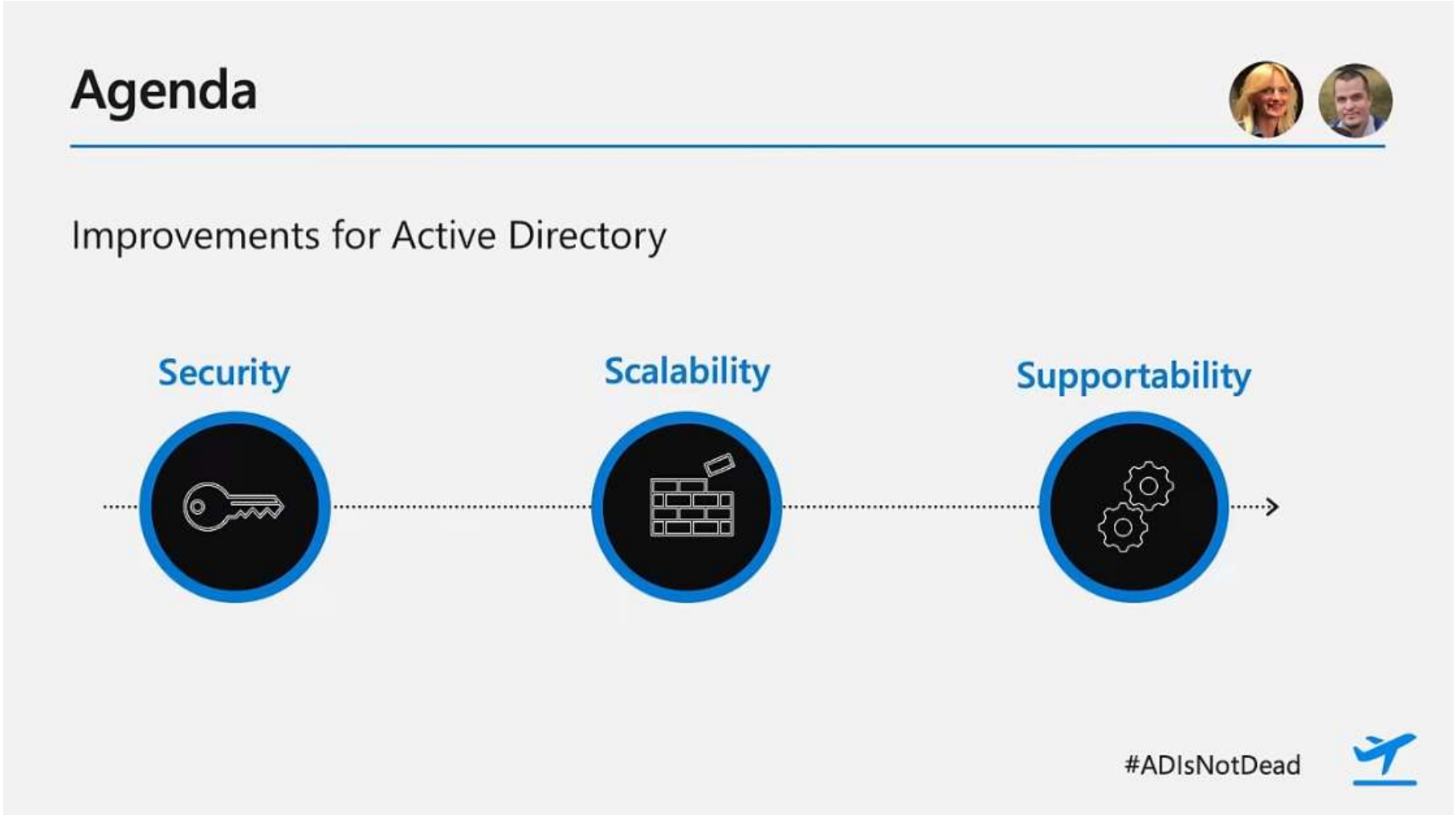


Active Directory Is Not Dead

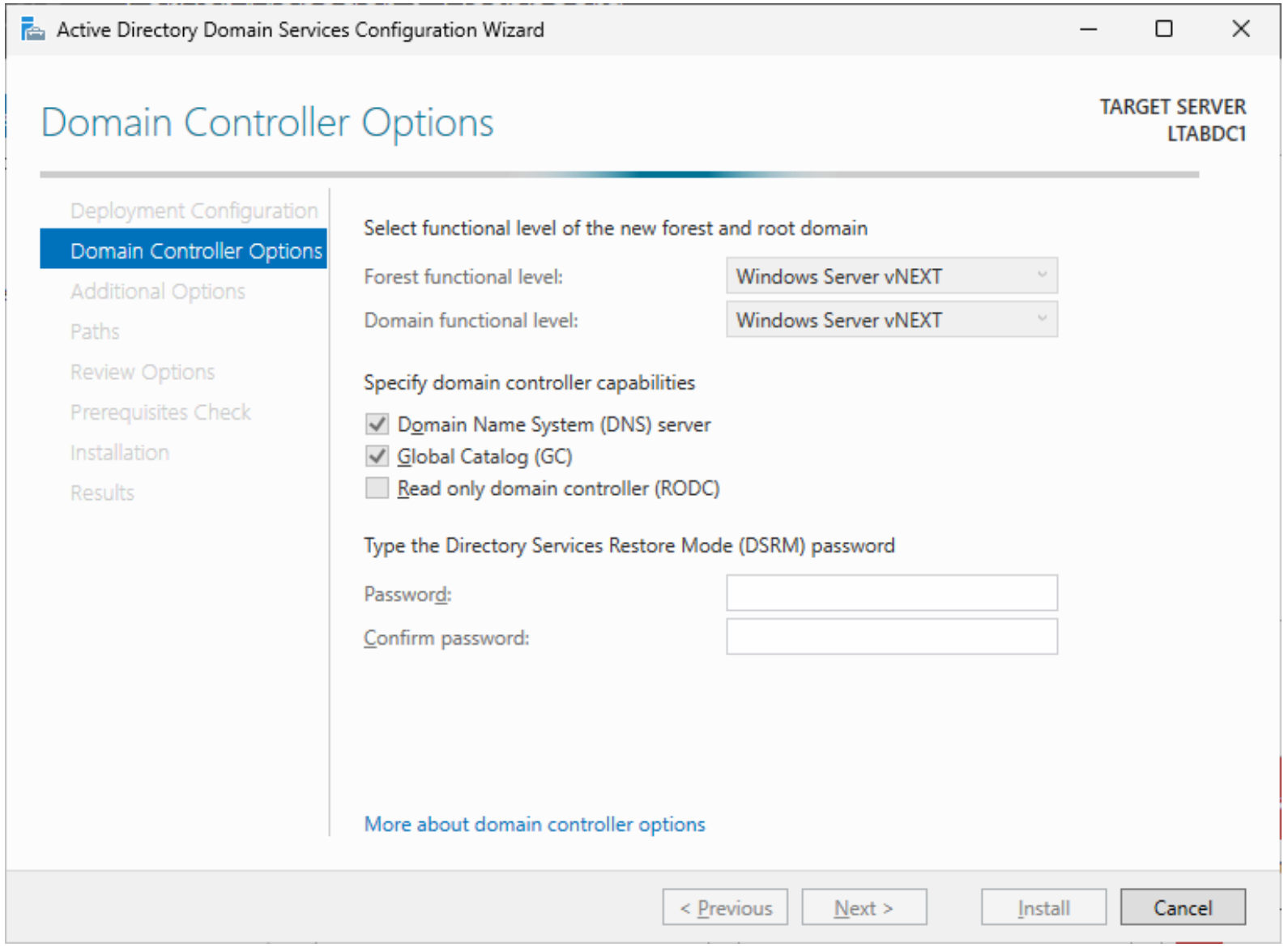
Windows Server Insiders Preview



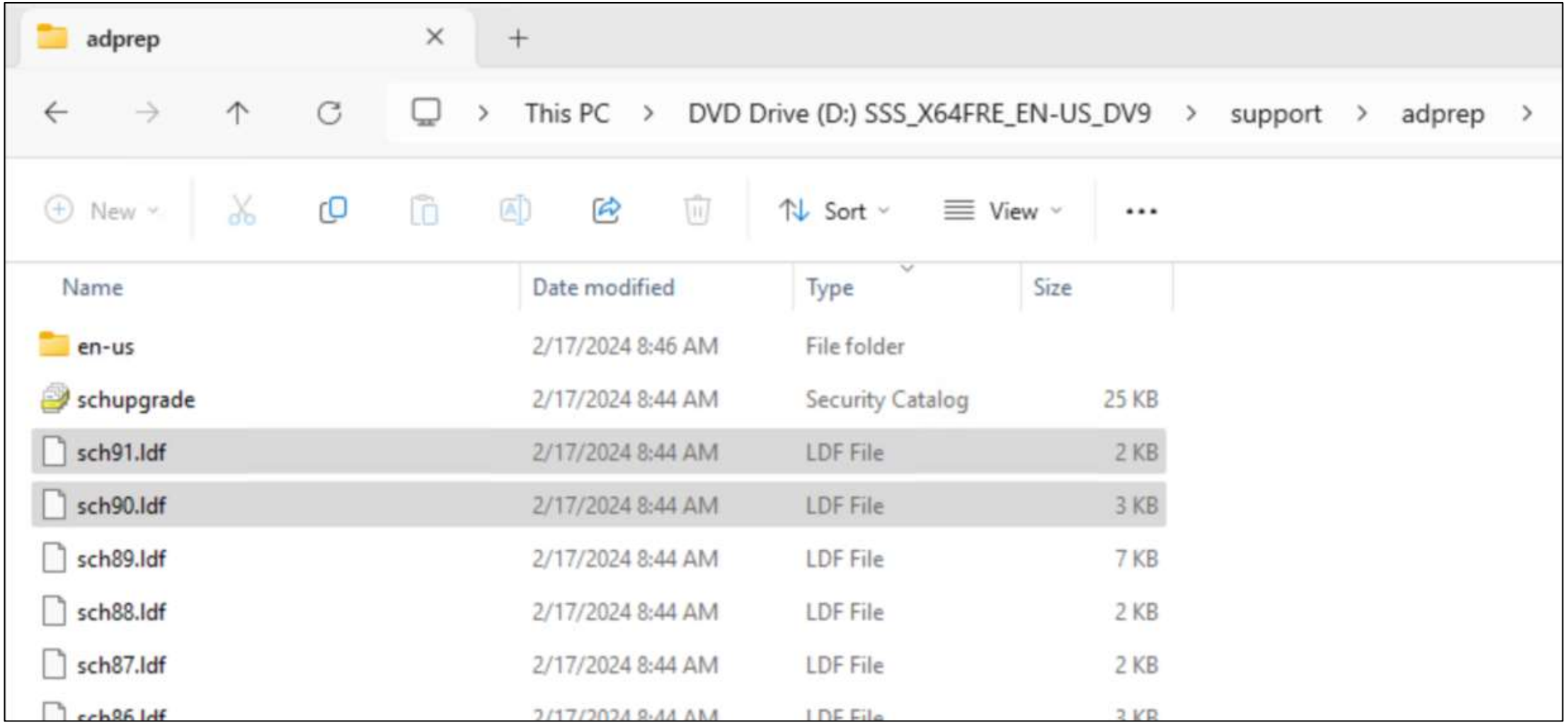
#ADIsNotDead



New Functional Levels



Schema Updates



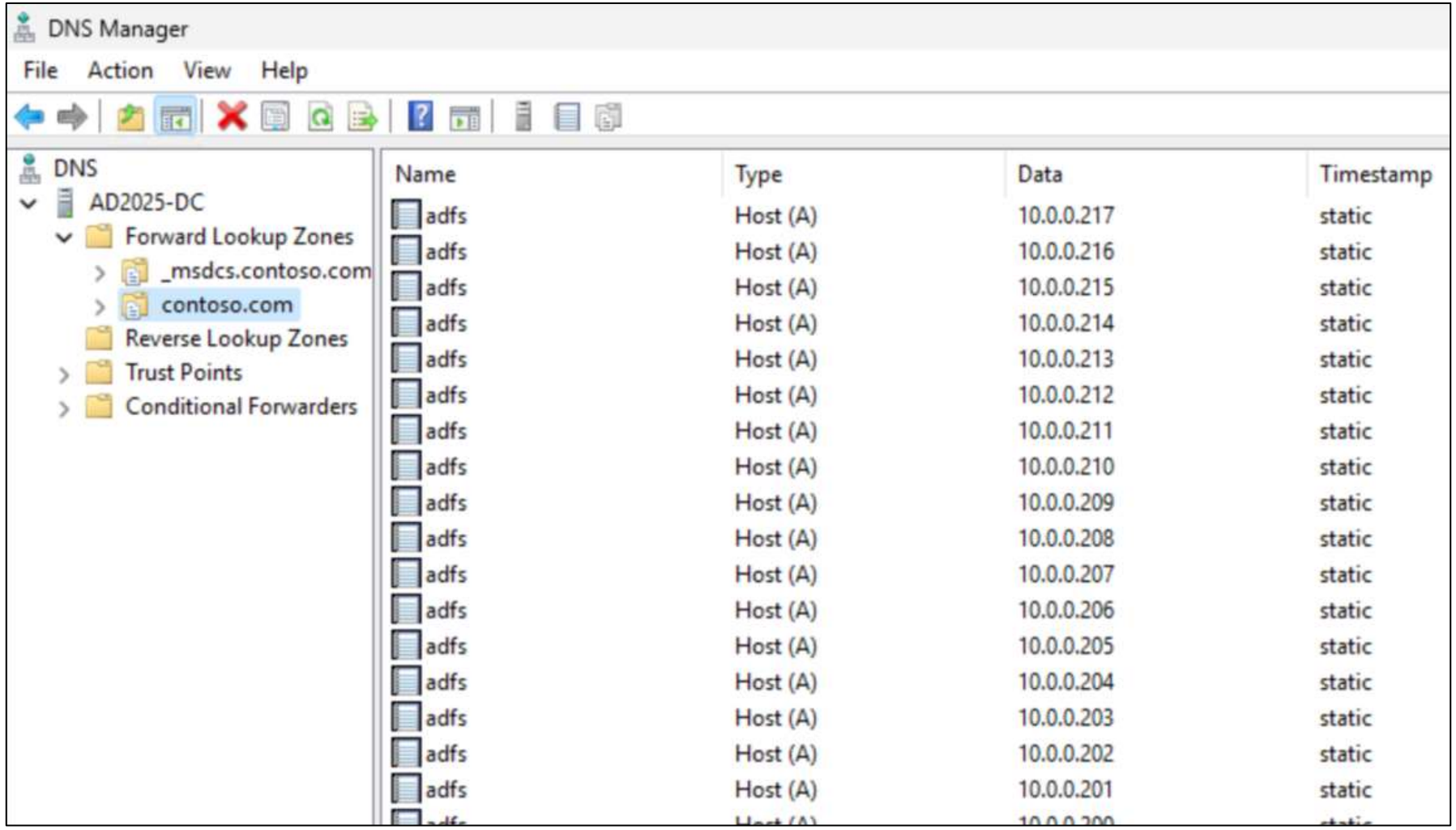
32k Database Page Size Optional Feature

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
                            27m:38s    0 /  15    0
                            16m:16s    0 /  15    0
                            26m:20s    0 /  15    0
                            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.
```

Image Source: https://www.azure365pro.com/the-maximum-size-of-an-object-has-been-exceeded/

32k Database Page Size Optional Feature



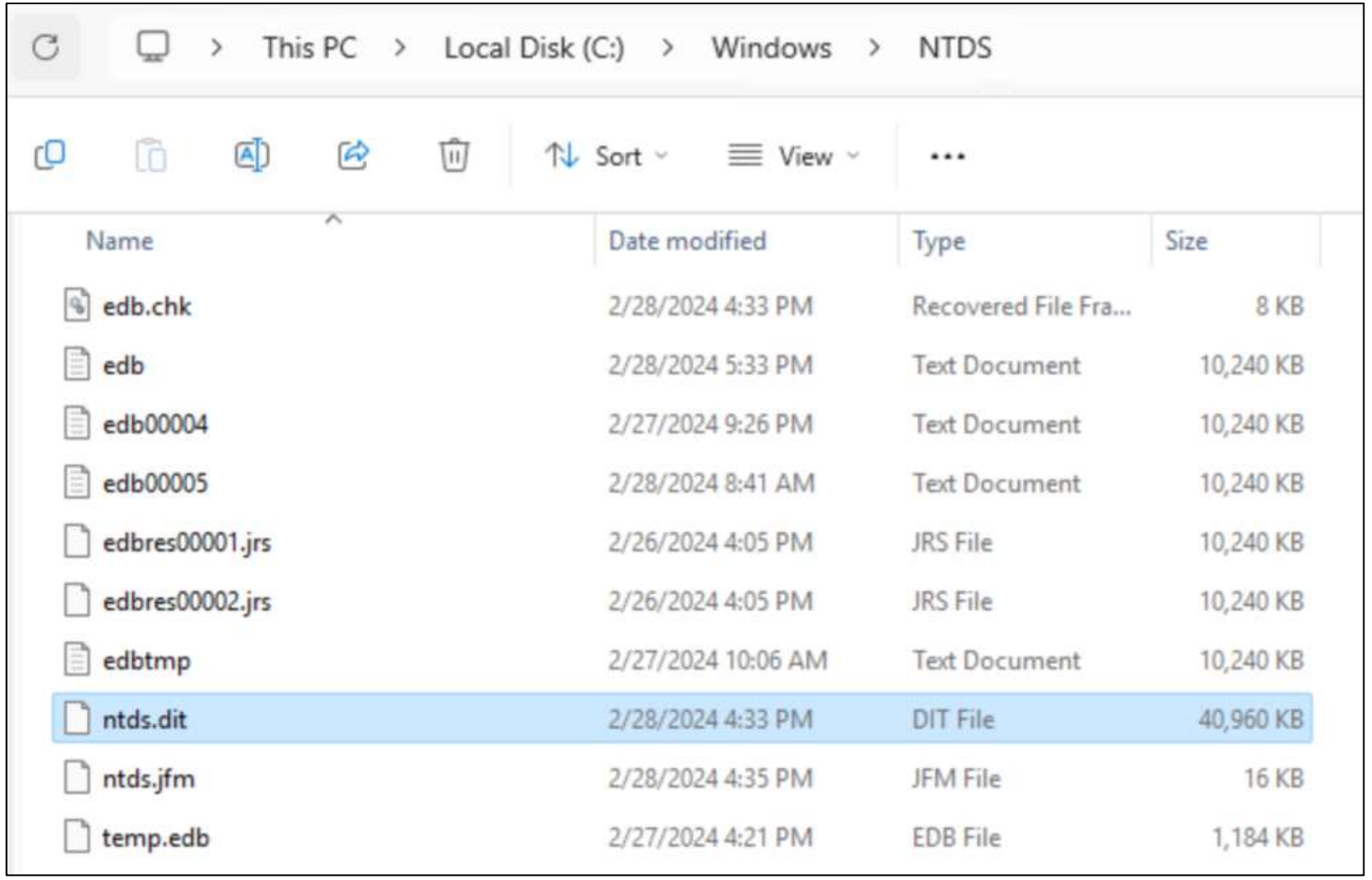
32k Database Page Size Optional Feature

