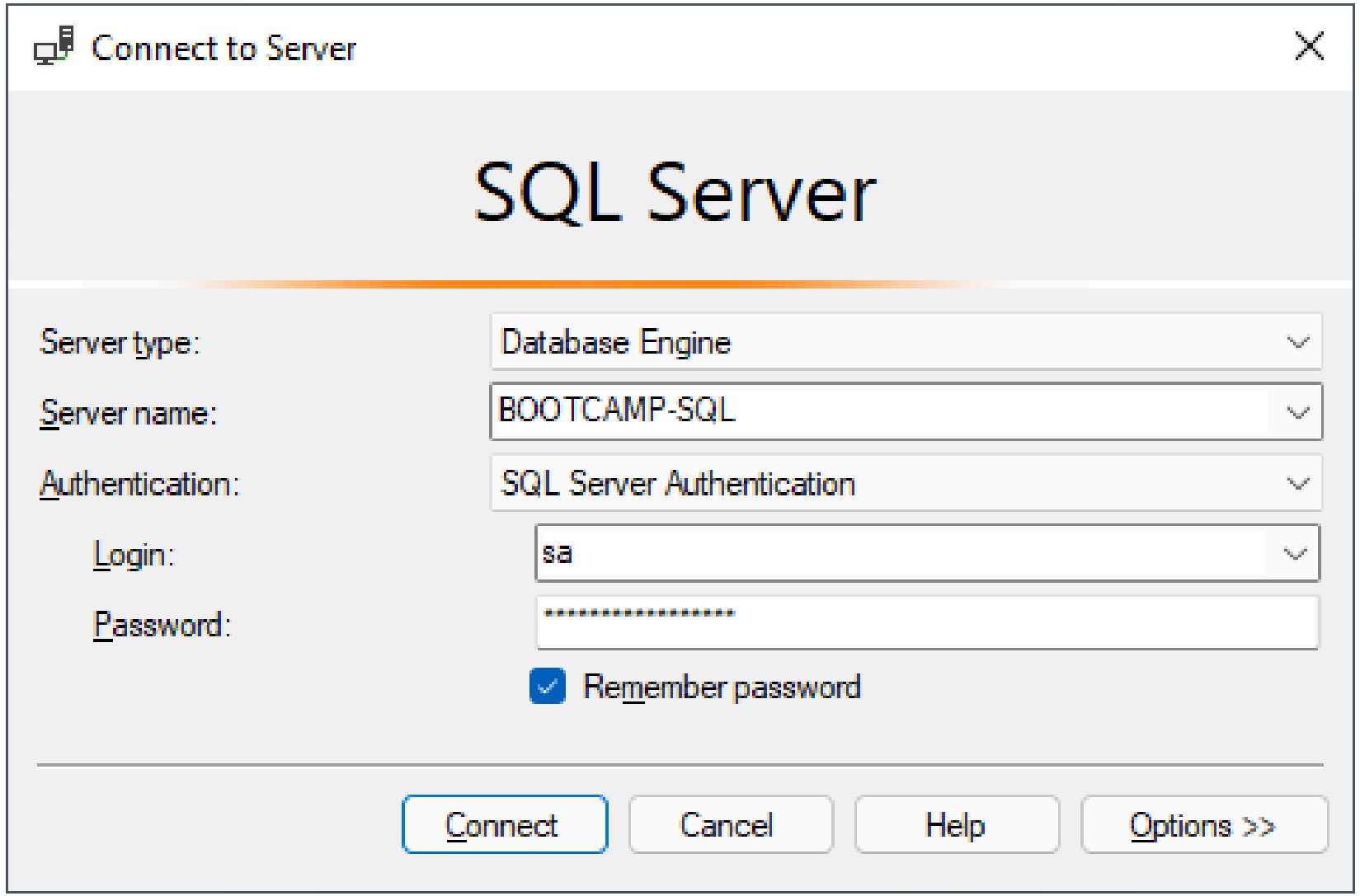
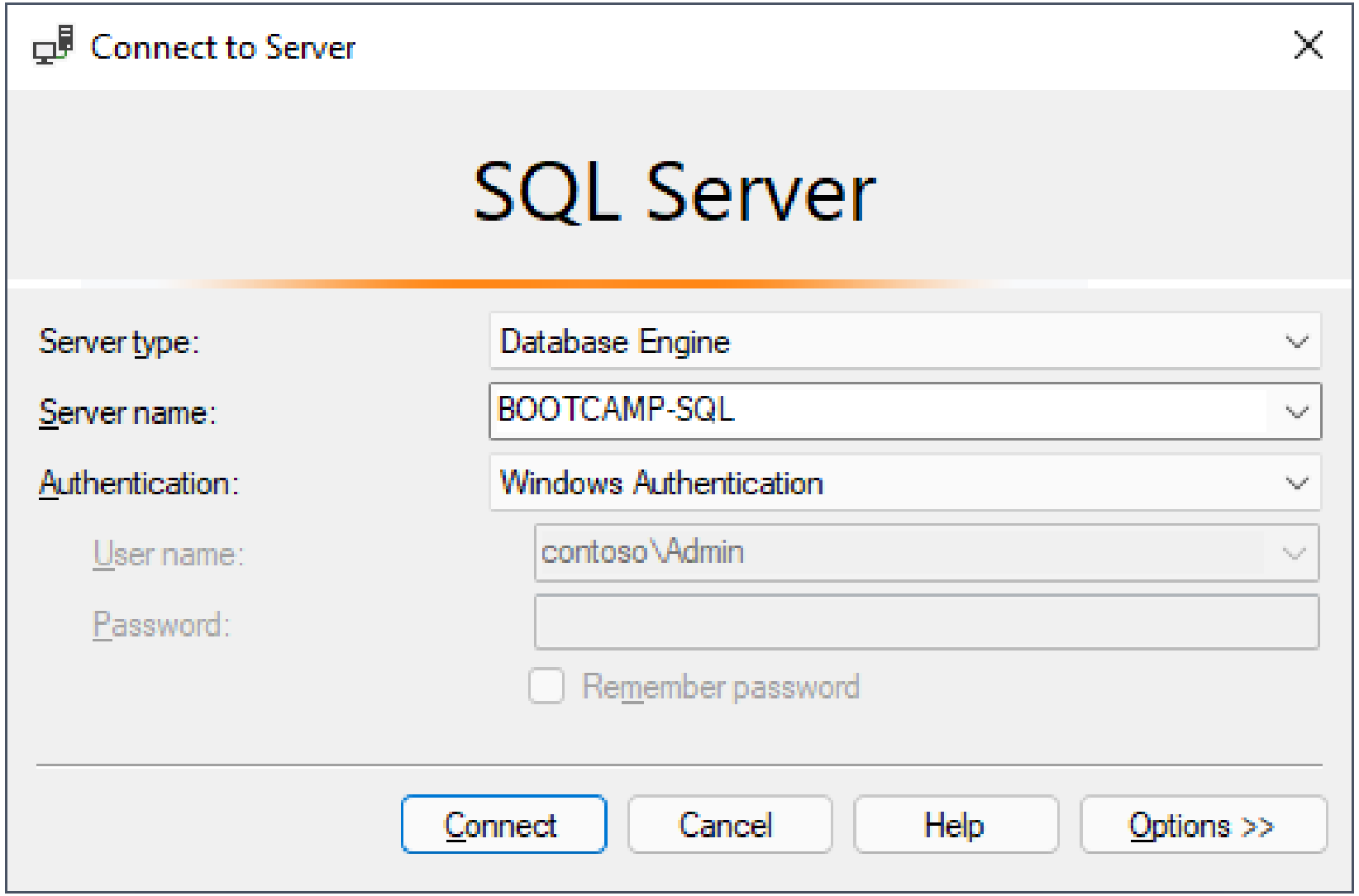
SQL Server
Windows Authentication Internals