```
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 dwTimed
        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
```

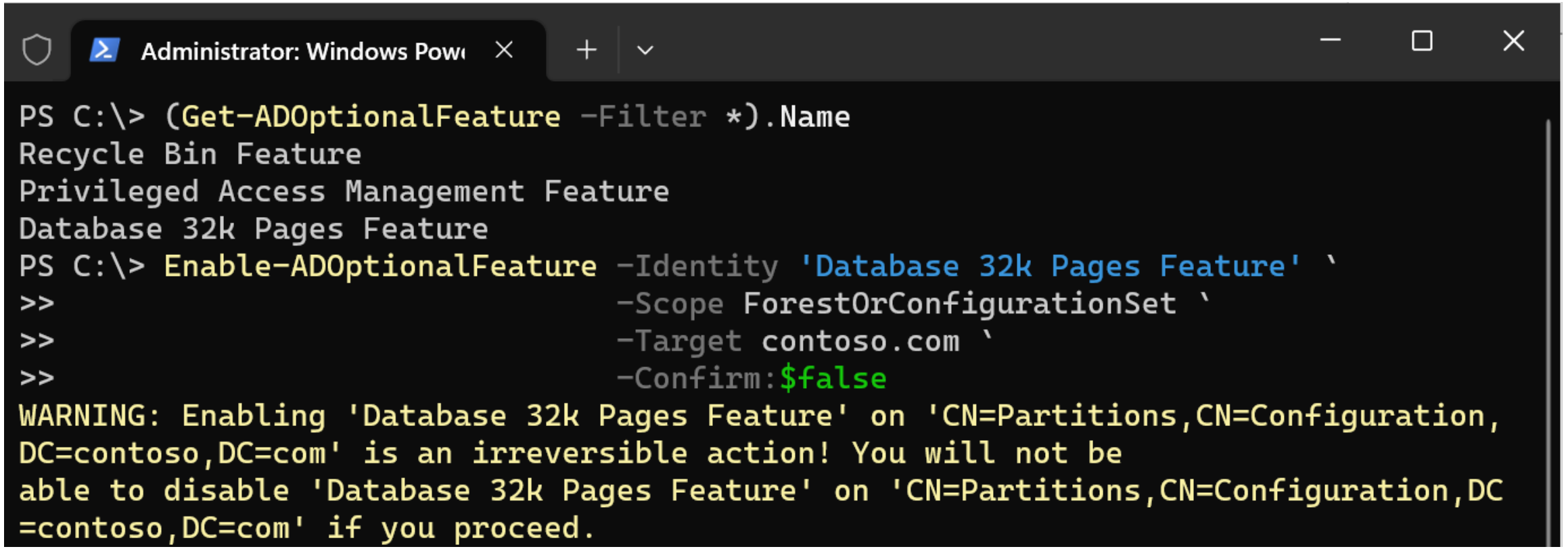
32k Database Page Size Optional Feature



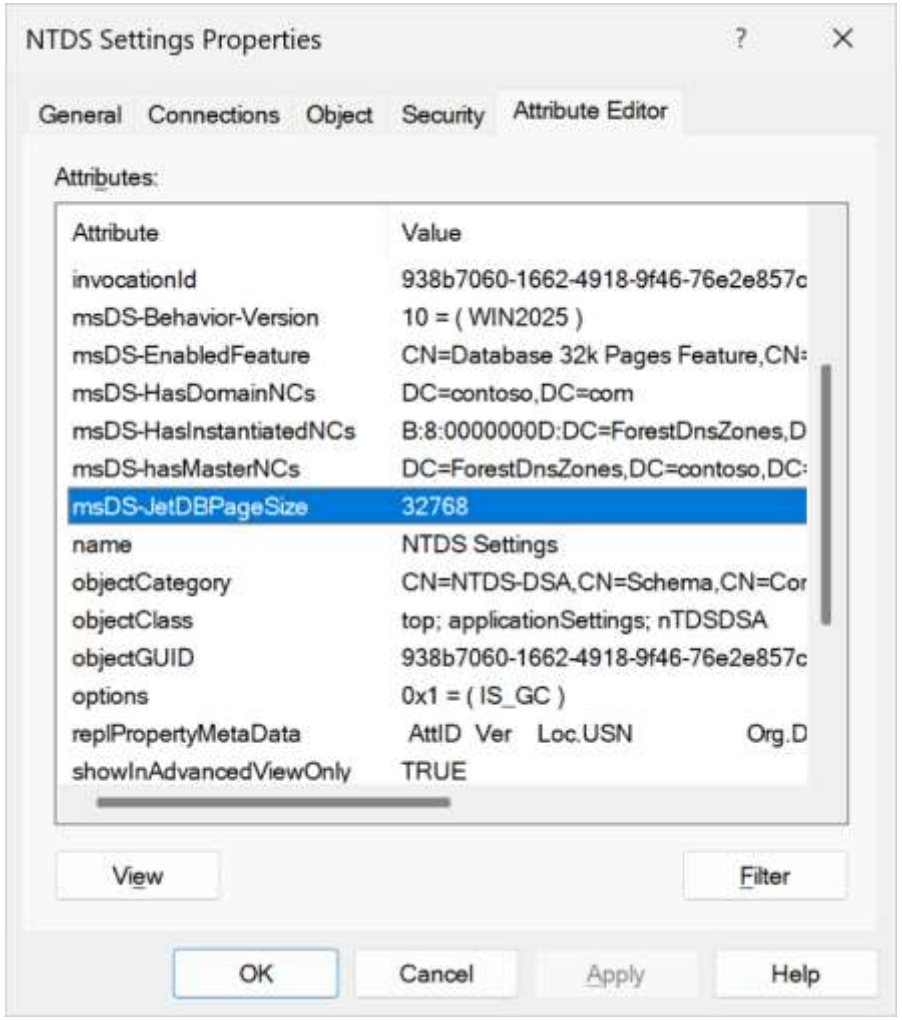
32k Database Page Size Optional Feature

```
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
```

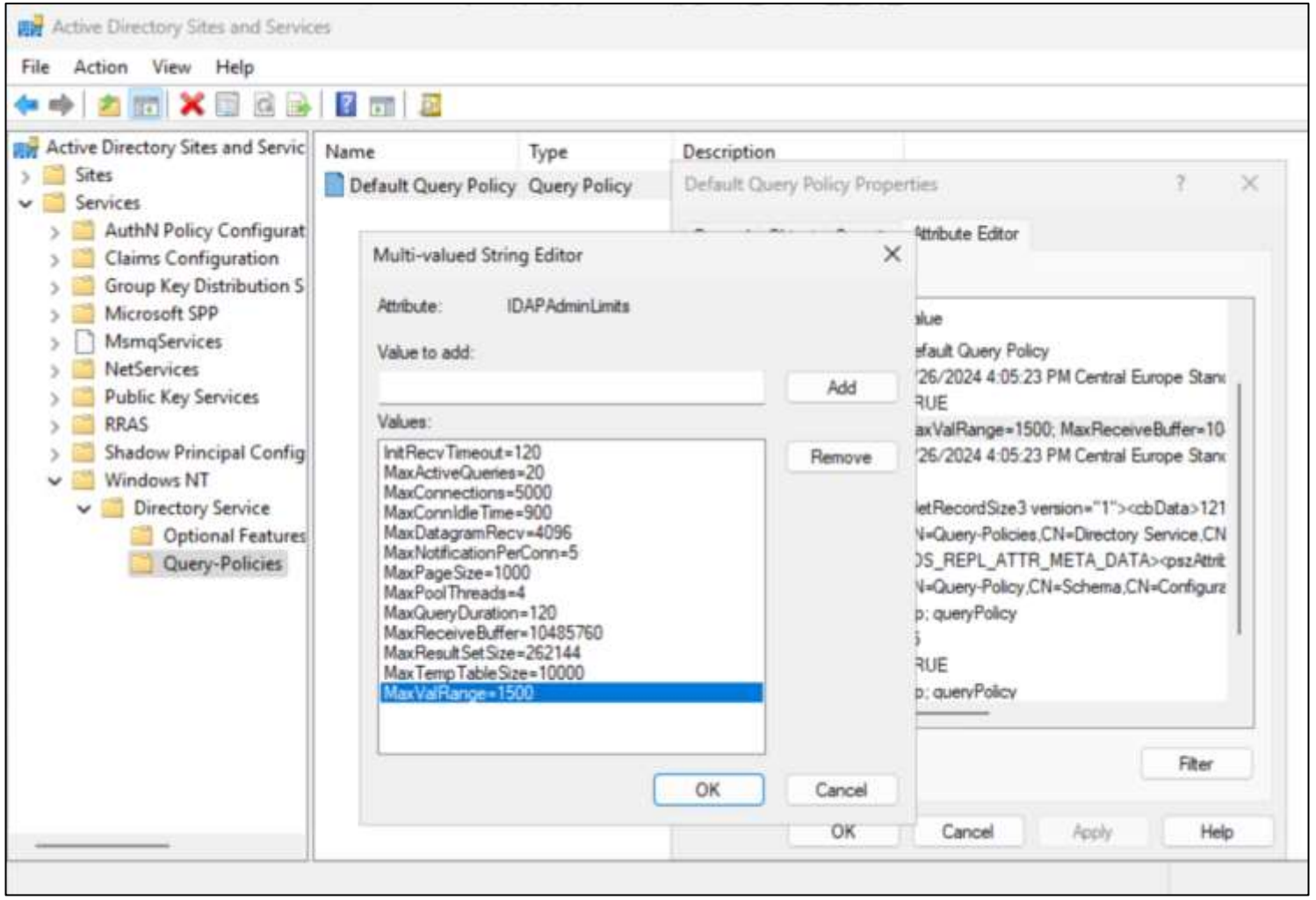
32k Database Page Size Optional Feature



32k Database Page Size Optional Feature



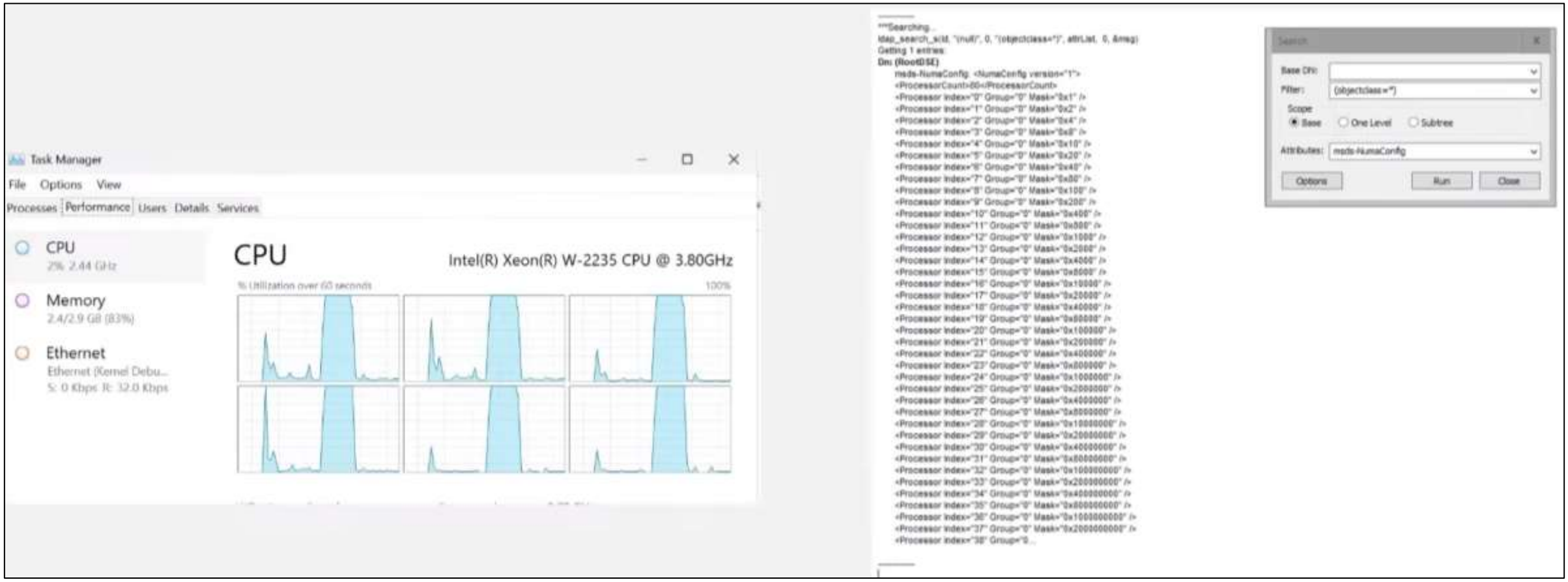
32k Database Page Size Optional Feature



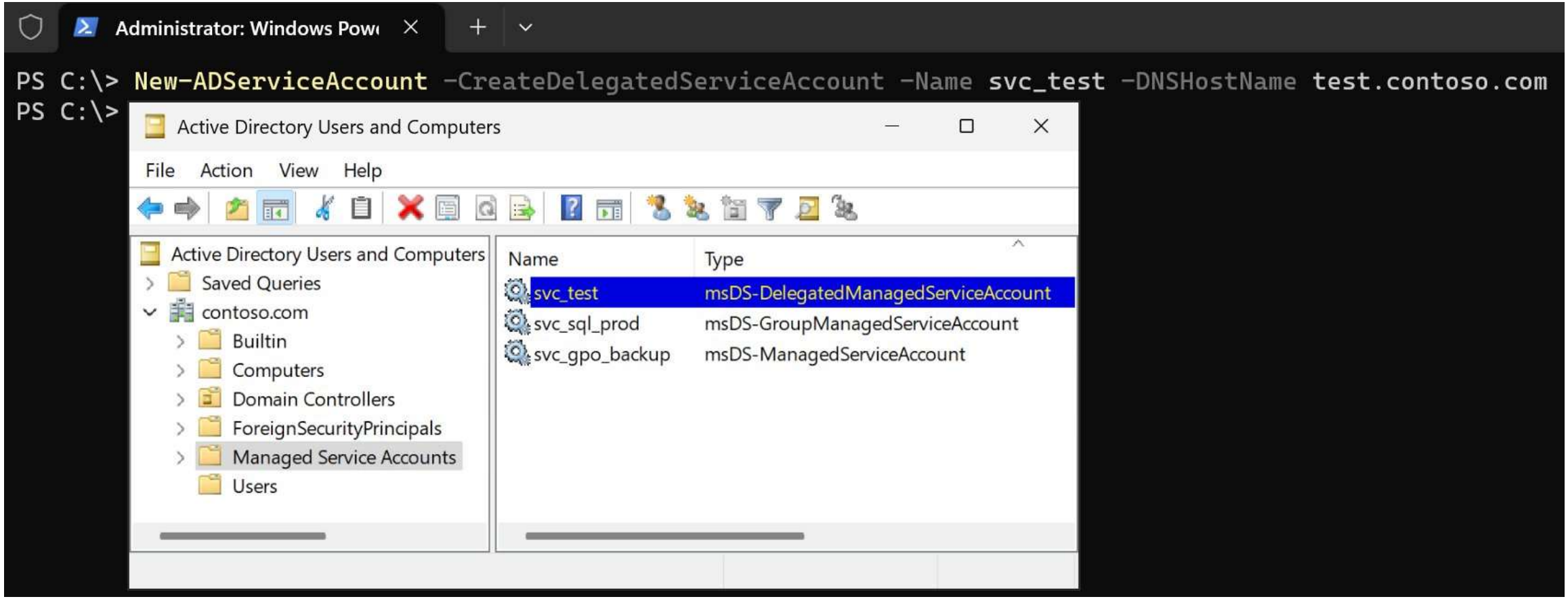
32k Database Page Size Optional Feature

```
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:
        dwTtlSeconds: 269352960 dwTimeout: 0 dwStartRefreshHr: 0 Data: 10.0.64.95; wDataLength: 4 wType: 1; Version: 5 Rank: 240
        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>
    <cIntrinsicLongValues>3</cIntrinsicLongValues>
    <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)



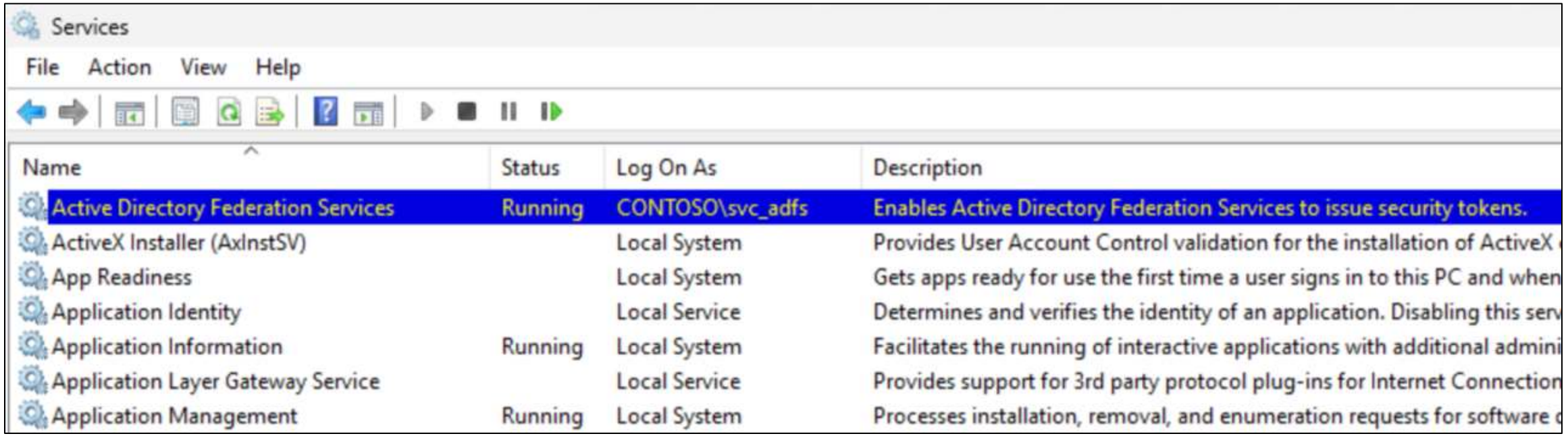
Delegated Managed Service Account



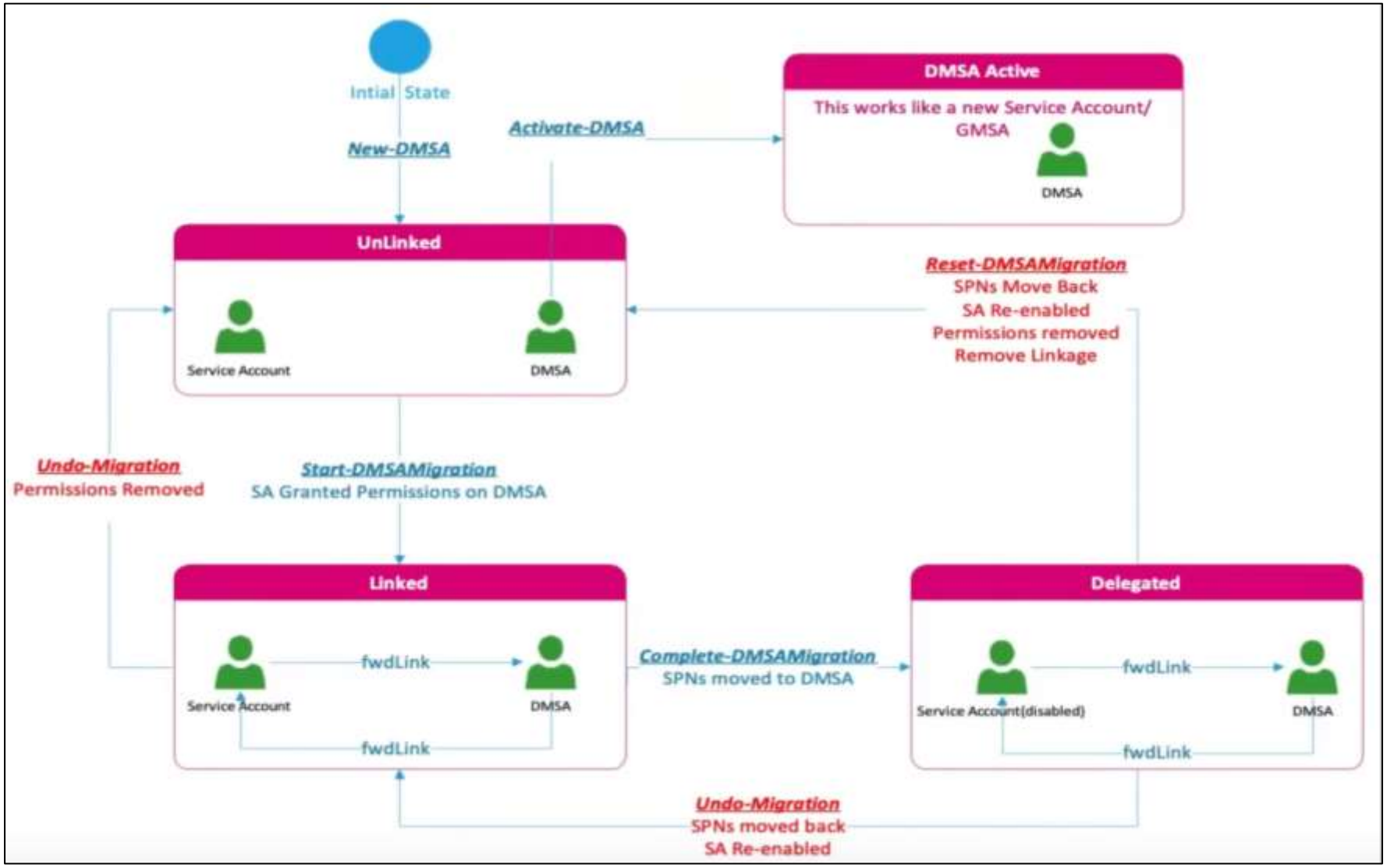
Delegated Managed Service Account

- 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



Delegated Managed Service Account



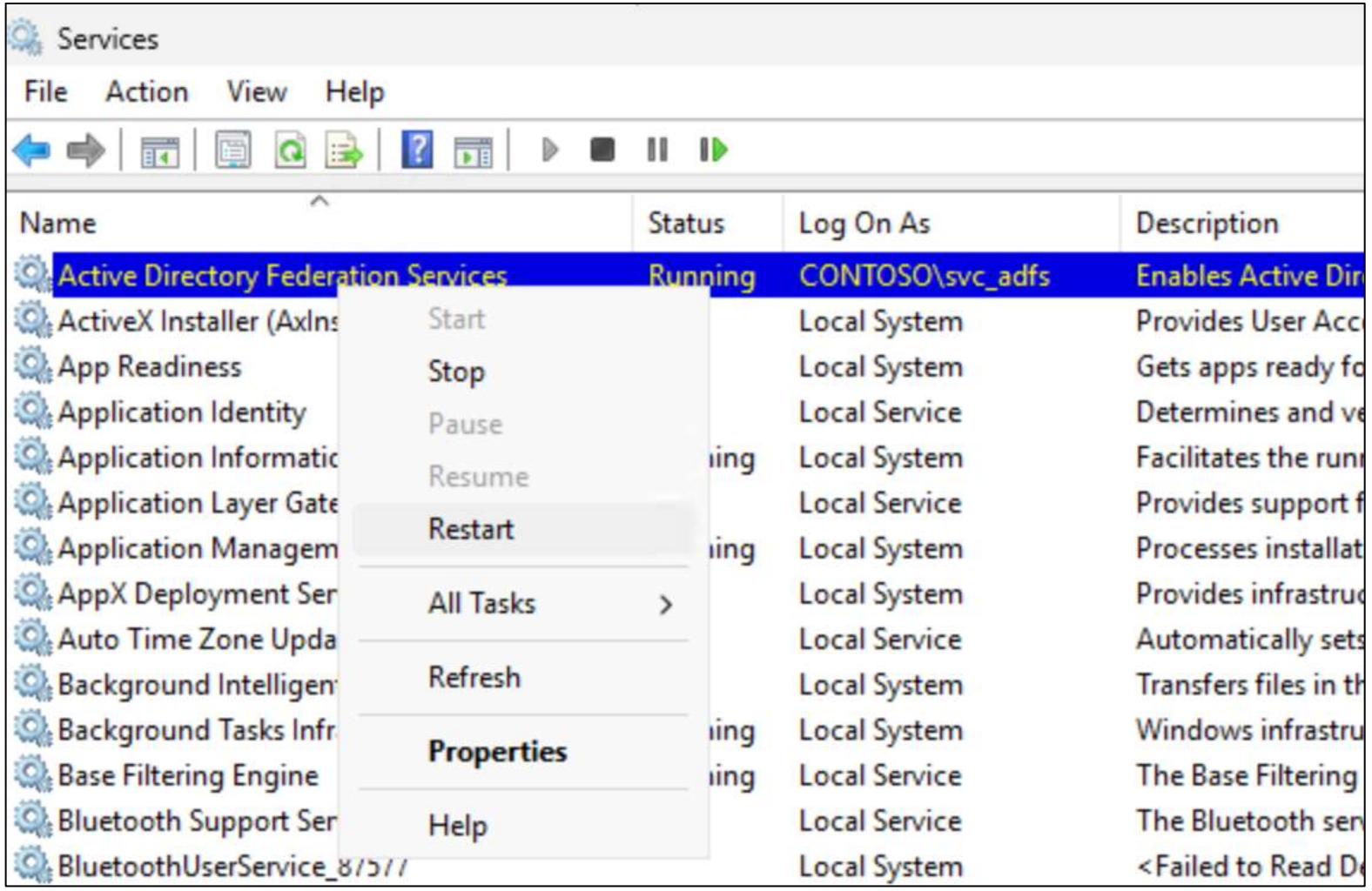
Delegated Managed Service Account

```
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
```