Mgr. Michael Grafnetter
MVP | MCT
michael.grafnetter@outlook.com
@MGrafnetter

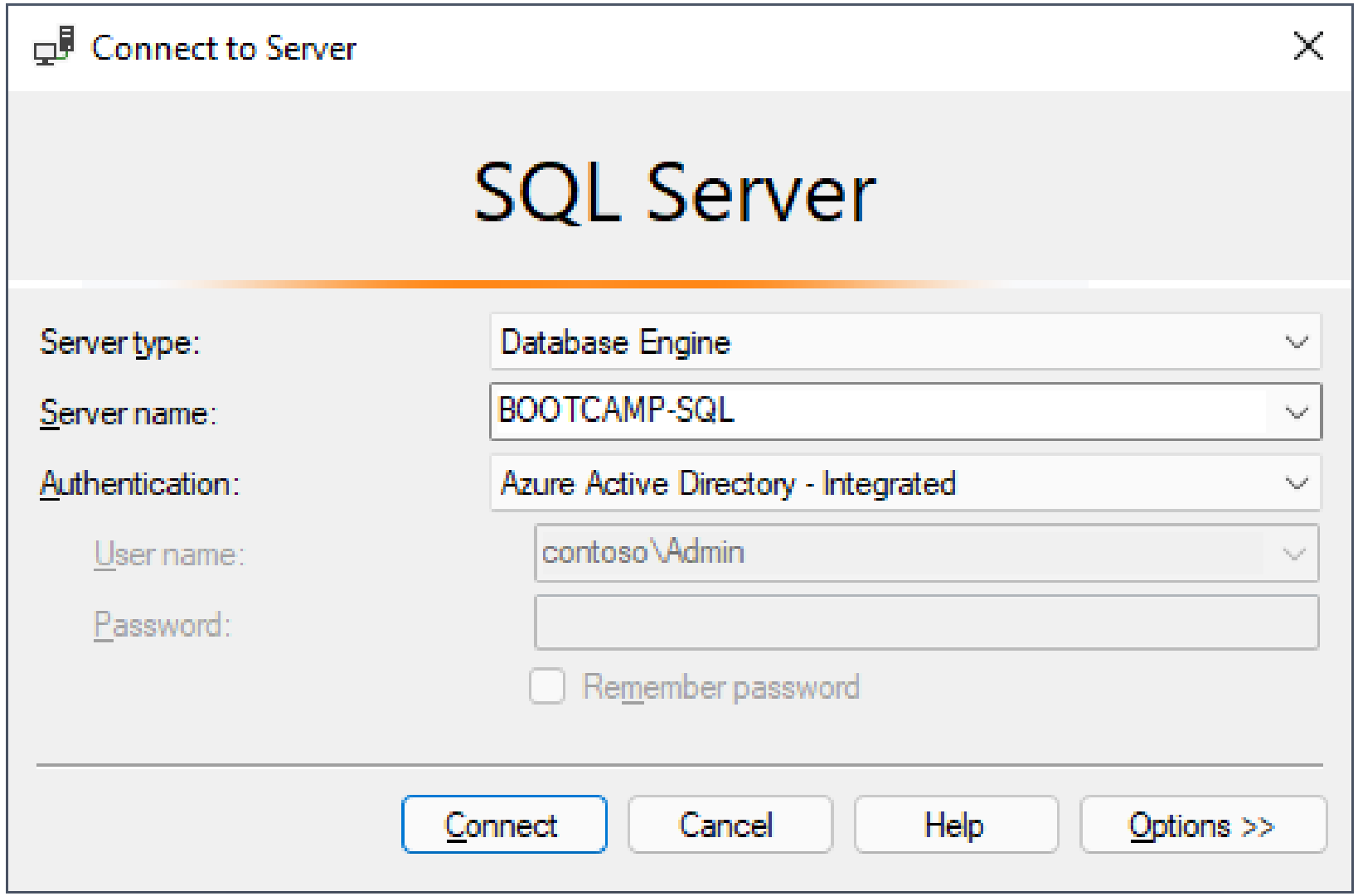
SQL Server Authentication – Out of Scope



Windows Integrated Authentication – Our Scope



AAD Integrated Authentication – Out of Scope

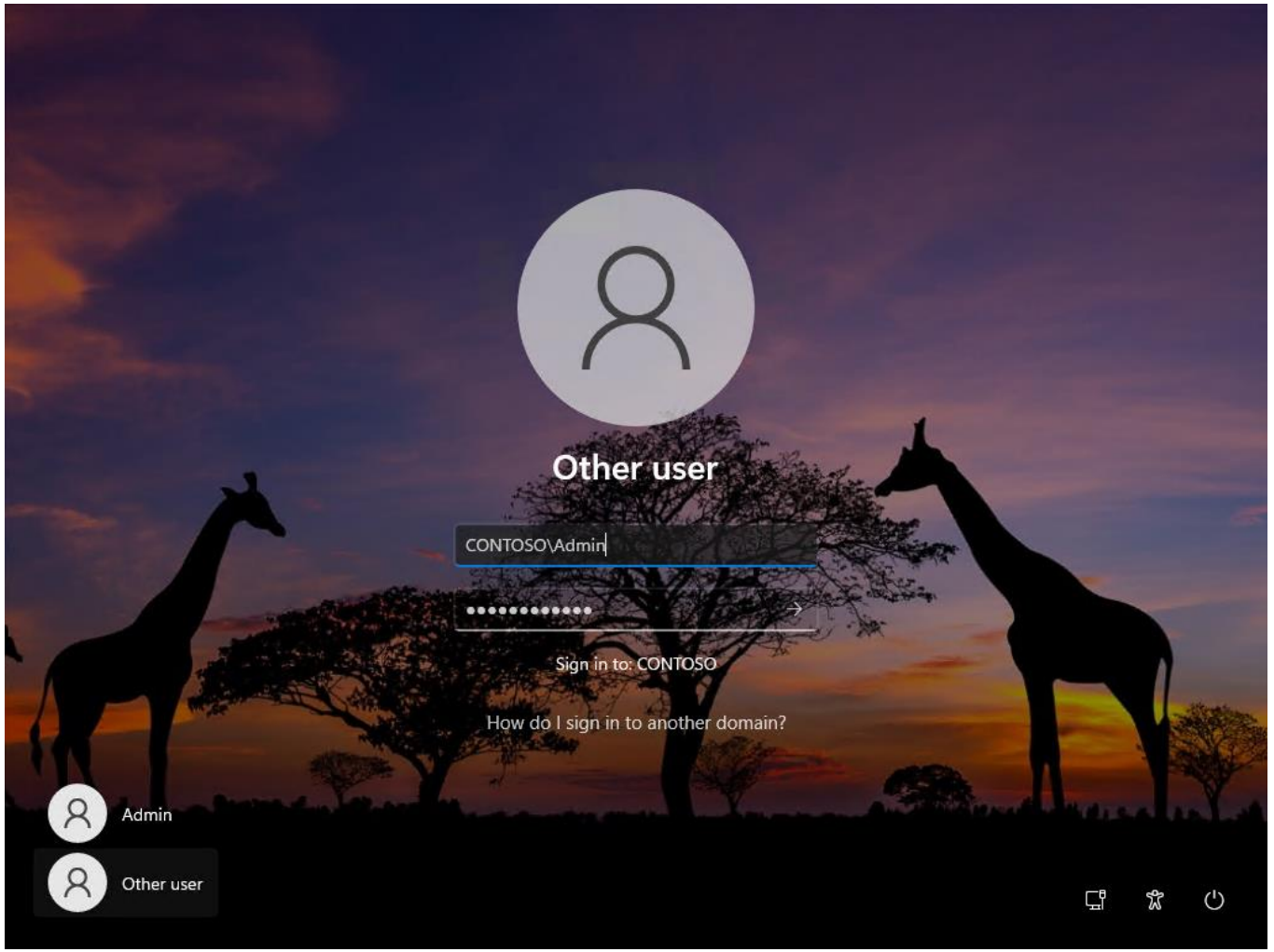


Agenda

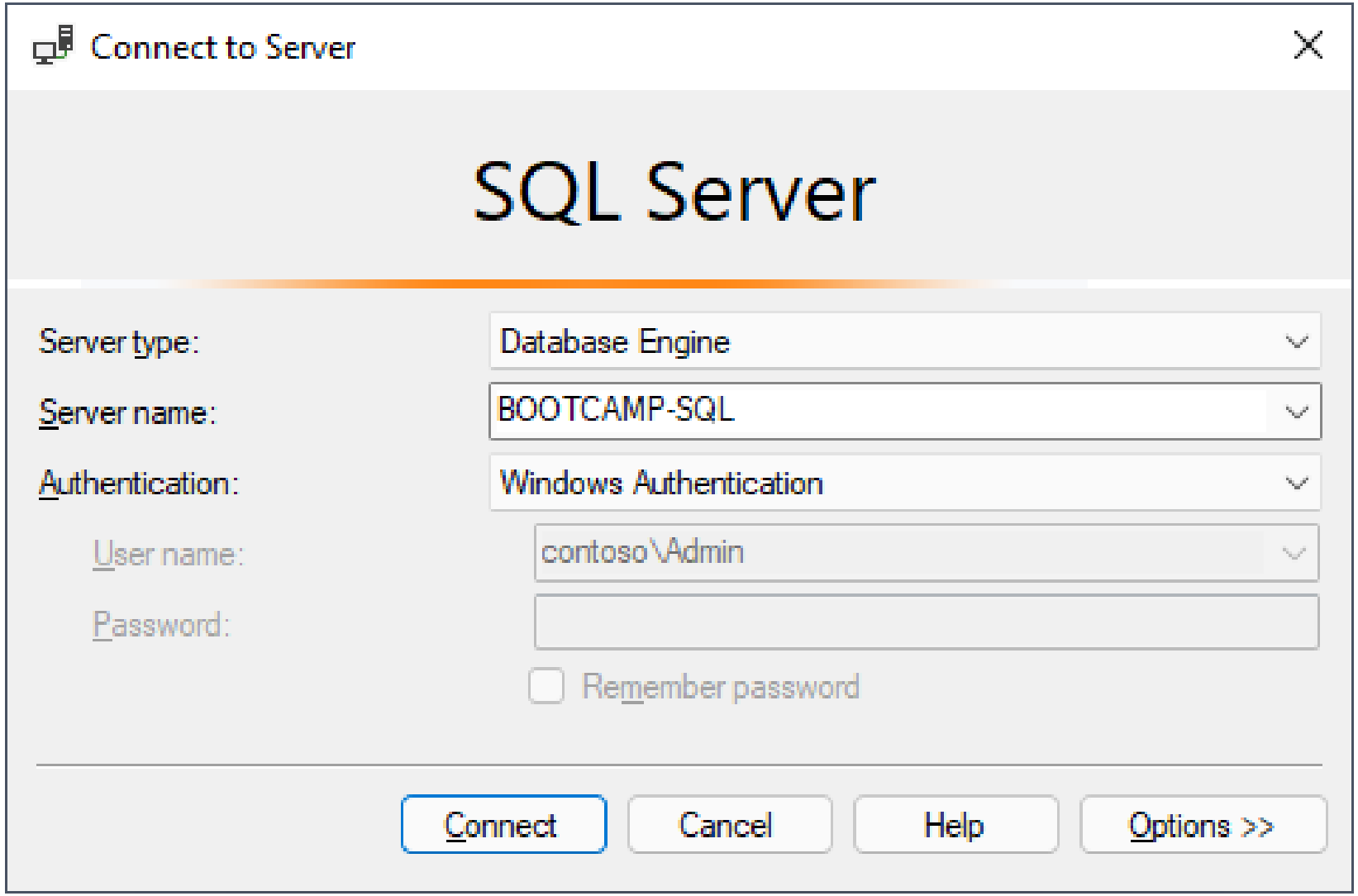
- Windows Integrated Authentication Overview
- WIA Under the Hood
  - NTLM
  - Kerberos (Security Best Practices, Delegation)
- SQL Server Identity
  - Built-In Identities
  - Service Accounts
  - Group Managed Service Accounts
- Common Misconfigurations and Attacks
  - SQL Server MITM
  - NTLM Relay
  - Dumping LSA Secrets
  - Kerberoasting