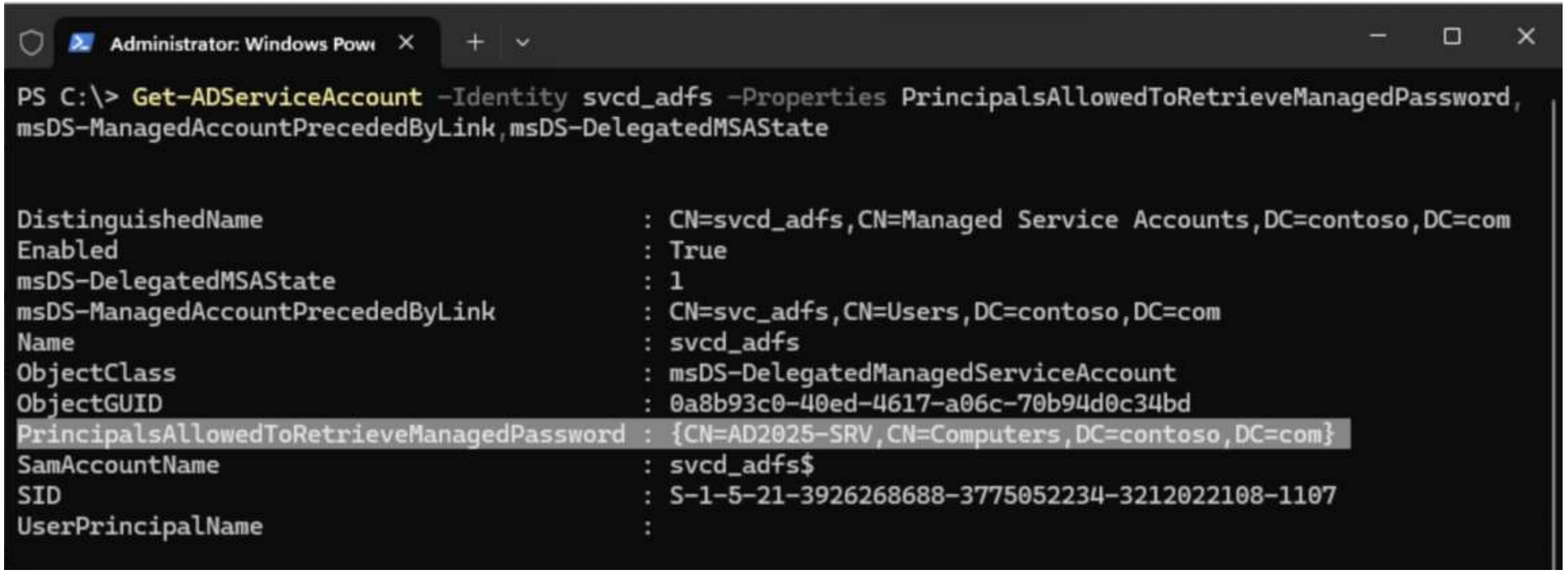
Start-ADServiceAccountMigration

- 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

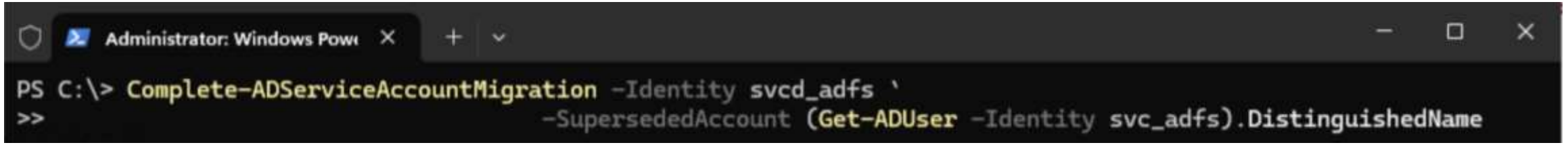
Delegated Managed Service Account



Delegated Managed Service Account



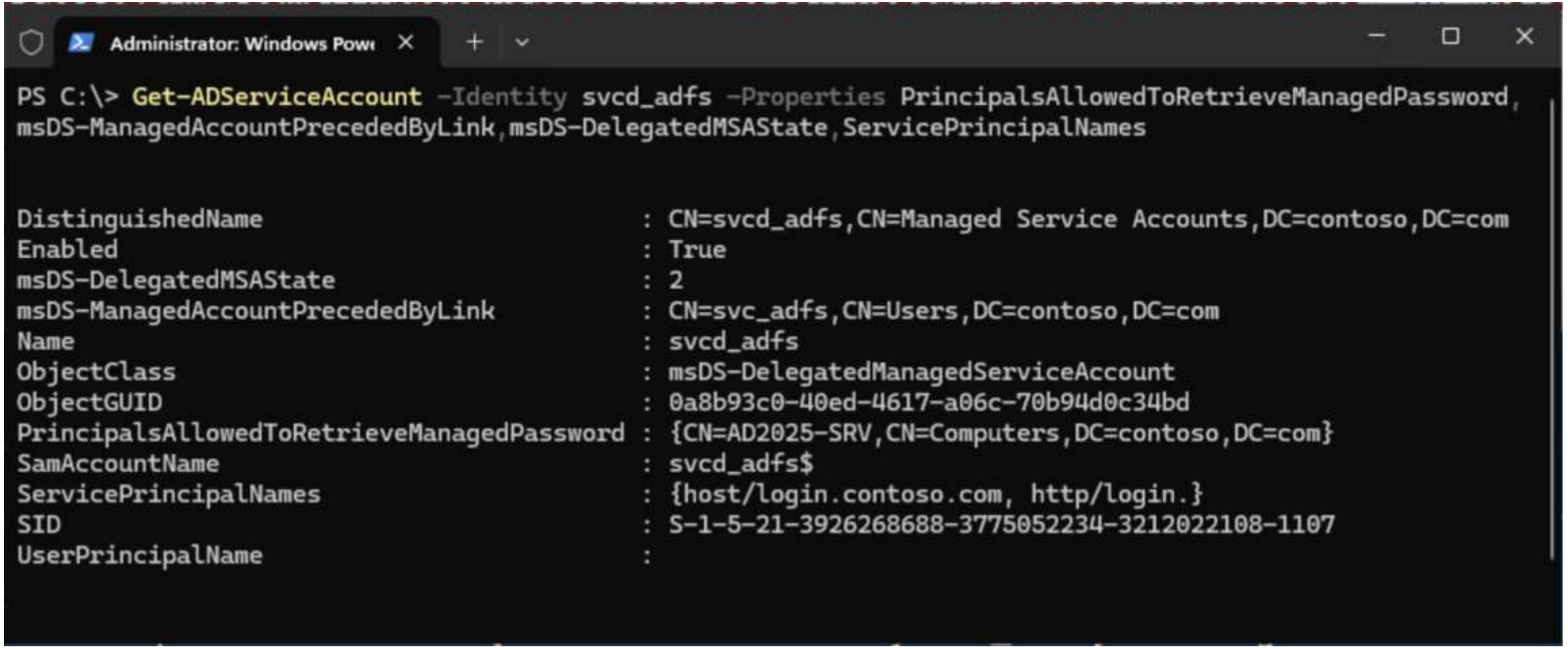
Delegated Managed Service Account



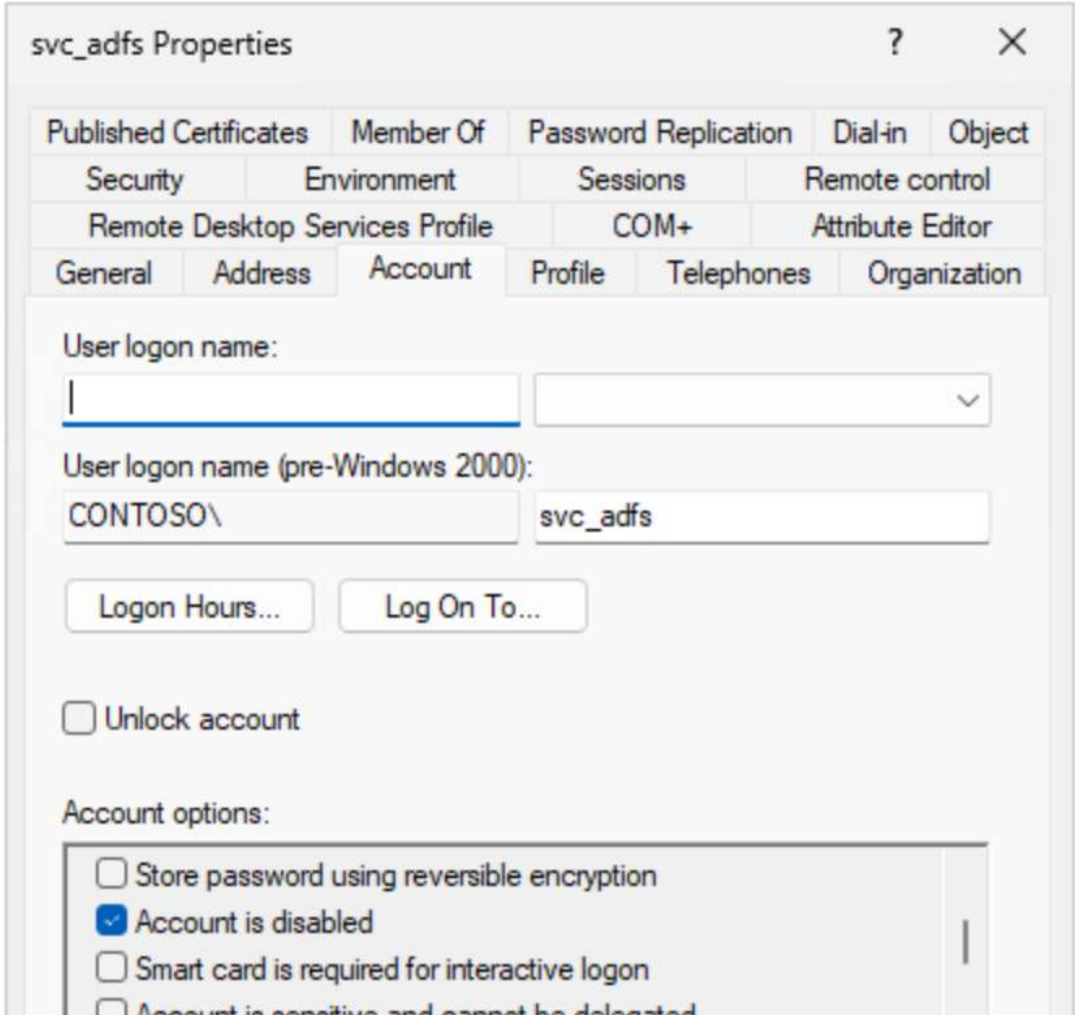
Complete-ADServiceAccountMigration

- 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

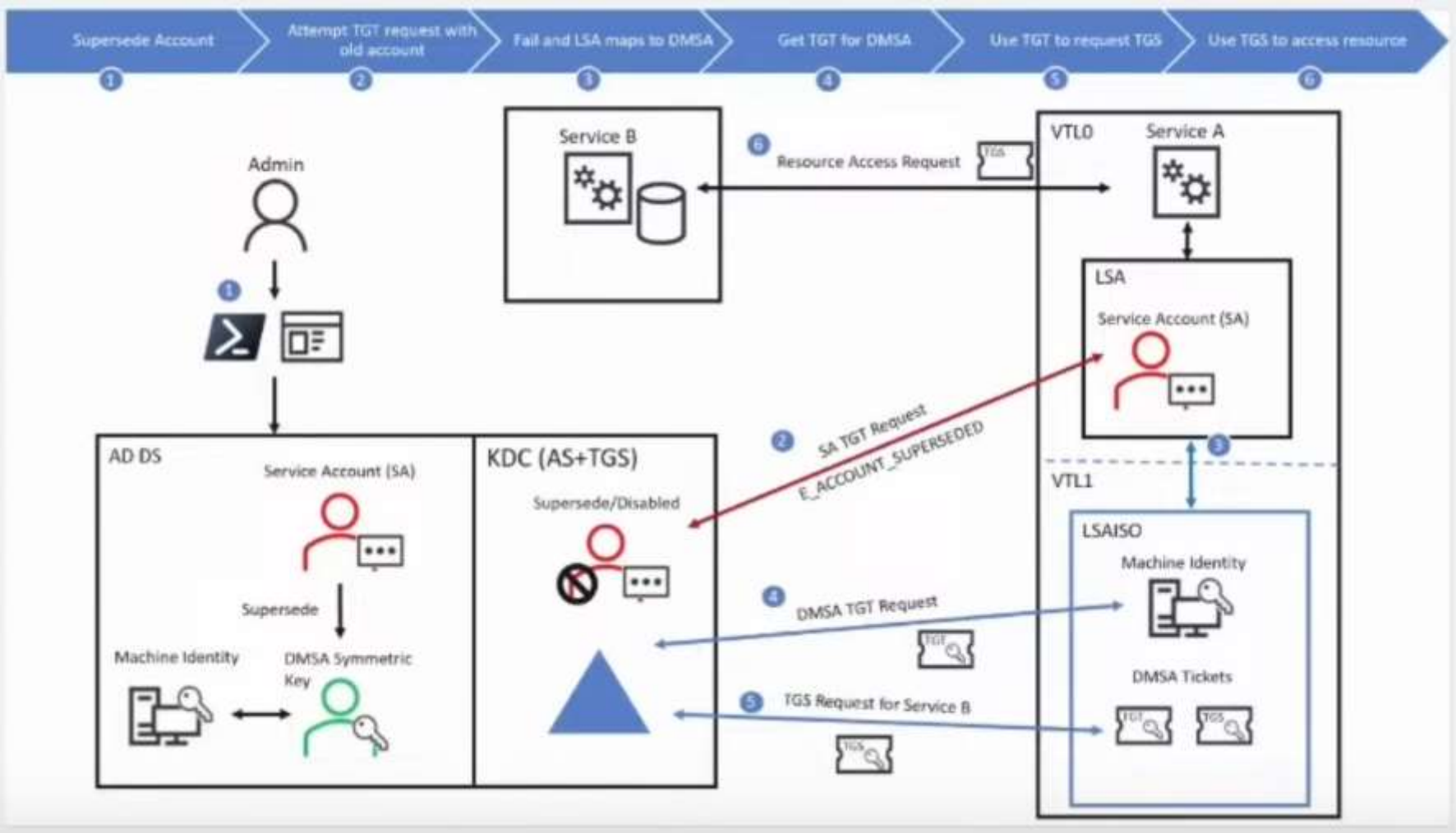
Delegated Managed Service Account



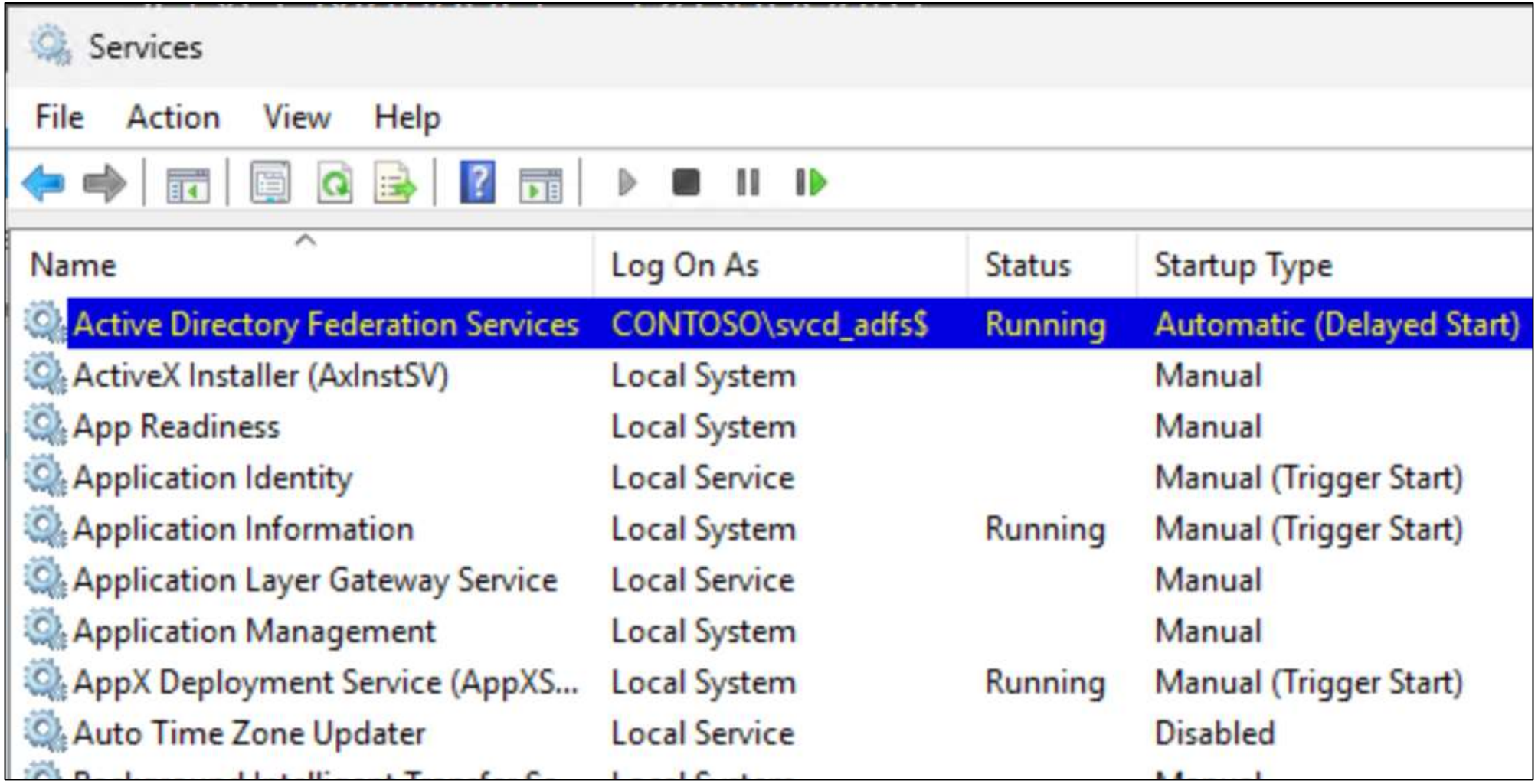
Delegated Managed Service Account



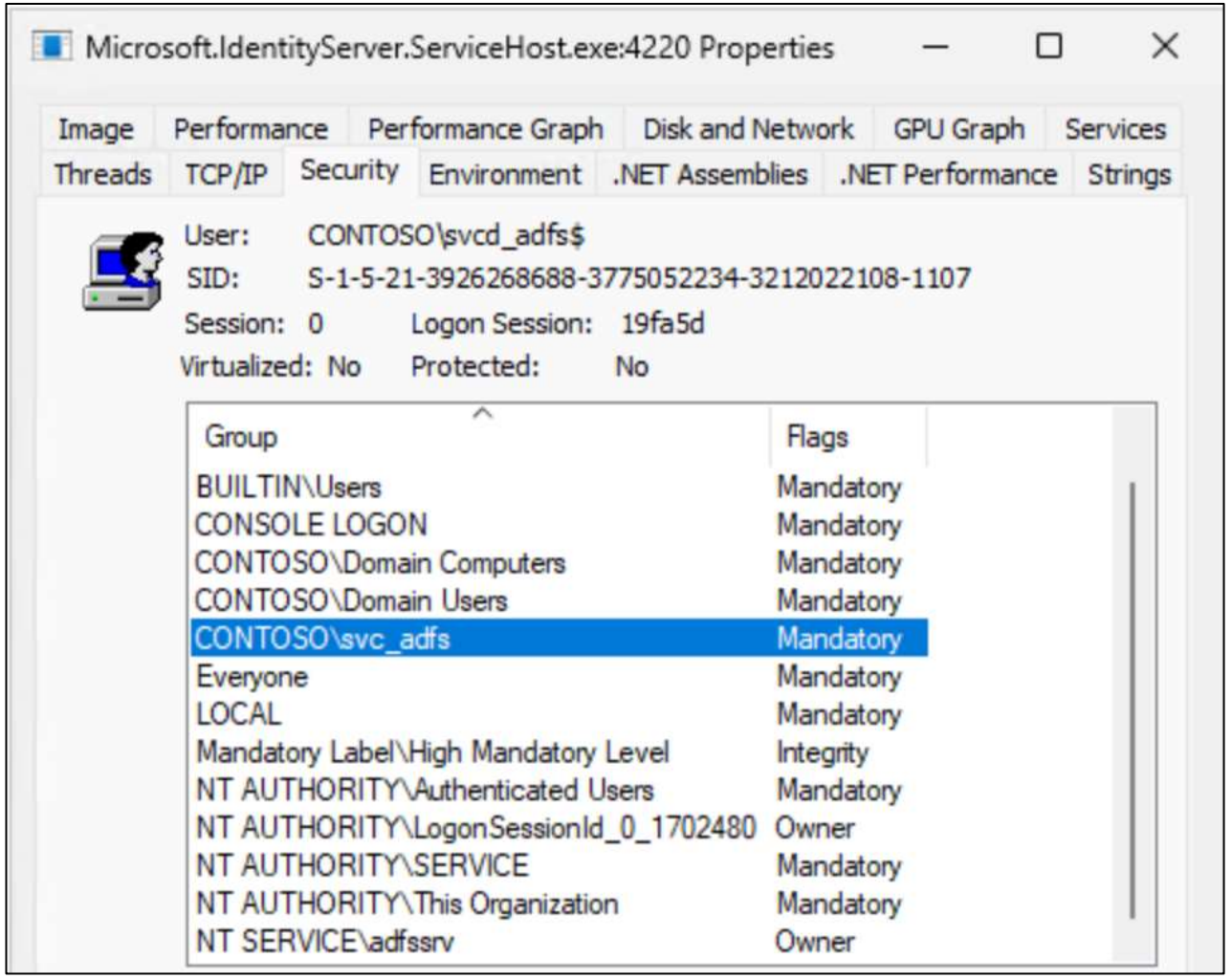
Delegated Managed Service Account



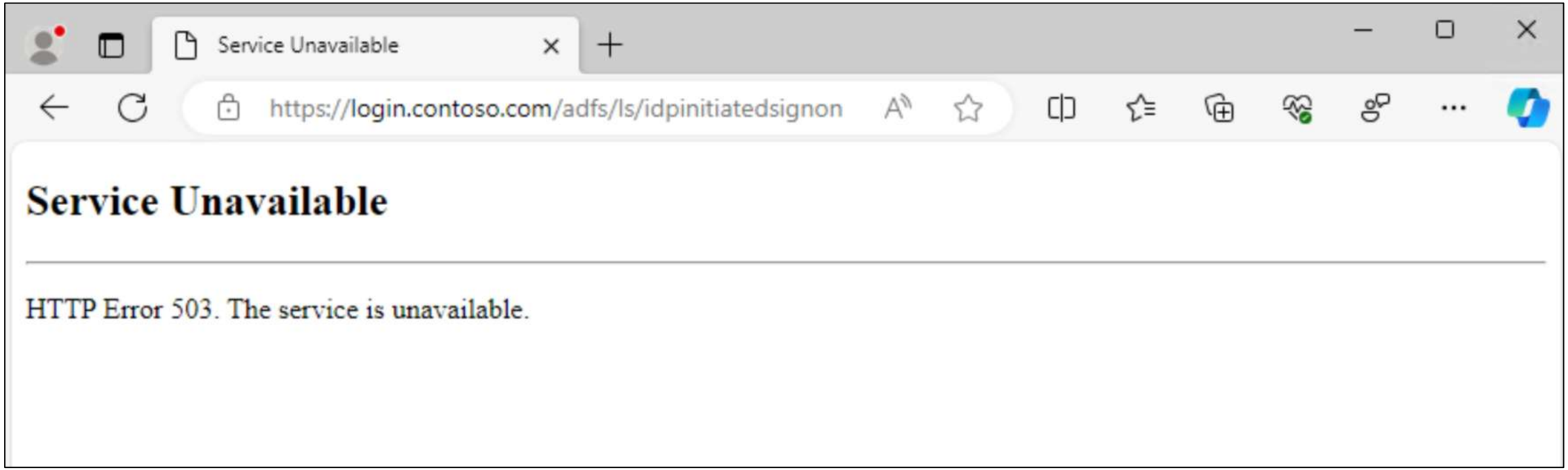
Delegated Managed Service Account



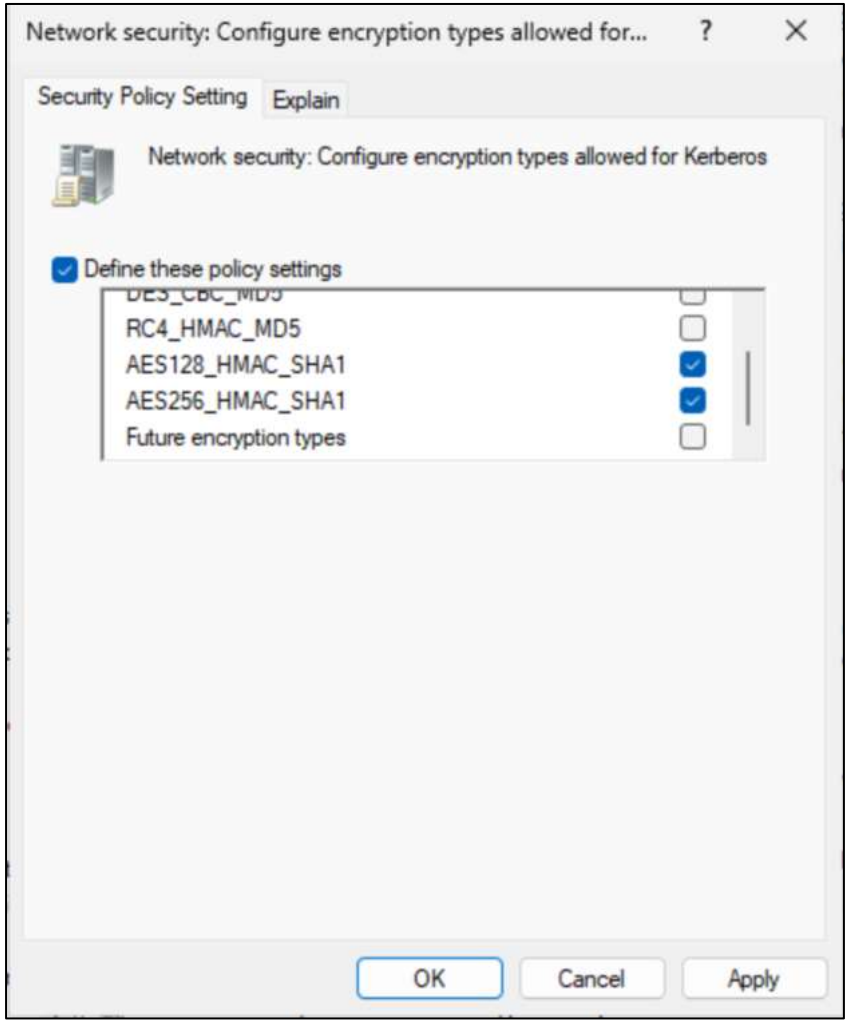
Delegated Managed Service Account



Delegated Managed Service Account



Kerberos AES SHA256 and SHA384 Support



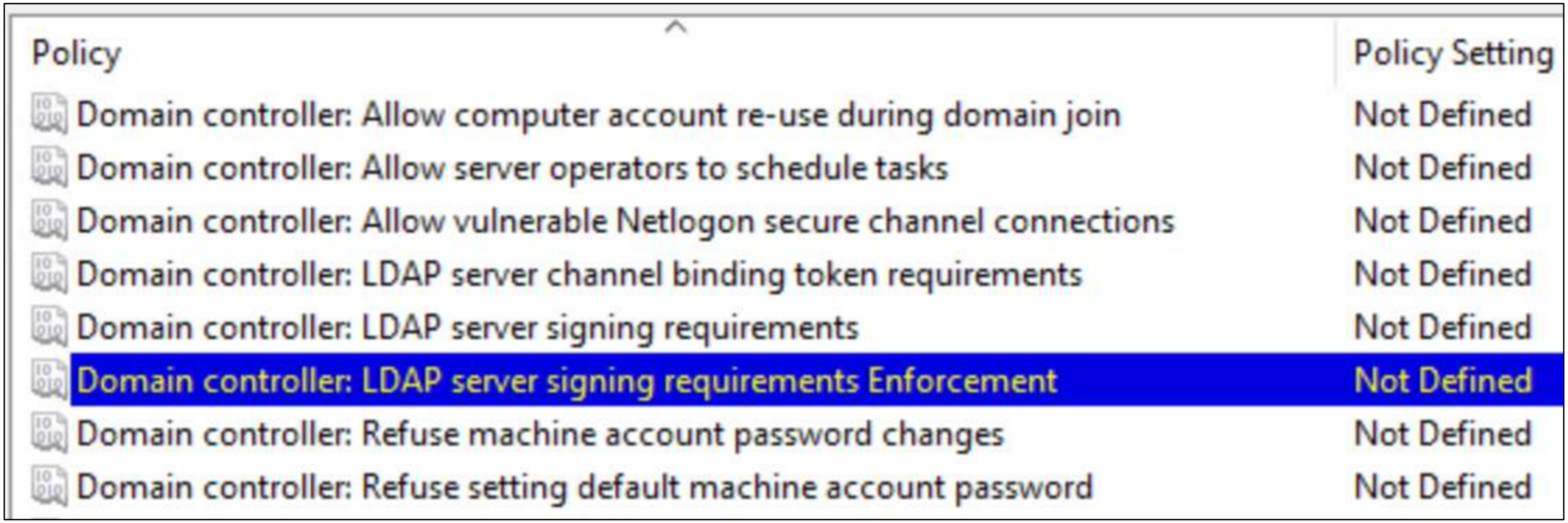
Kerberos AES SHA256 and SHA384 Support

```
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)

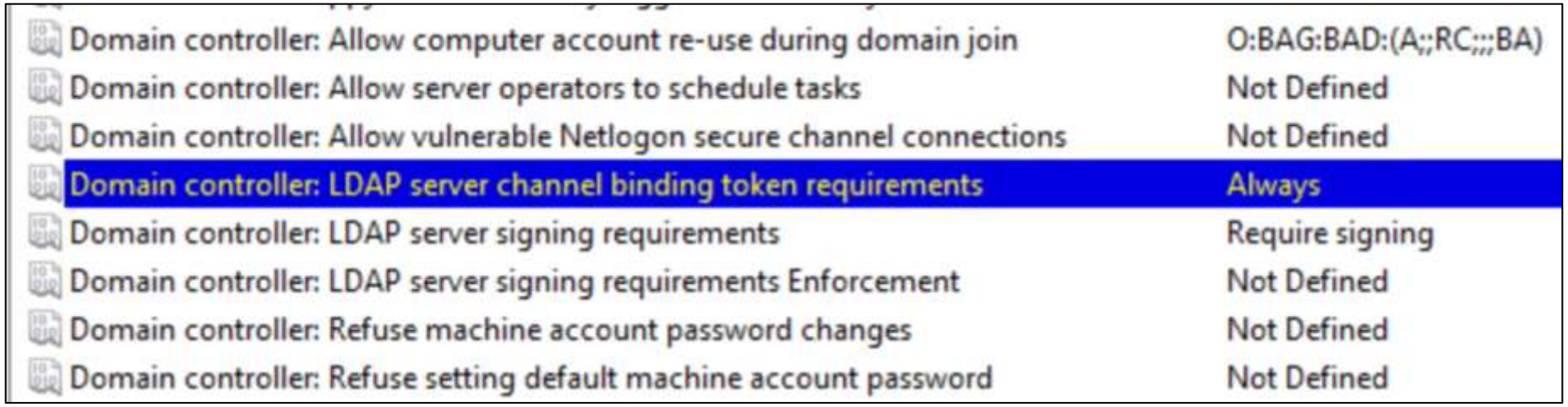
```
# nmap --script ssl-enum-ciphers -p 636 contoso-dc.contoso.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 22:06 CET
Nmap scan report for contoso-dc.contoso.com (10.213.0.3)
Host is up (0.0015s latency).
rDNS record for 10.213.0.3: CONTOSO-DC.contoso.com

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

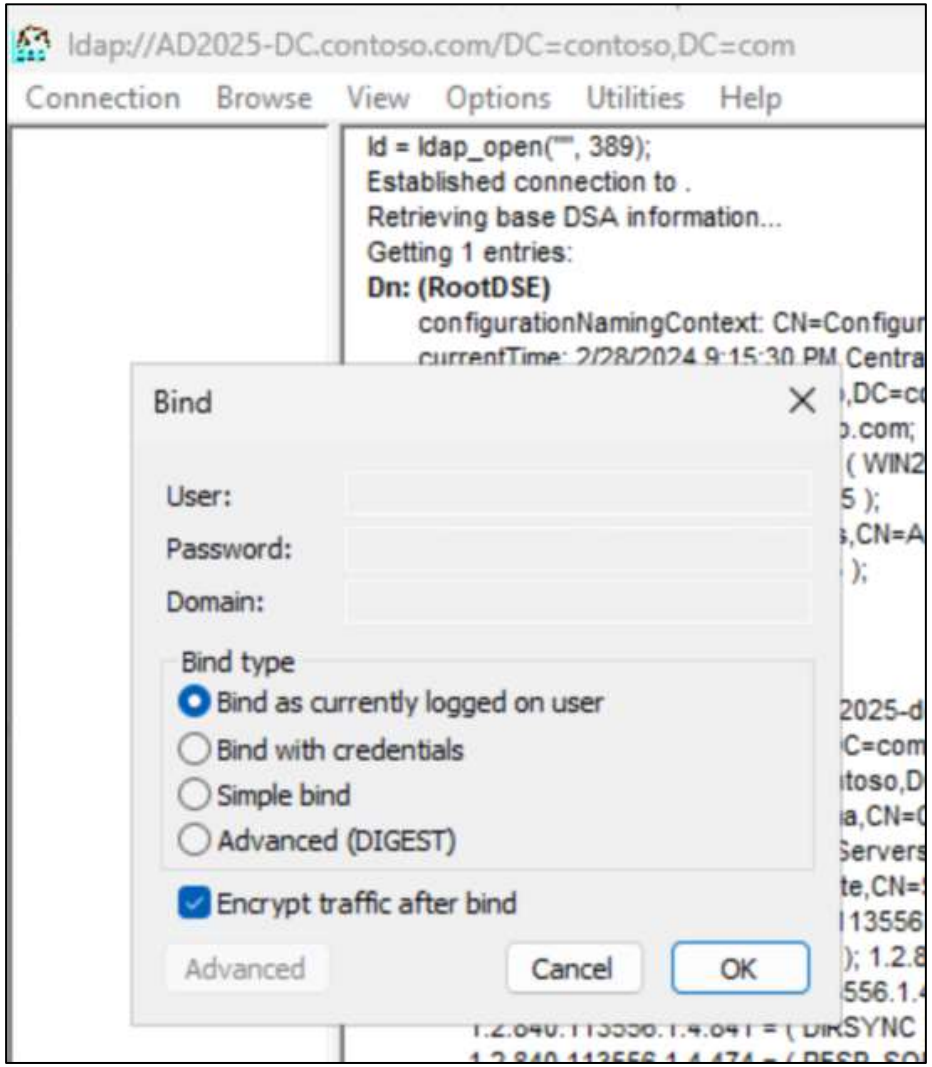
LDAP Channel Binding Audit Support (WS 2019+)



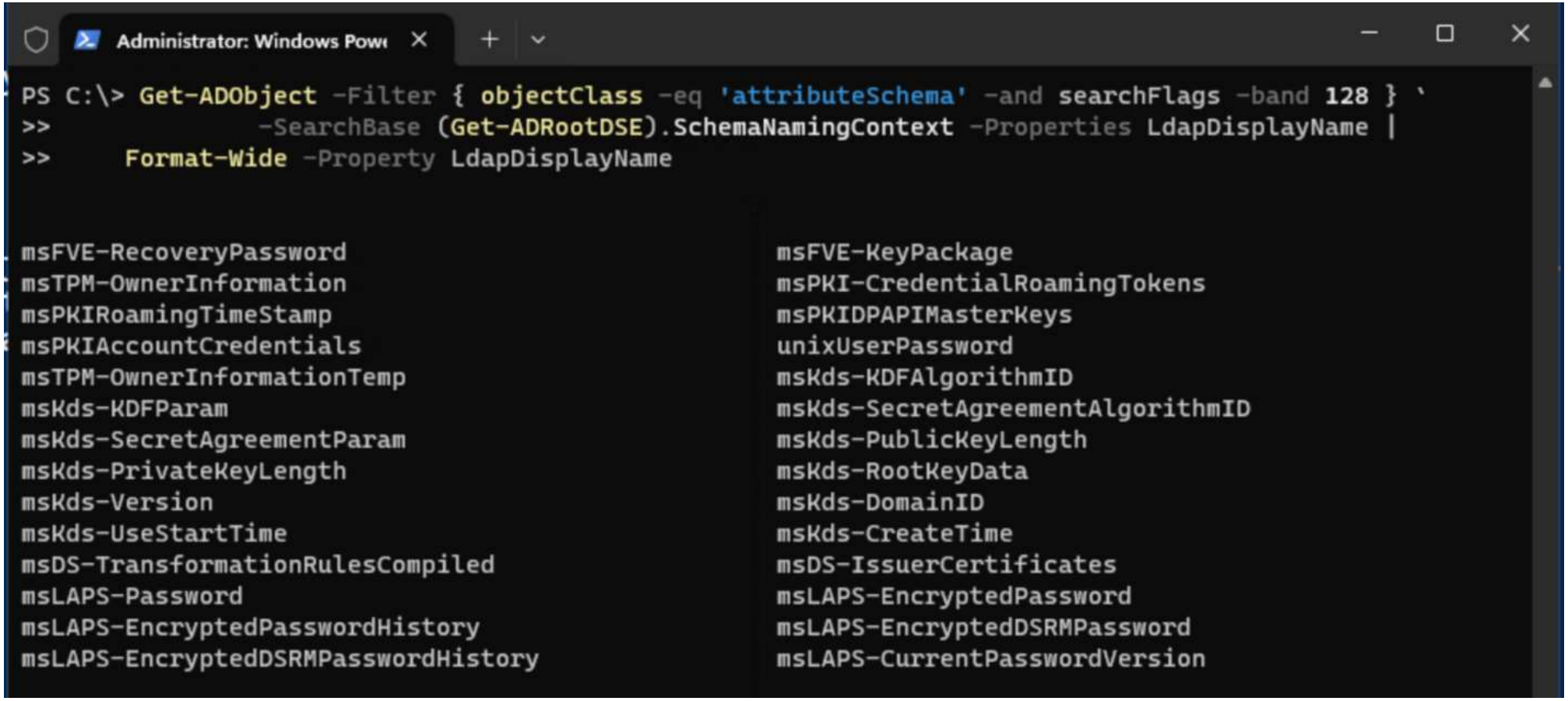
Domain controller: Allow computer account re-use during domain join	O:BAG:BAD:(A;;RC;;;BA)
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel connections	Not Defined
Domain controller: LDAP server channel binding token requirements	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.