WIA Overview

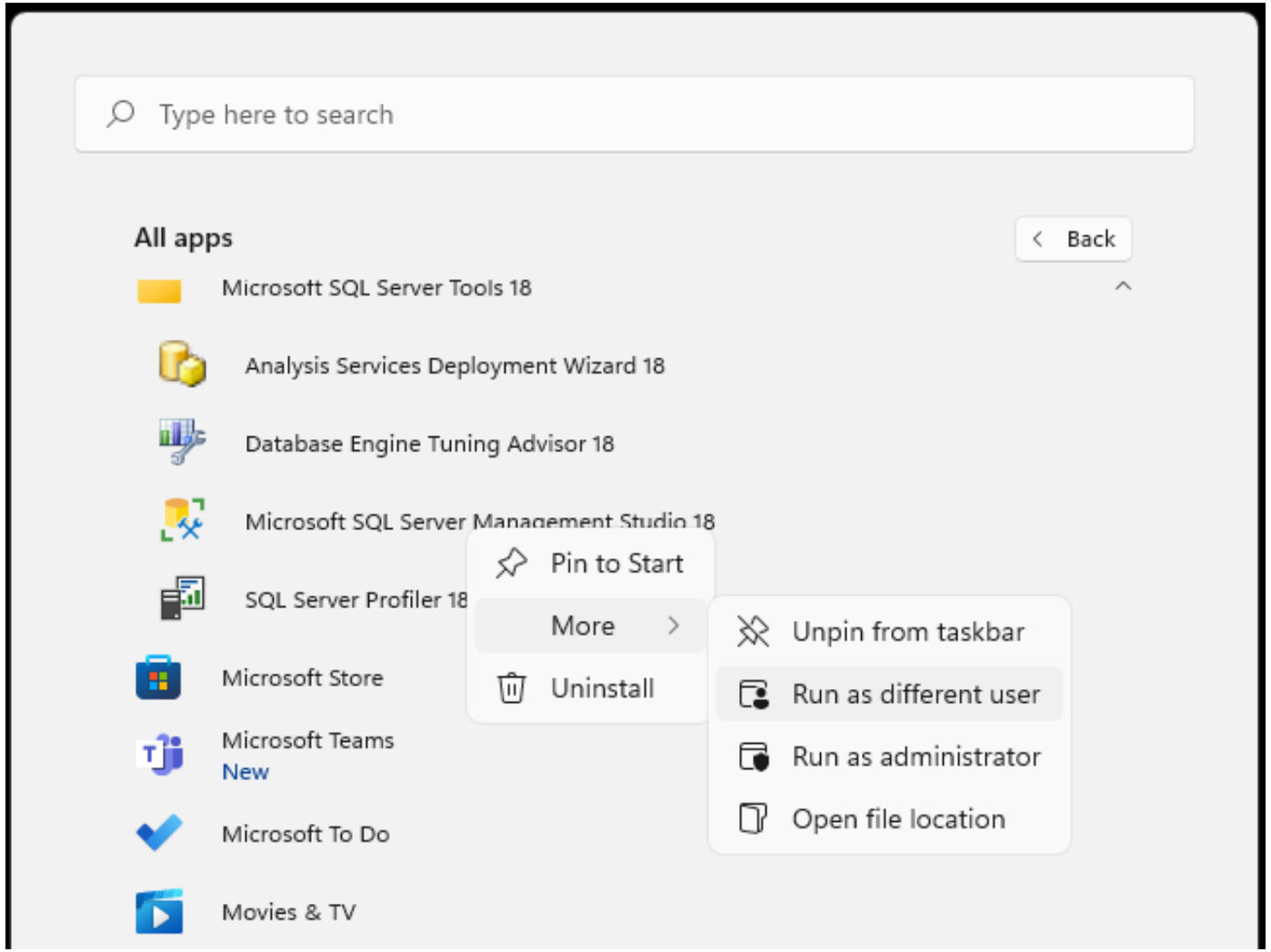
Windows Logon



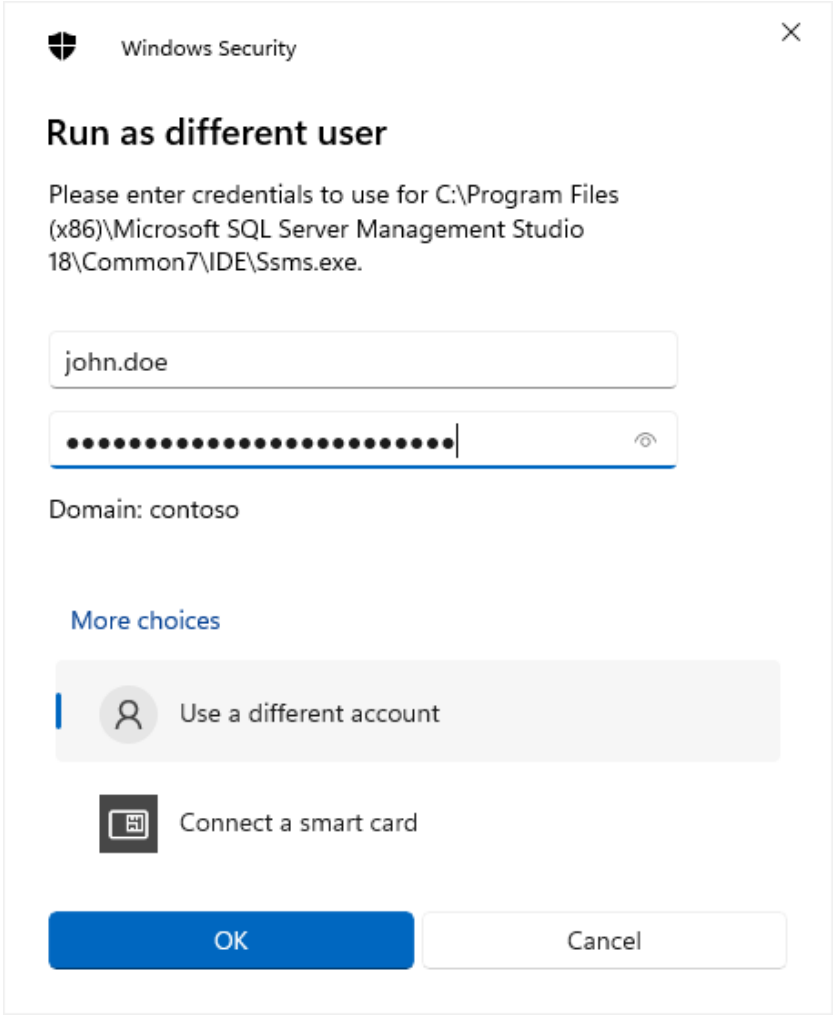
Single Sign-On (SSO)