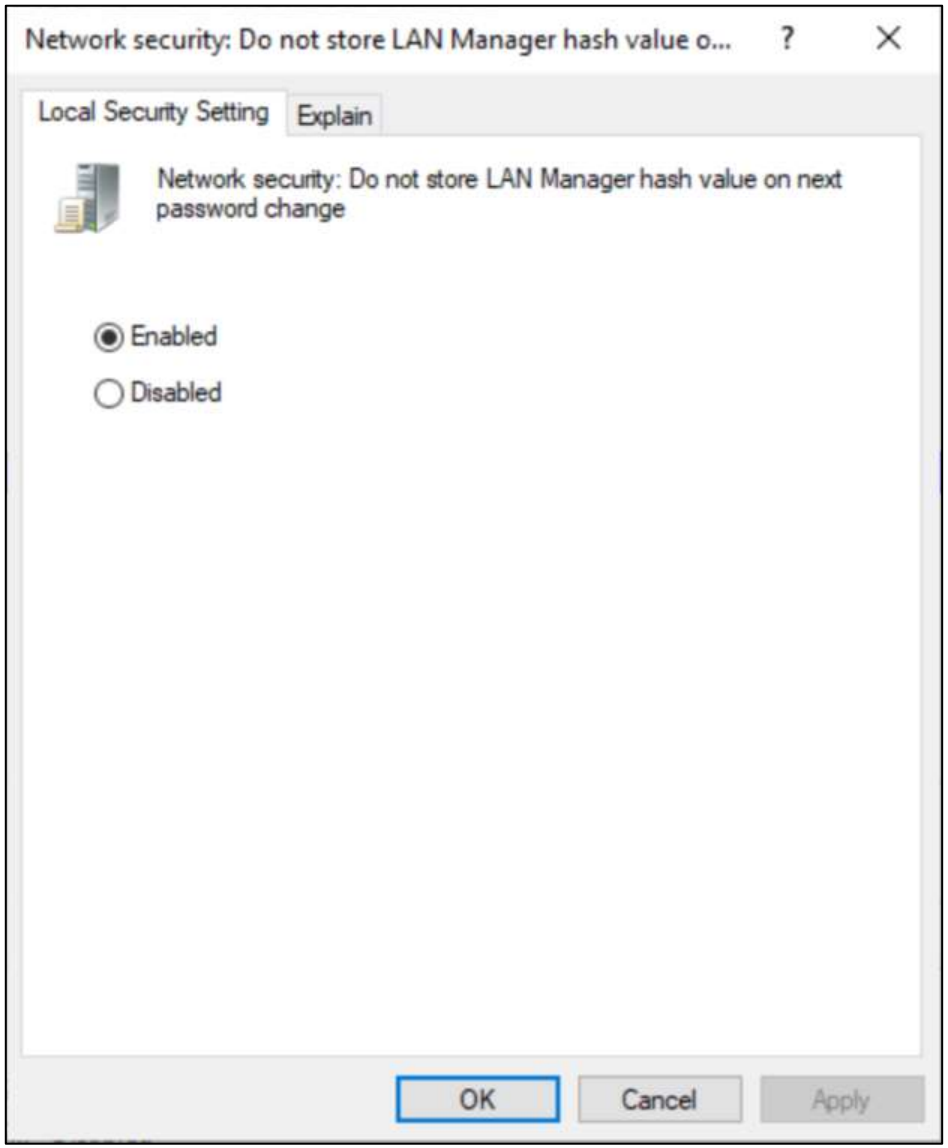
LDAP Client Encryption by Default (SASL)



Confidential Attributes Require Encryption



LAN Manager GPO Setting Removed

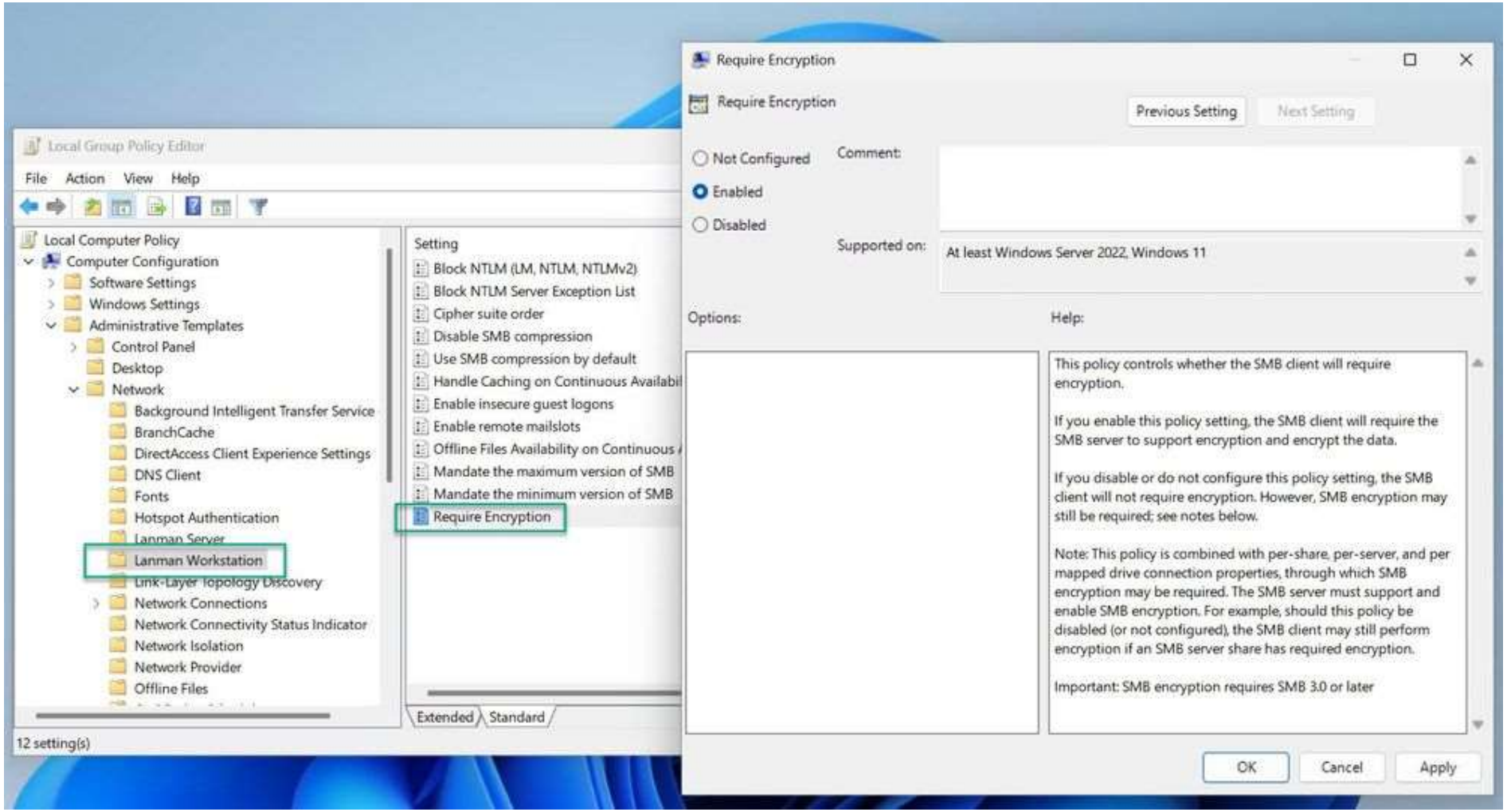


Kerberos PKINIT Support for Cryptographic Agility

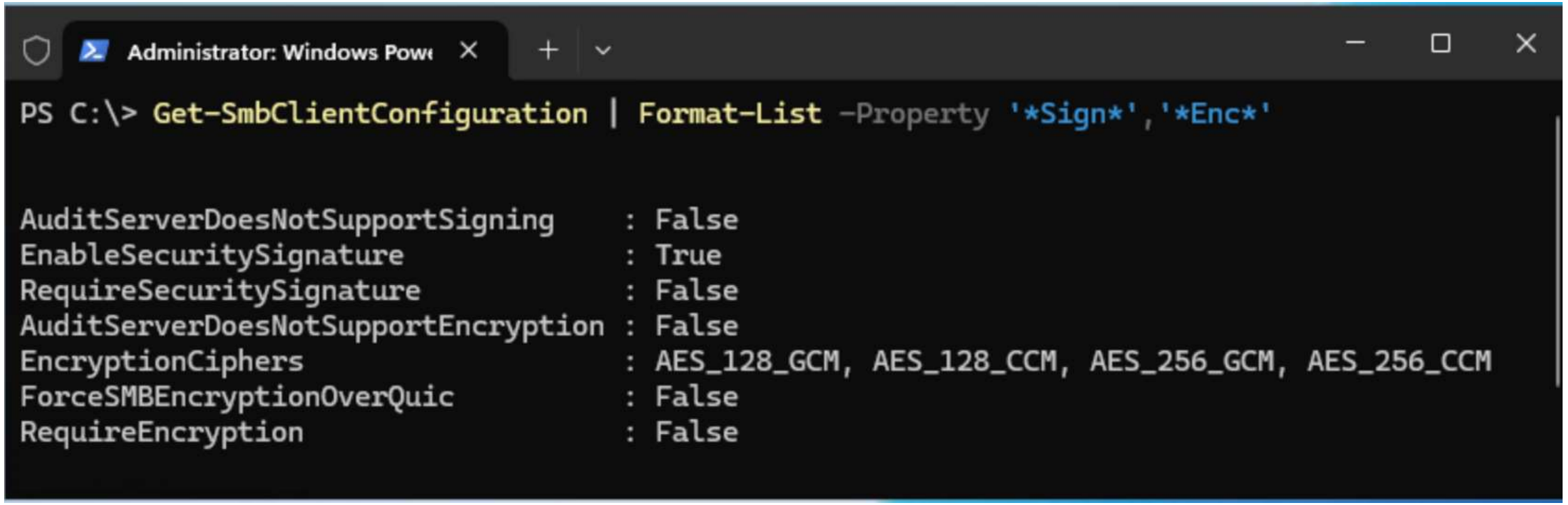
Currently supported algorithms:

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

Enforce SMB Encryption on Clients

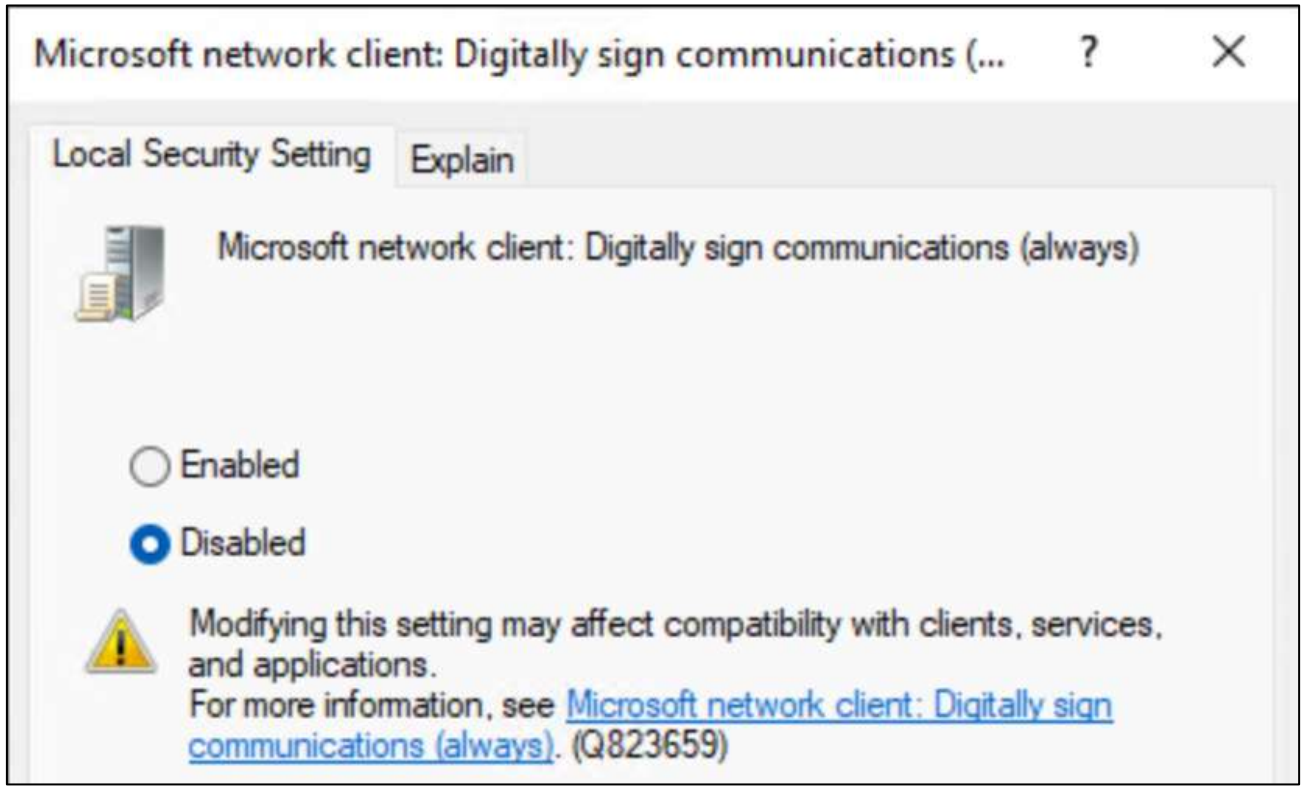


Enforce SMB Encryption on Clients

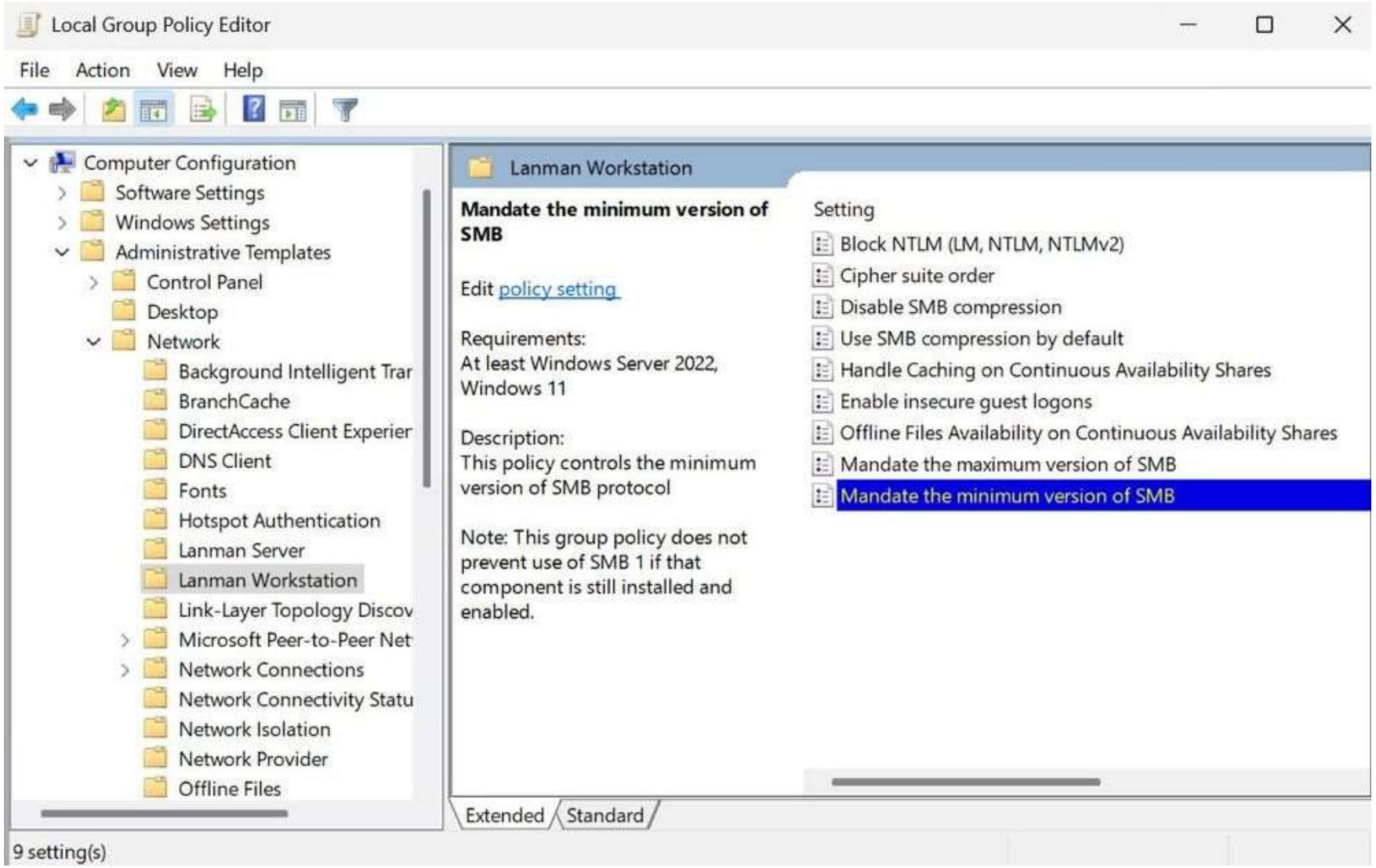


SMB Client Signing Enabled by Default

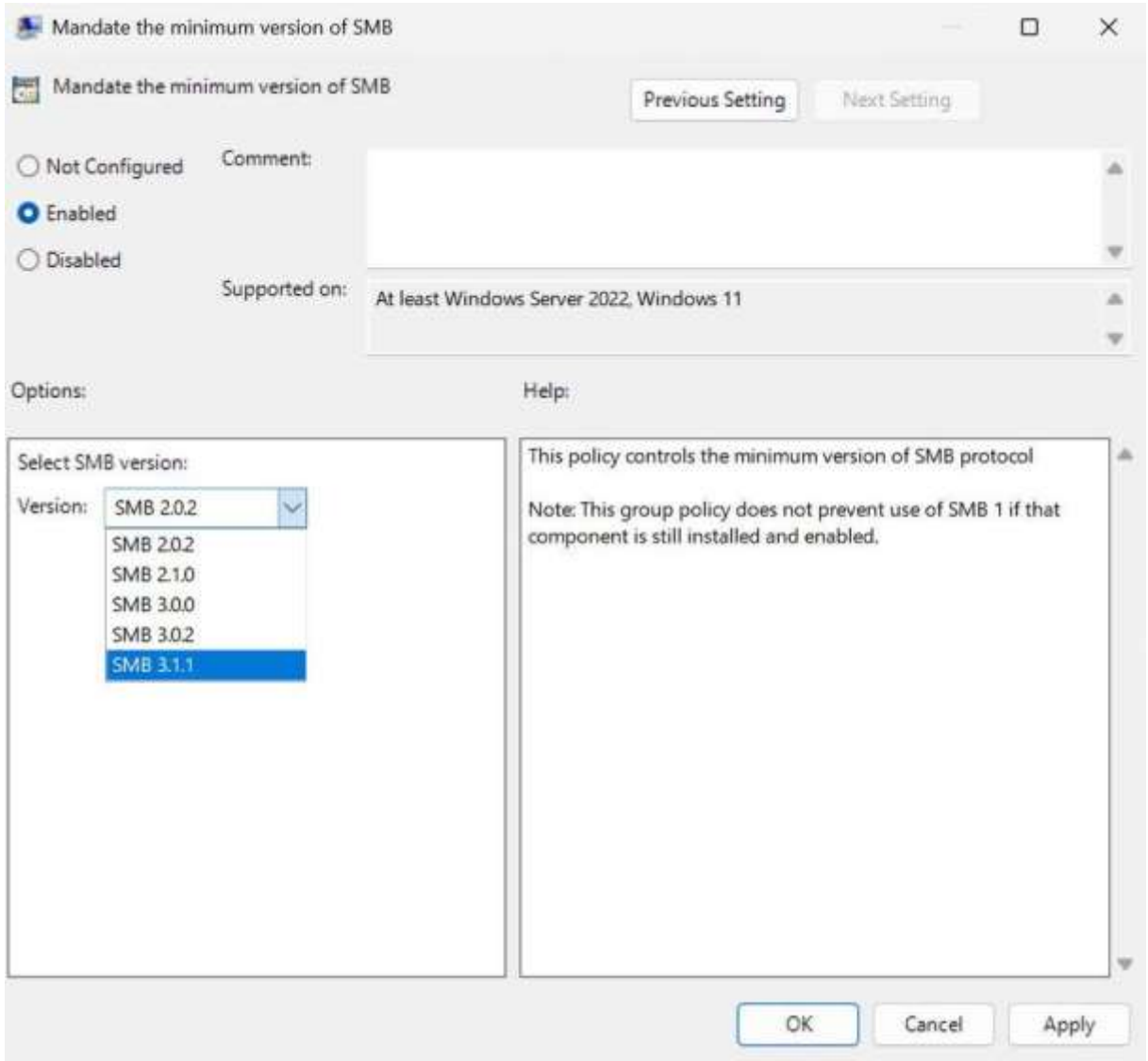
SMB signing is now required by default for all SMB outbound connections where previously it was only required when connecting to shares named SYSVOL and NETLOGON on AD domain controllers.



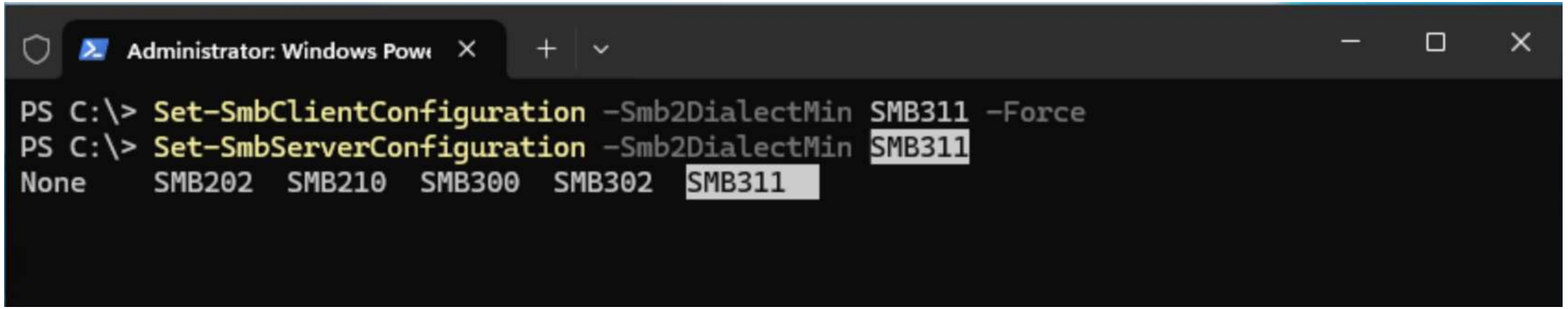
SMB Dialect Management



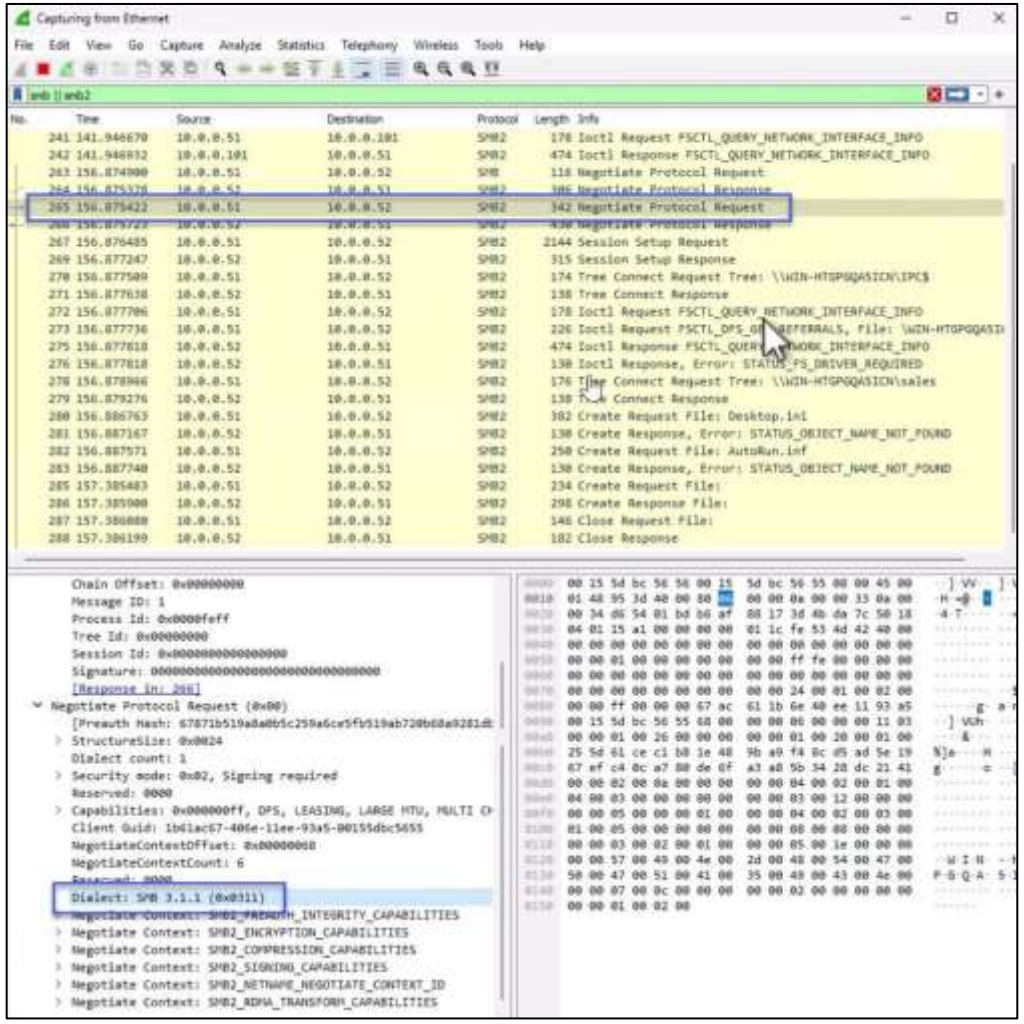
SMB Dialect Management



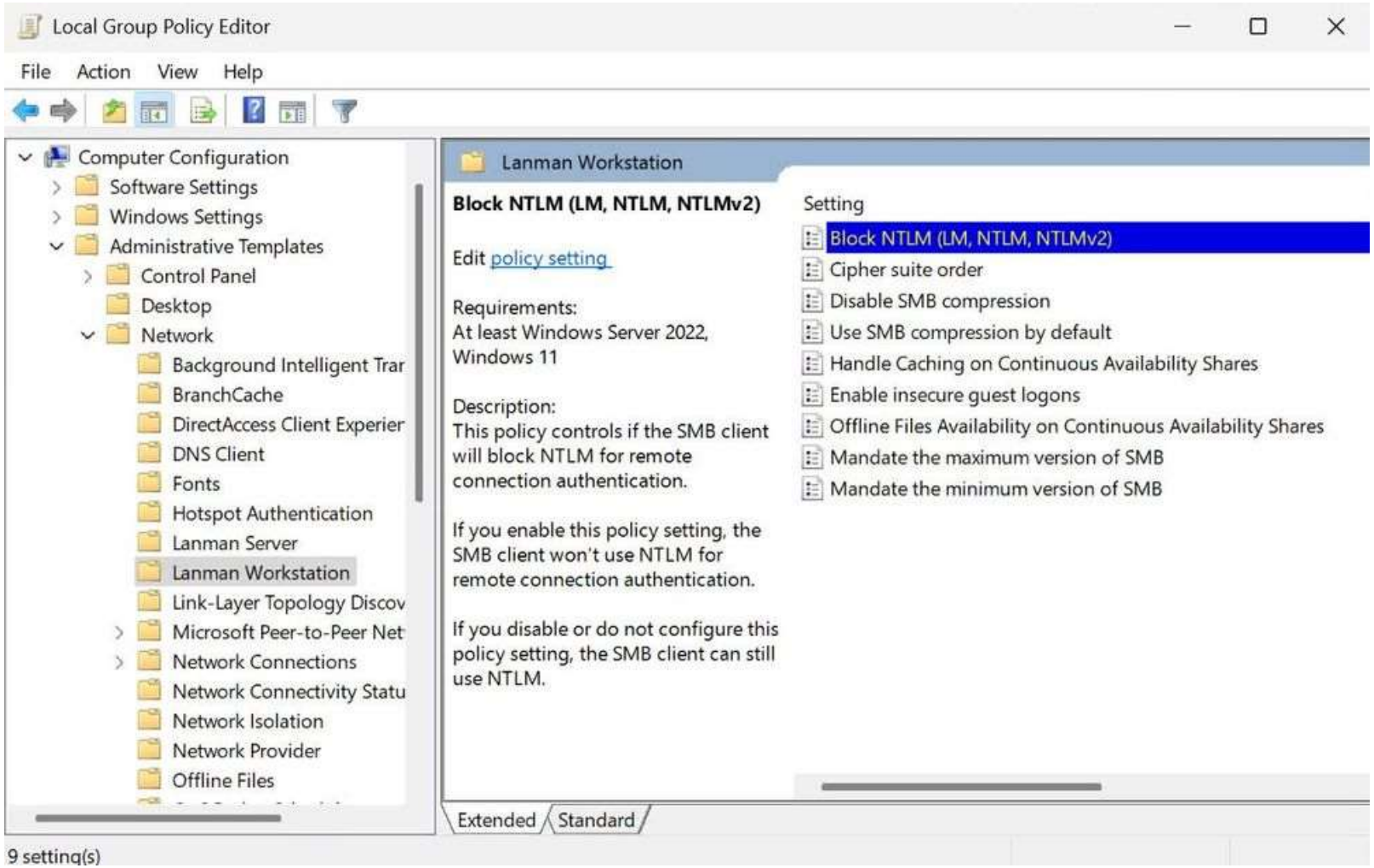
SMB Dialect Management



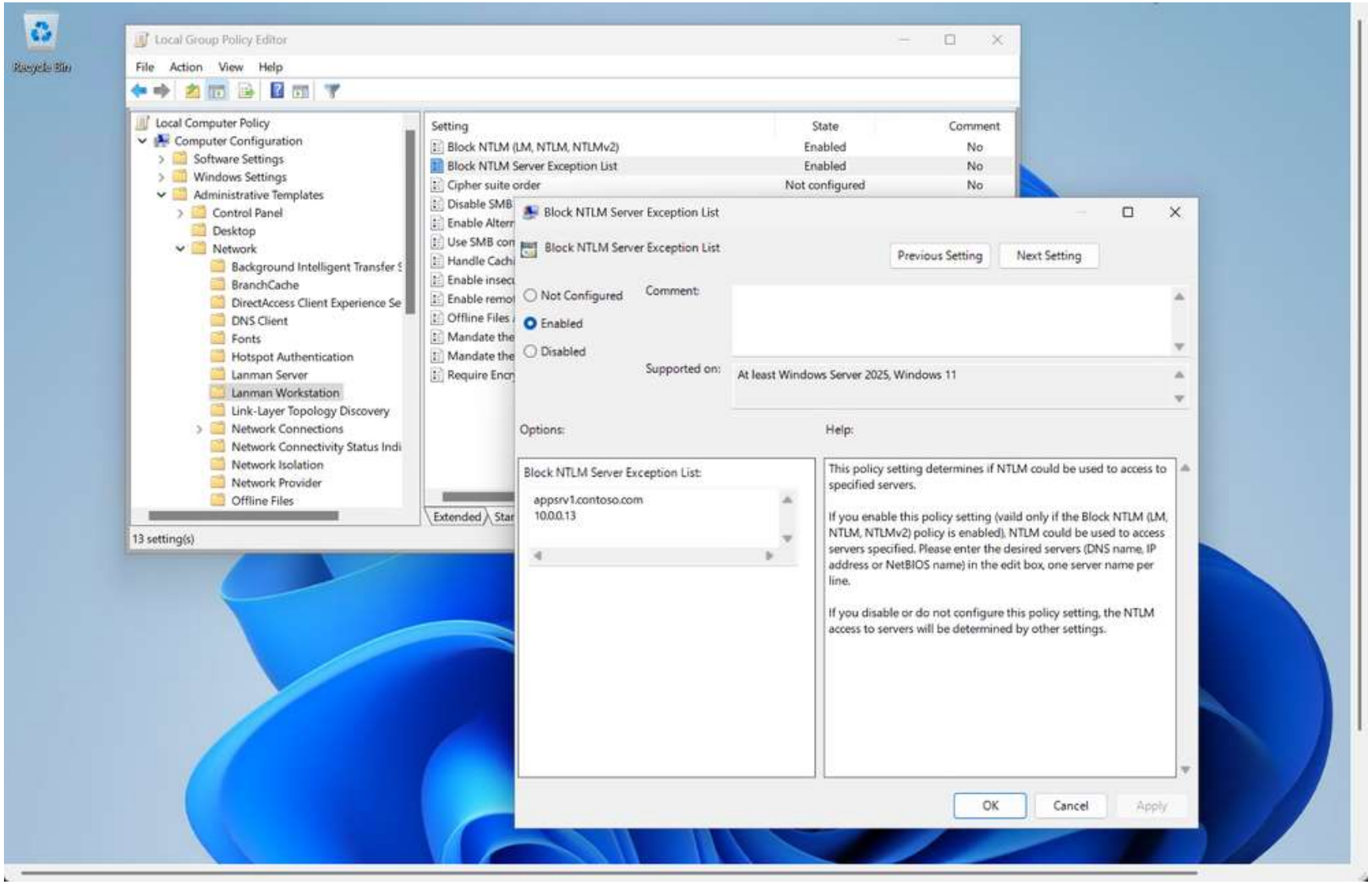
SMB Dialect Management



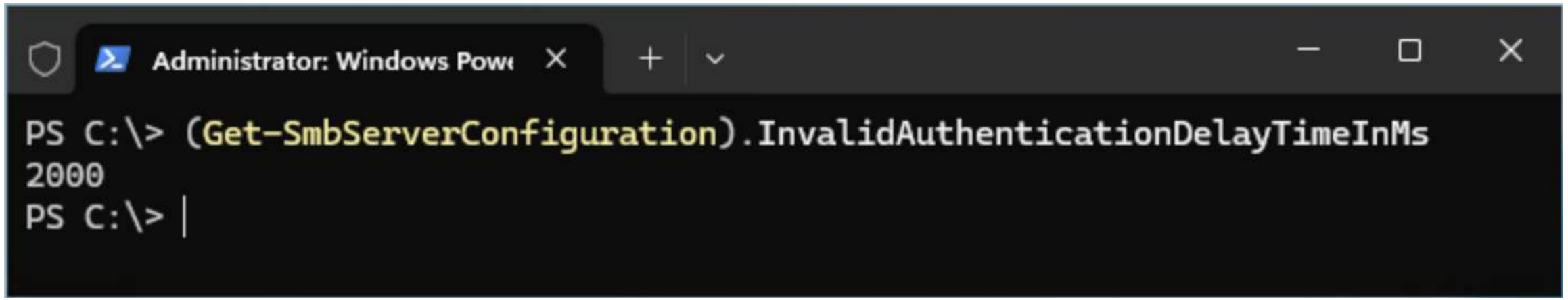
SMB Client NTLM Authentication Blocking



SMB Client NTLM Authentication Blocking



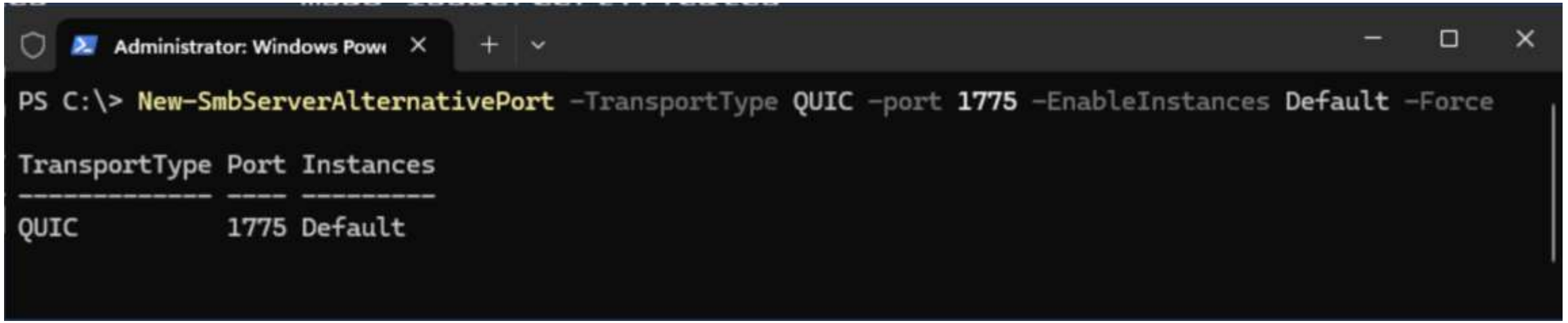
SMB Authentication Rate Limiter



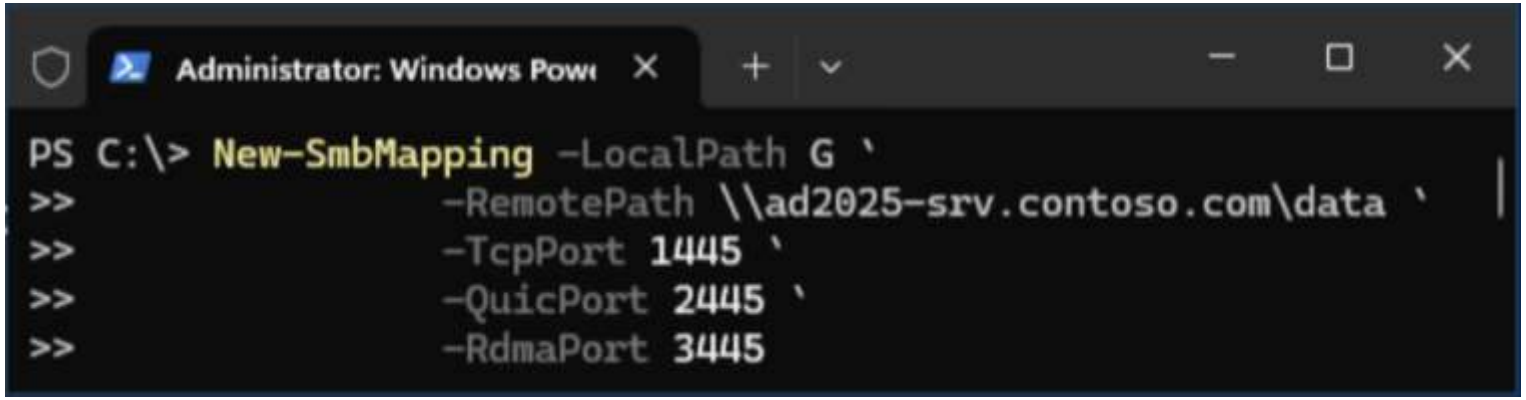
SMB Alternative Ports

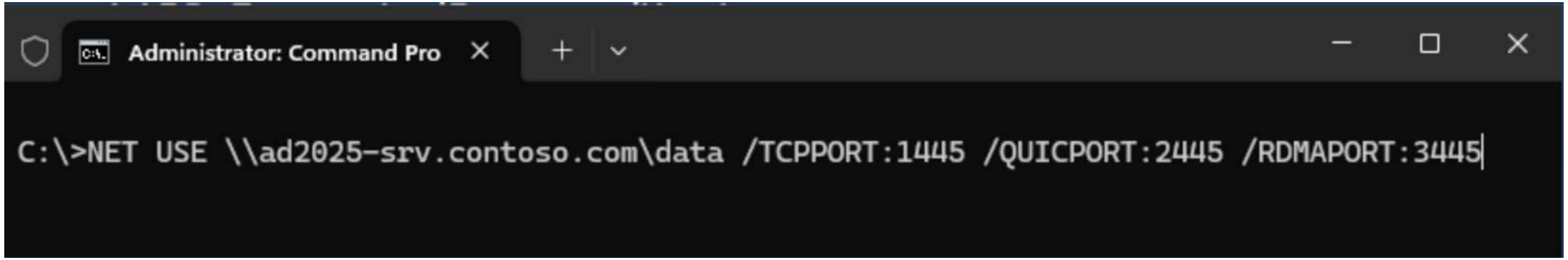
Protocol	Default Port
SMB over NetBIOS	TCP/139
SMP over IP	TCP/445
SMB over QUIC	UDP/443
SMB Direct (RDMA)	TCP/5445