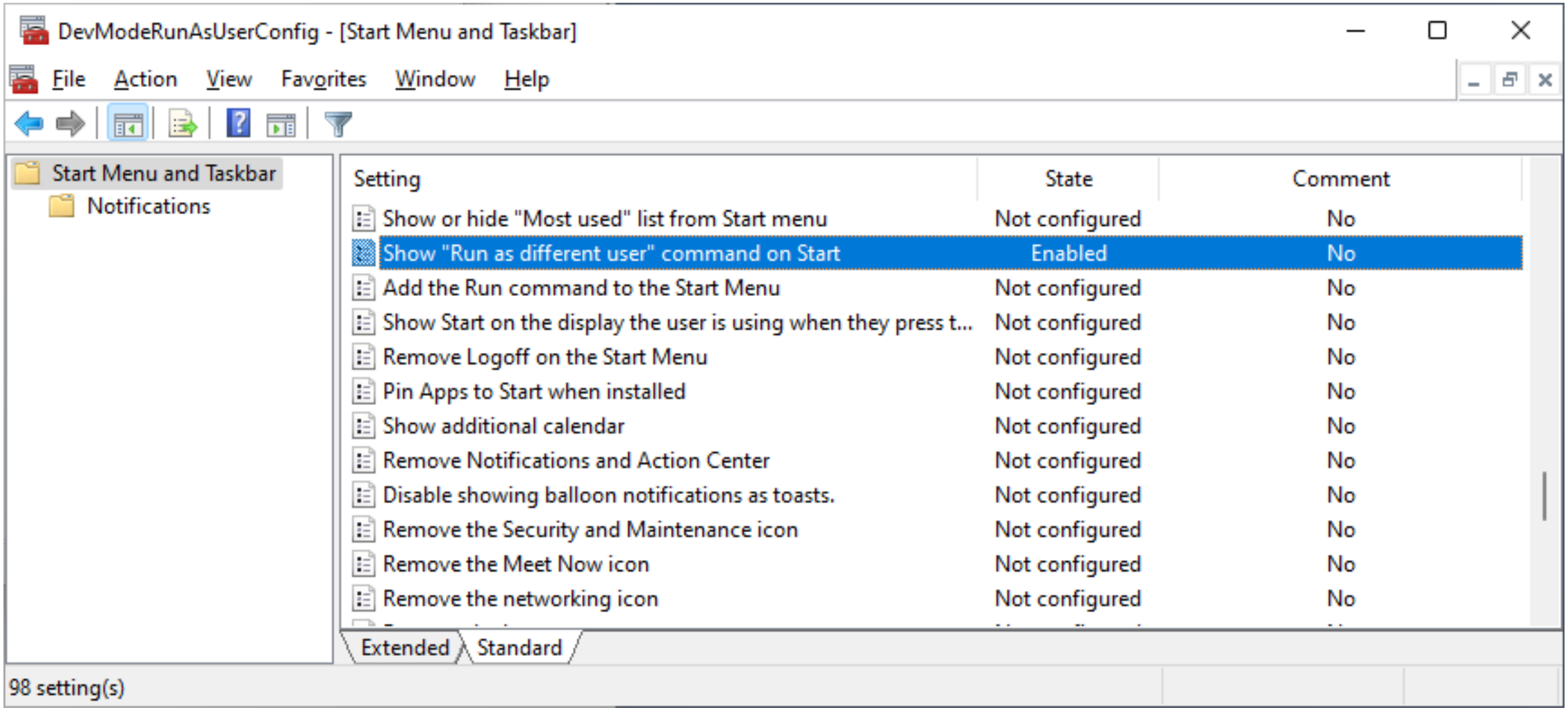
Run as Different User



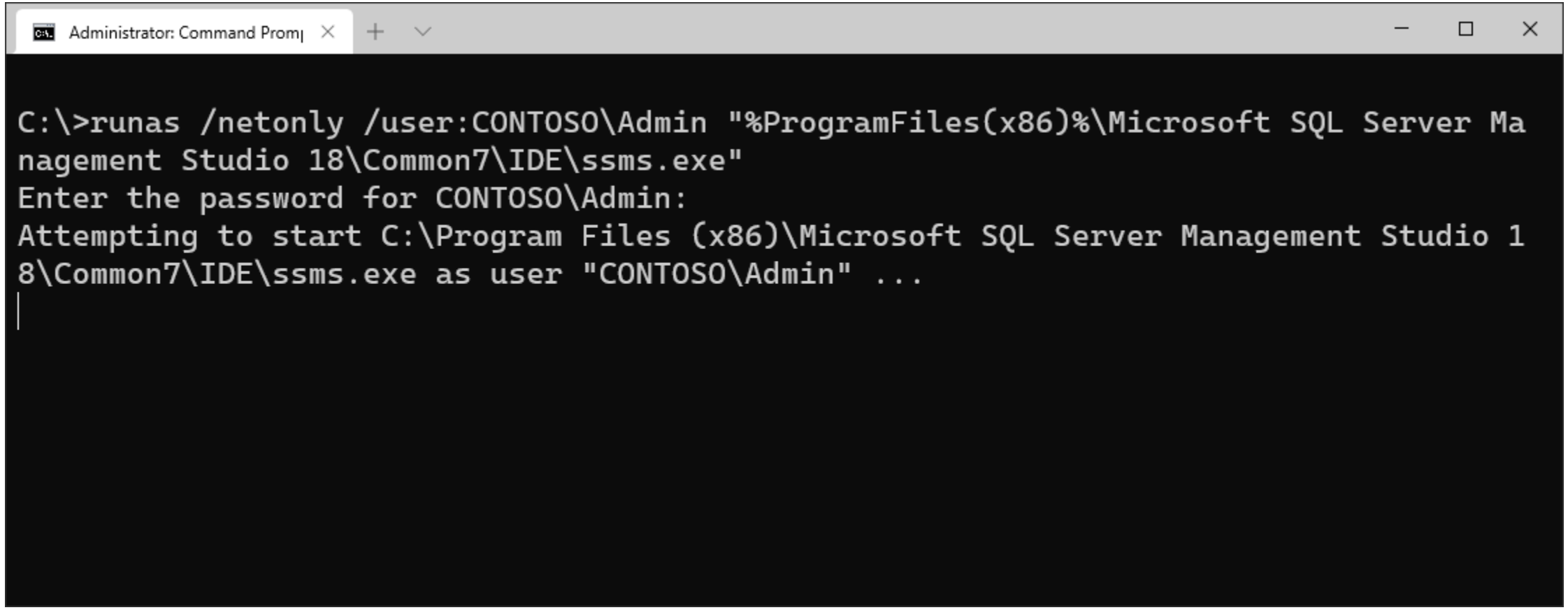
Run as Different User



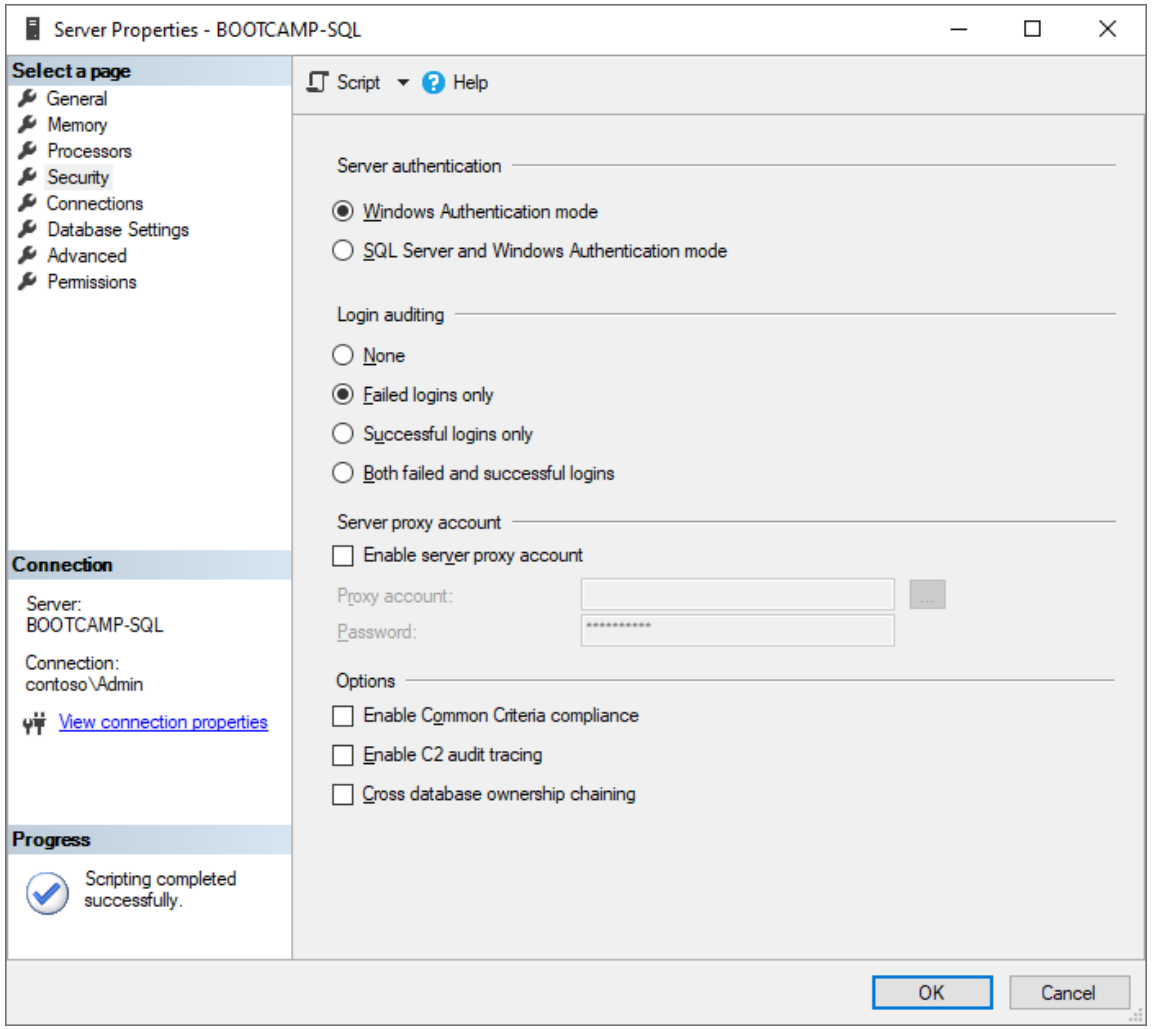