SMB Alternative Ports

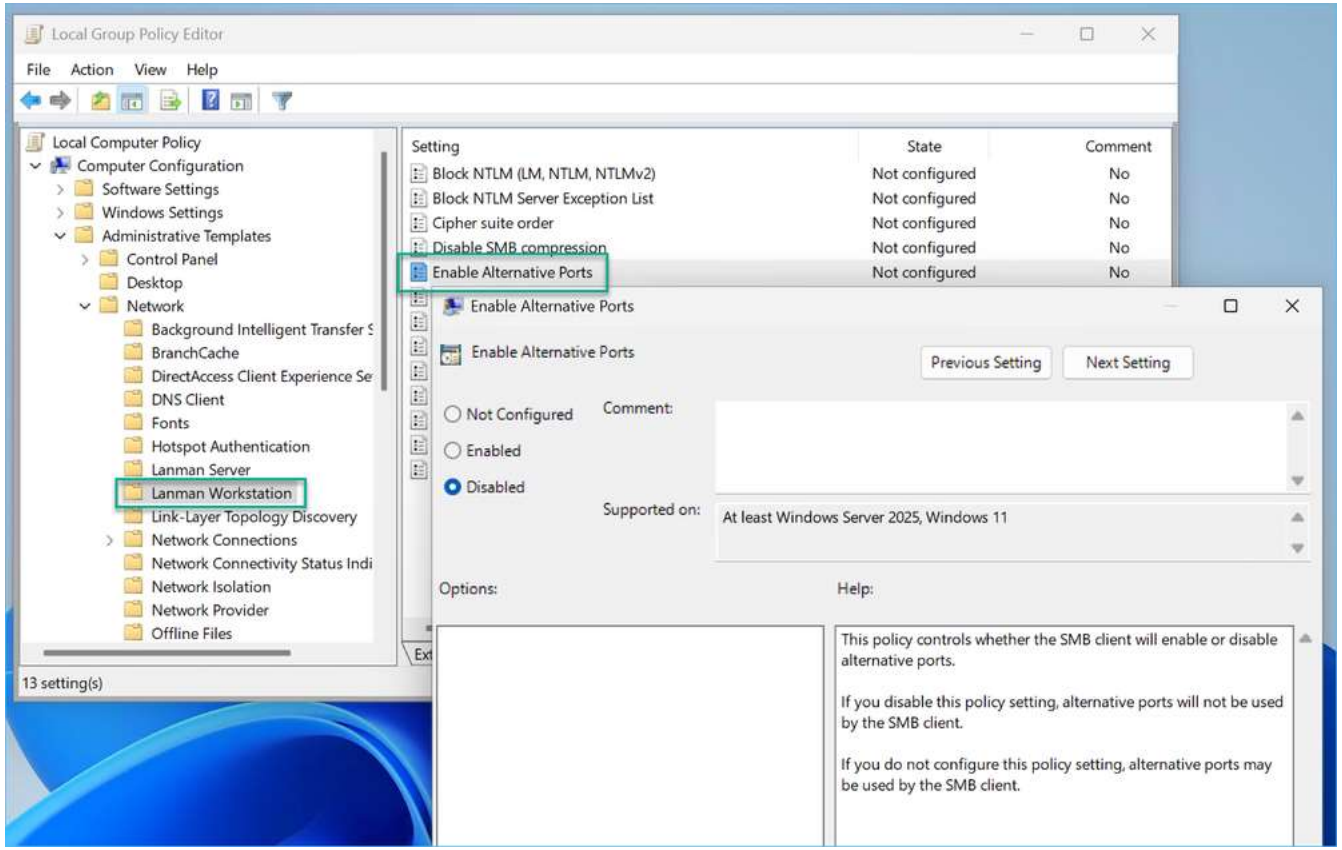


SMB Alternative Ports

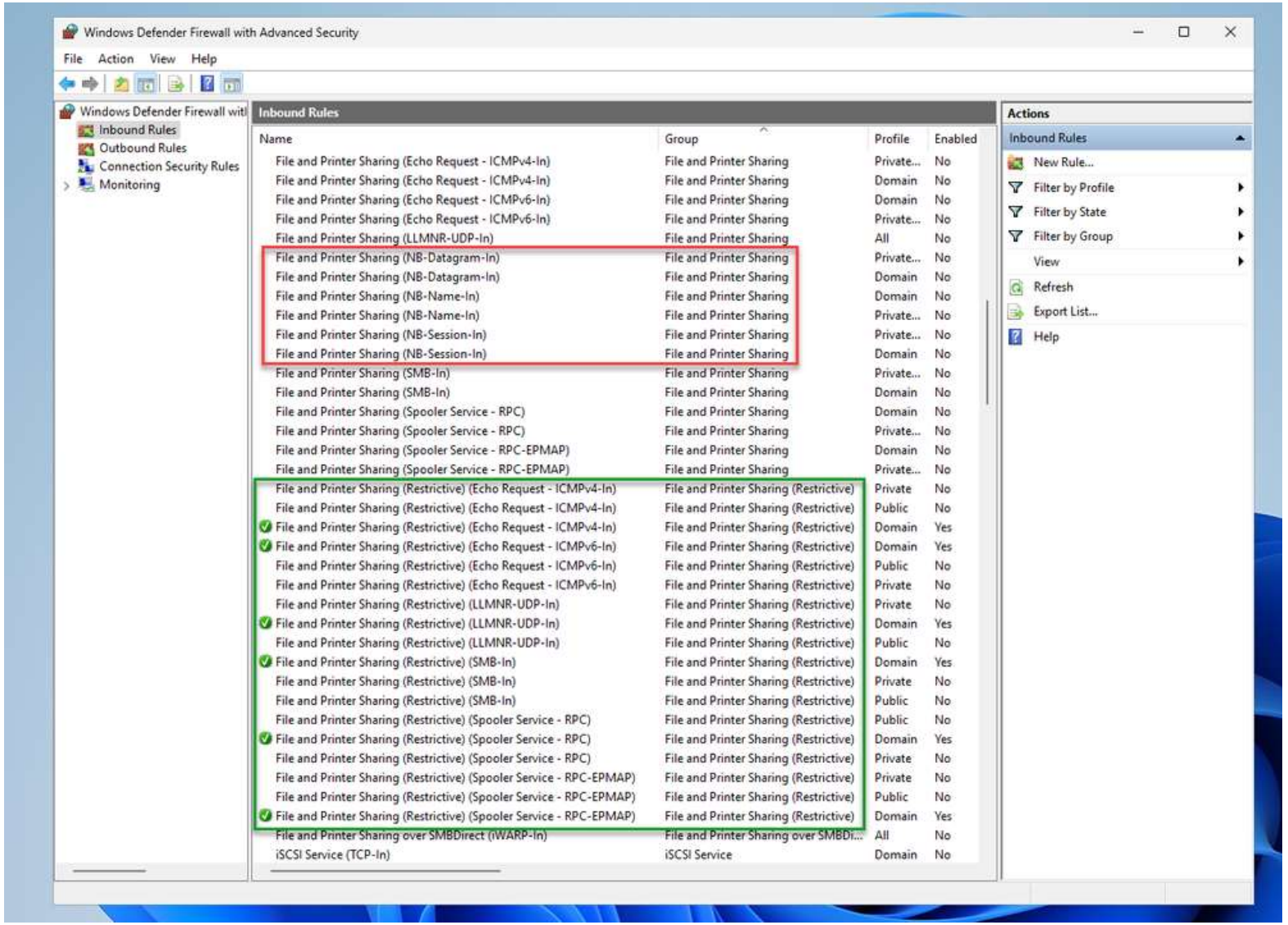




SMB Alternative Ports



File and Printer Sharing (Restrictive) FW Rules



Legacy SAM RPC Password Change Behavior

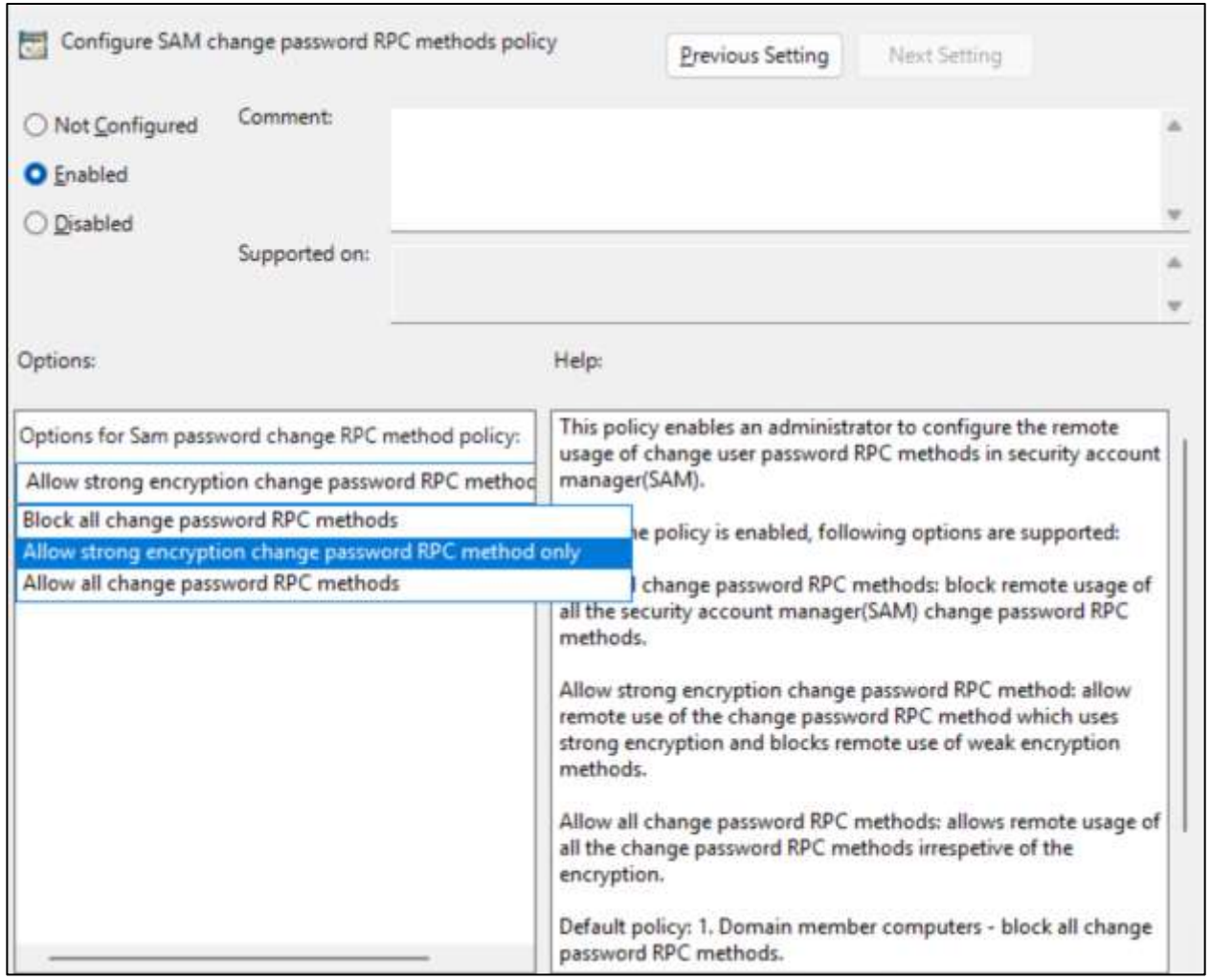
Remotely blocked RPC calls (DES-ECB-LM):

- SamrChangePasswordUser
- SamrOemChangePasswordUser2
- SamrUnicodeChangePasswordUser2

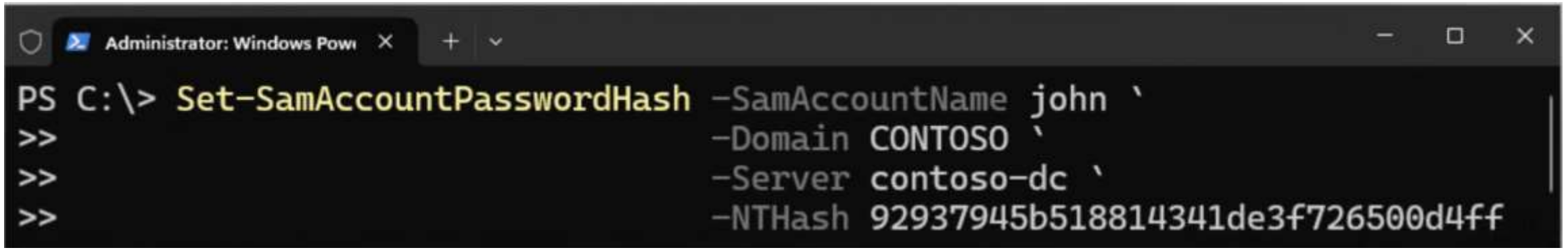
Members of the Protected Users group:

- SamrUnicodeChangePasswordUser4

Legacy SAM RPC Password Change Behavior



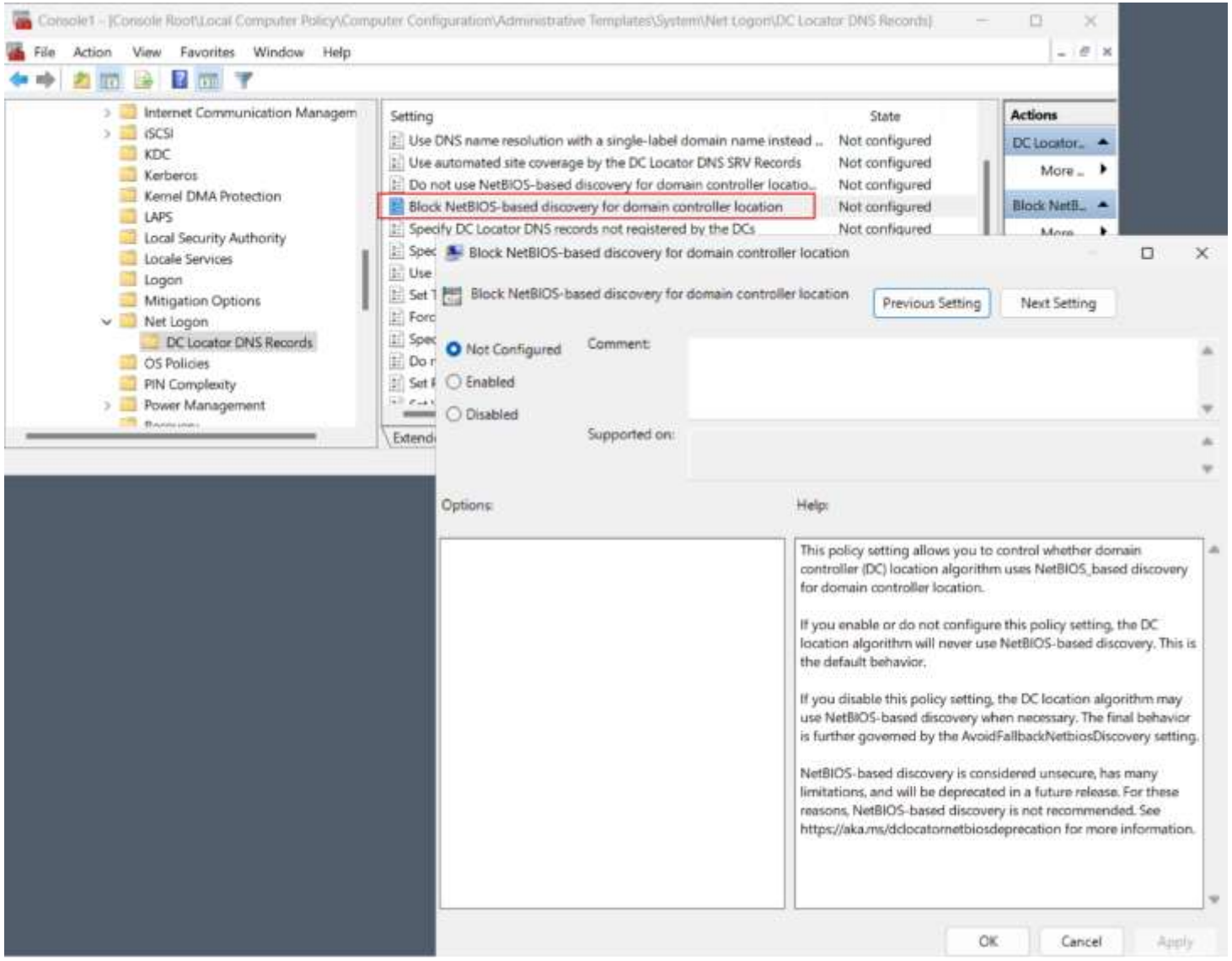
Legacy SAM RPC Password Change Behavior



SamrSetInformationUser(SAMPR_USER_INTERNAL1_INFORMATION)

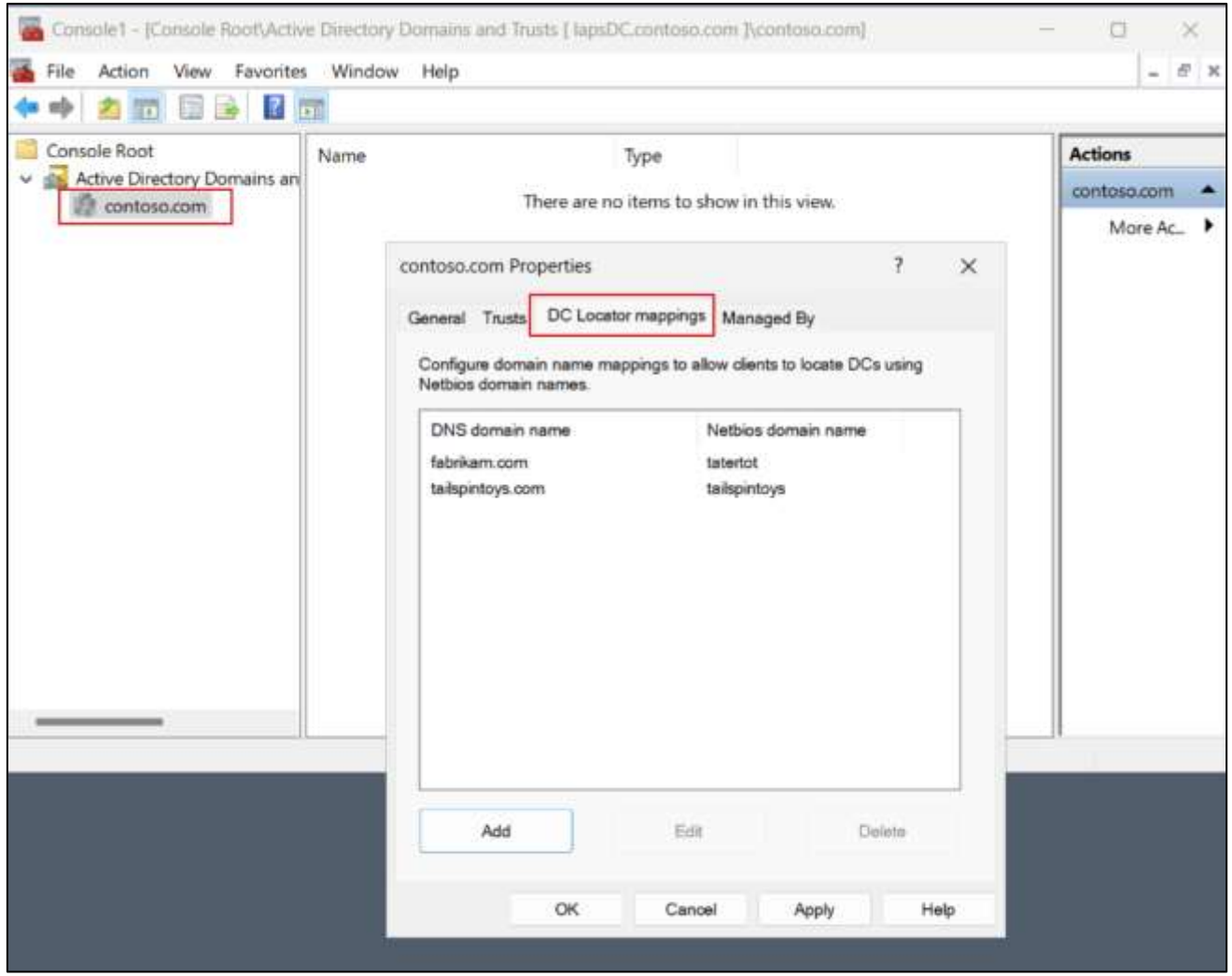
DC Locator NetBIOS Deprecation

DC Locator NetBIOS Deprecation

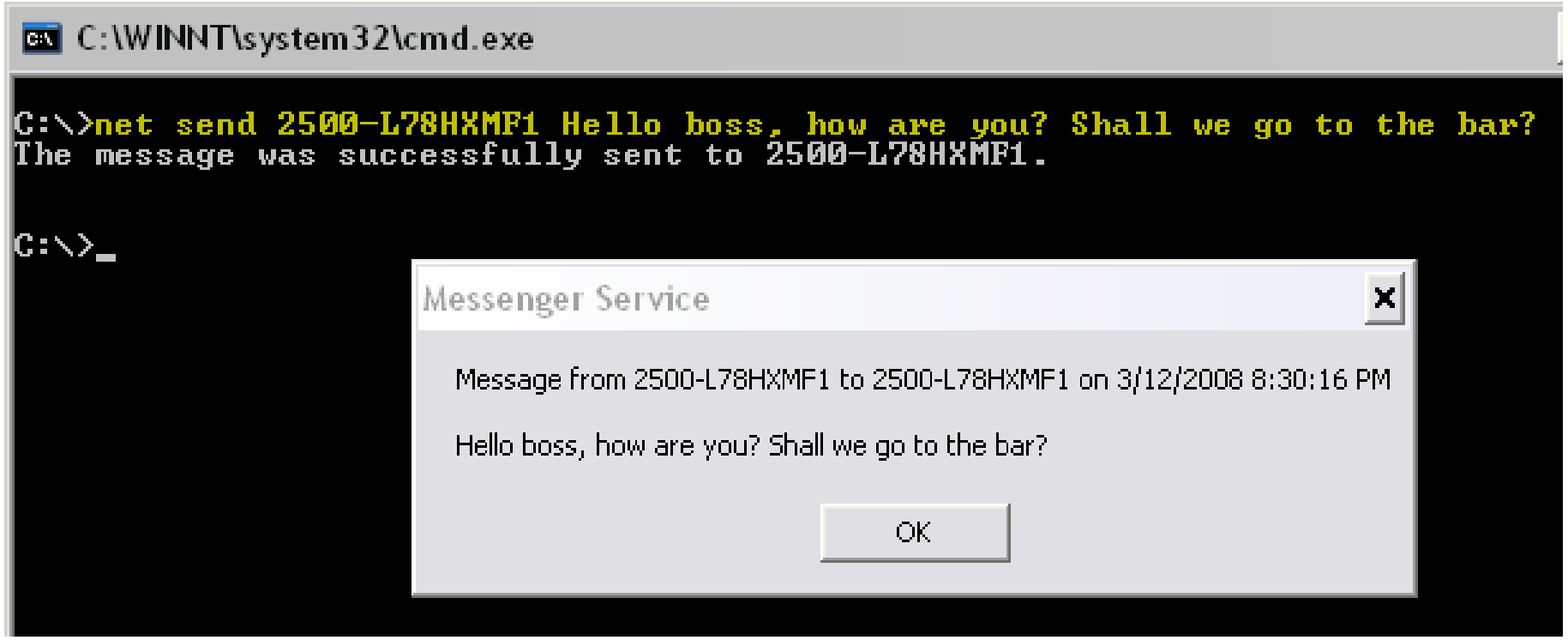


DC Locator NetBIOS Deprecation

DC Locator NetBIOS Deprecation



Deprecation of WINS and Remote Mailslots

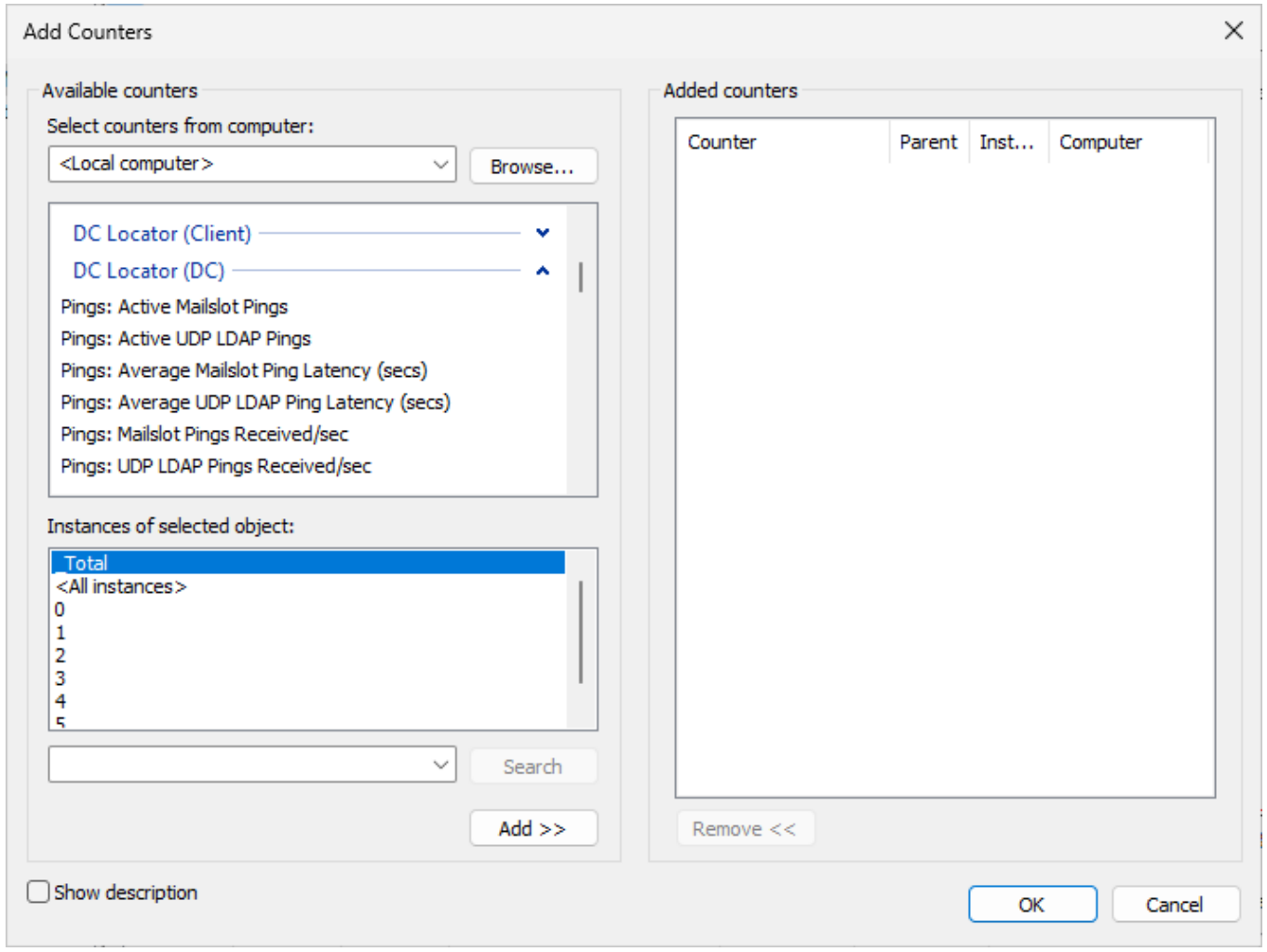


Set-SmbClientConfiguration -EnableMailslots $true

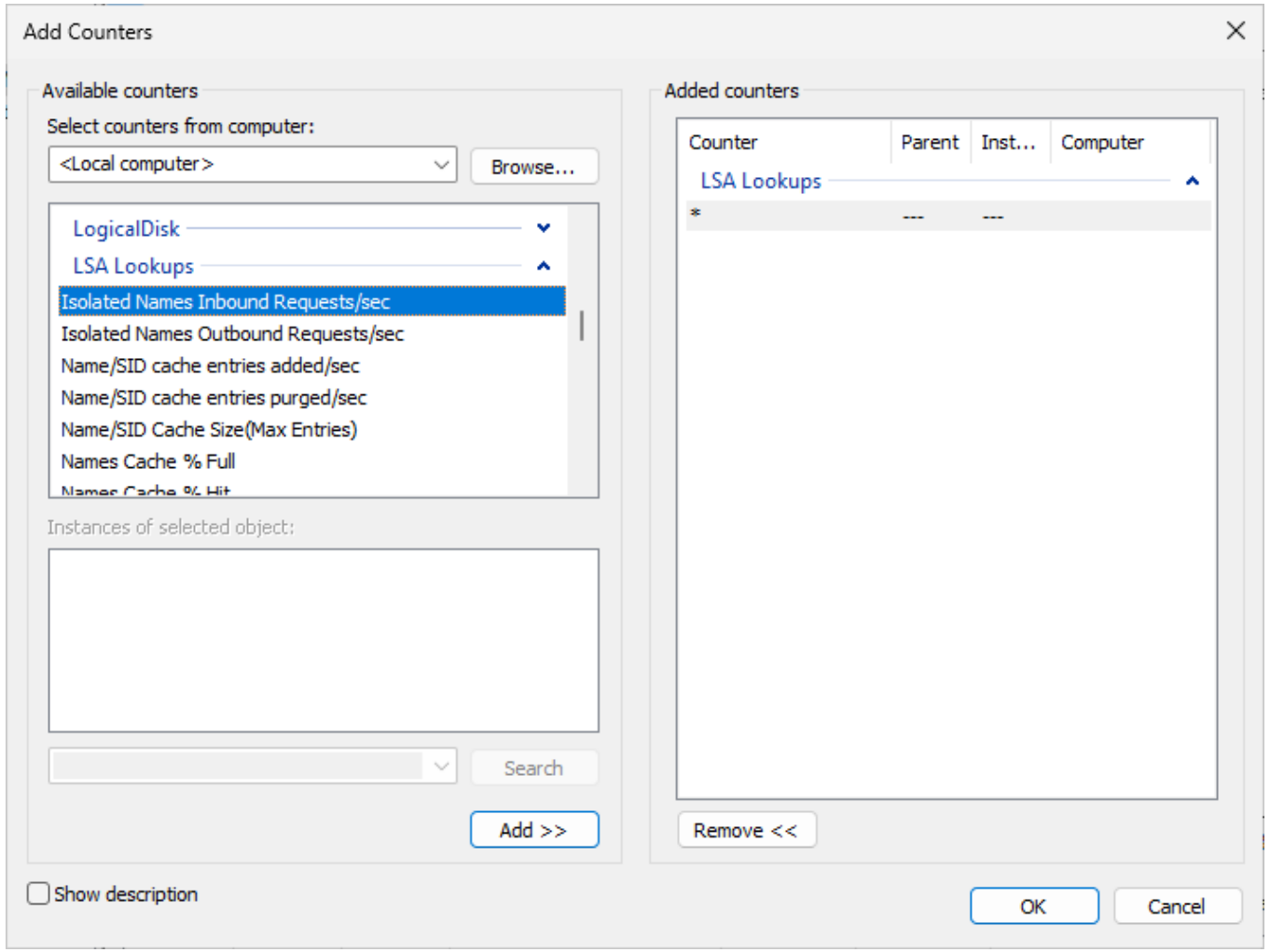
Replication Priority Order

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.

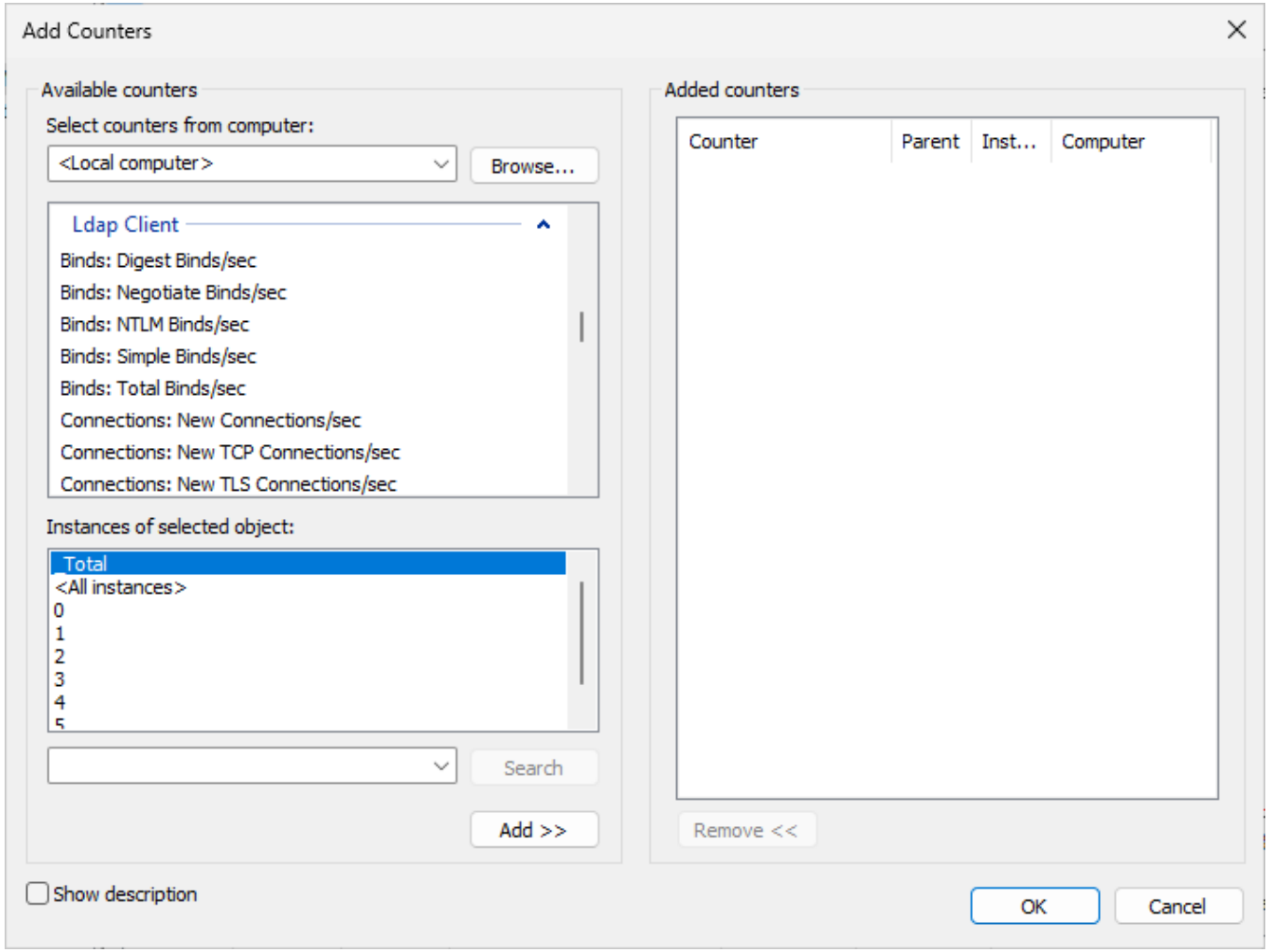
DC Locator Performance Counters



LSA Lookups Performance Counters



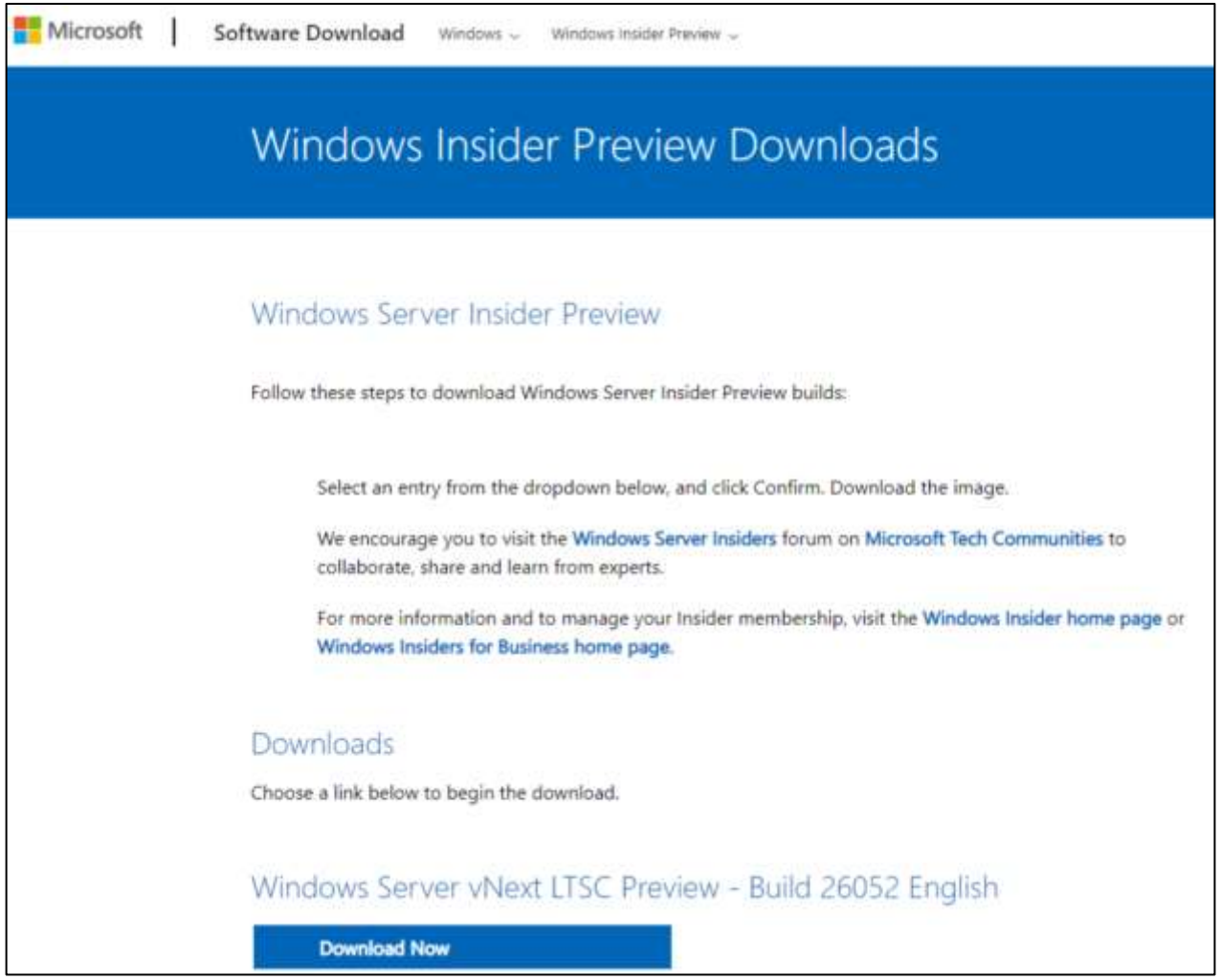
LDAP Client Performance Counters (WS2022+)



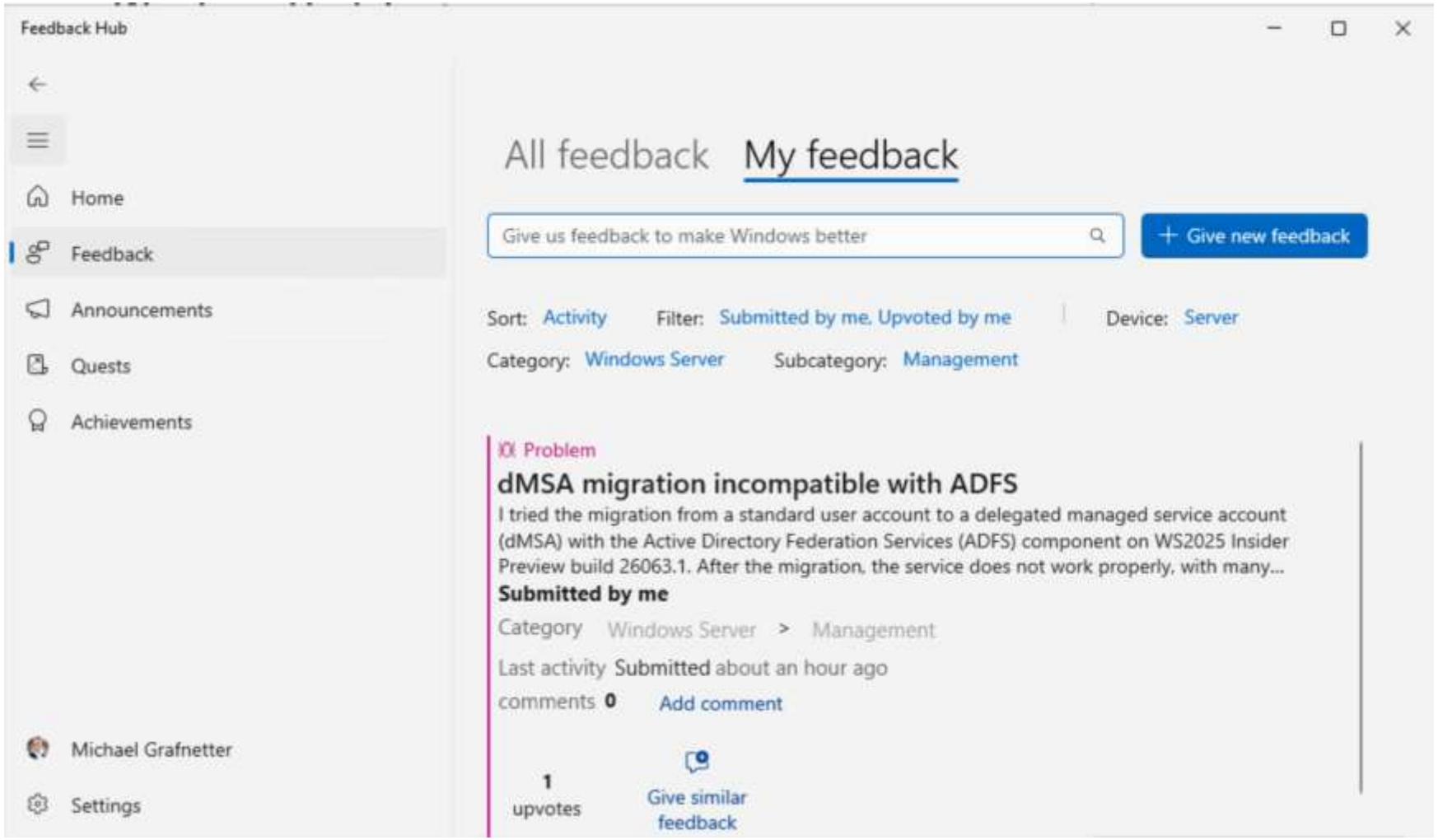
Summary: New AD and Security Features

- 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


Microsoft | Software Download Windows Windows Insider Preview
Windows Insider Preview Downloads
Windows Server Insider Preview
Follow these steps to download Windows Server Insider Preview builds:
Select an entry from the dropdown below, and click Confirm. Download the image.
We encourage you to visit the Windows Server Insiders forum on Microsoft Tech Communities to collaborate, share and learn from experts.
For more information and to manage your Insider membership, visit the Windows Insider home page or Windows Insiders for Business home page.
Downloads
Choose a link below to begin the download.
Windows Server vNext LTSC Preview - Build 26052 English
Download Now

Give 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