Run as Different User



Run as Different User – Network Only

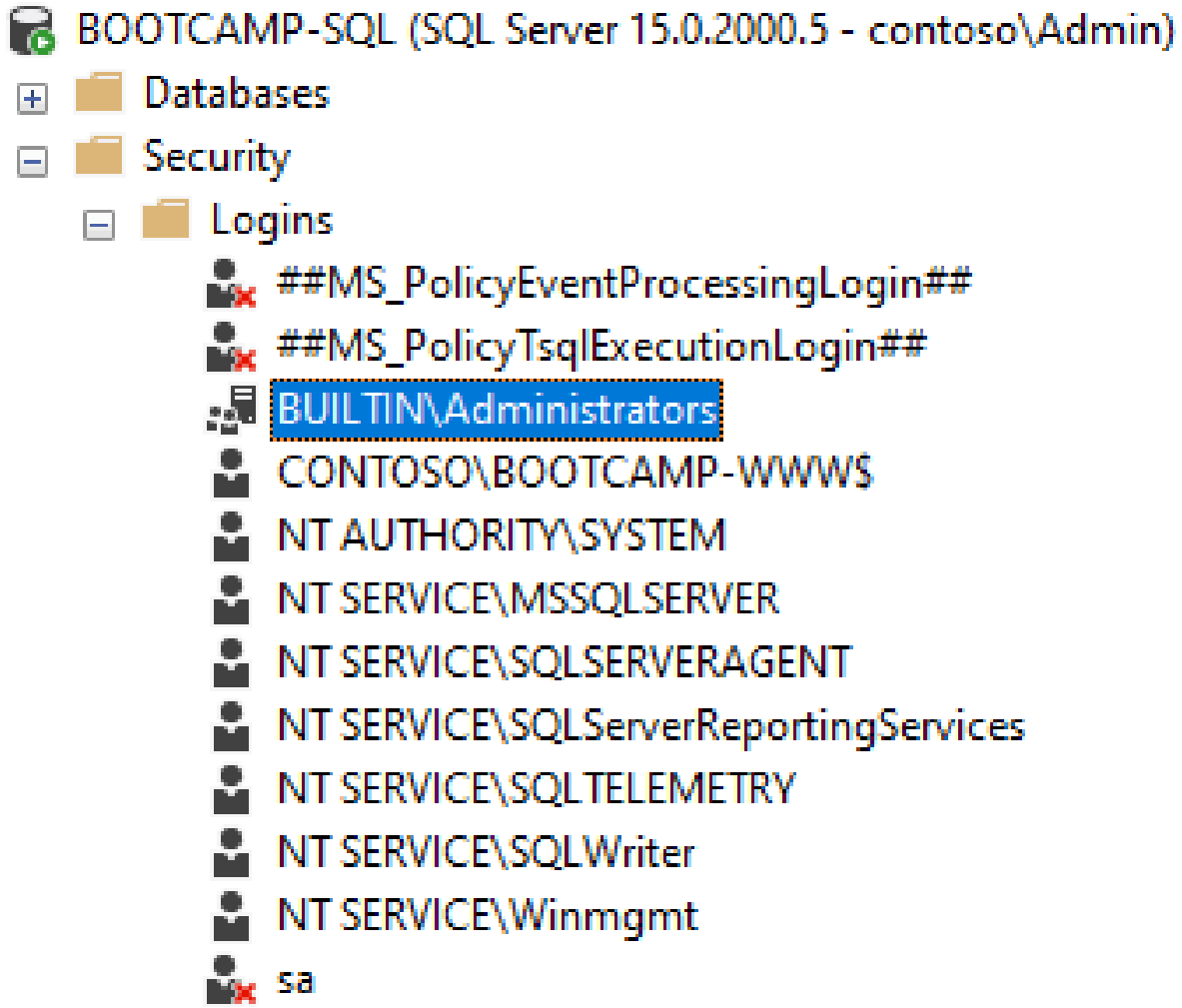


Server Authentication Mode

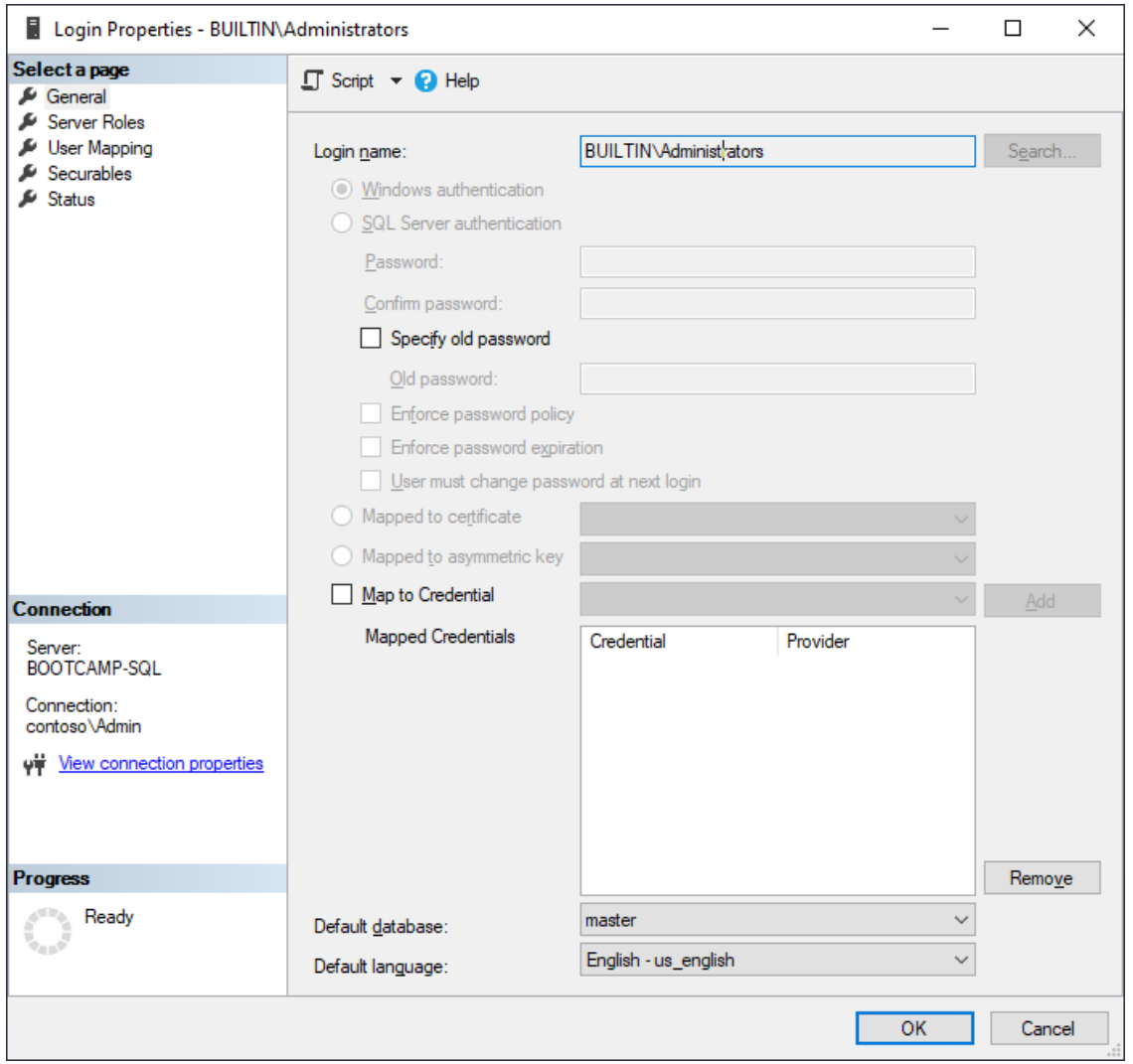



```
USE [master]
GO
EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'LoginMode', REG_DWORD, 1
GO
```

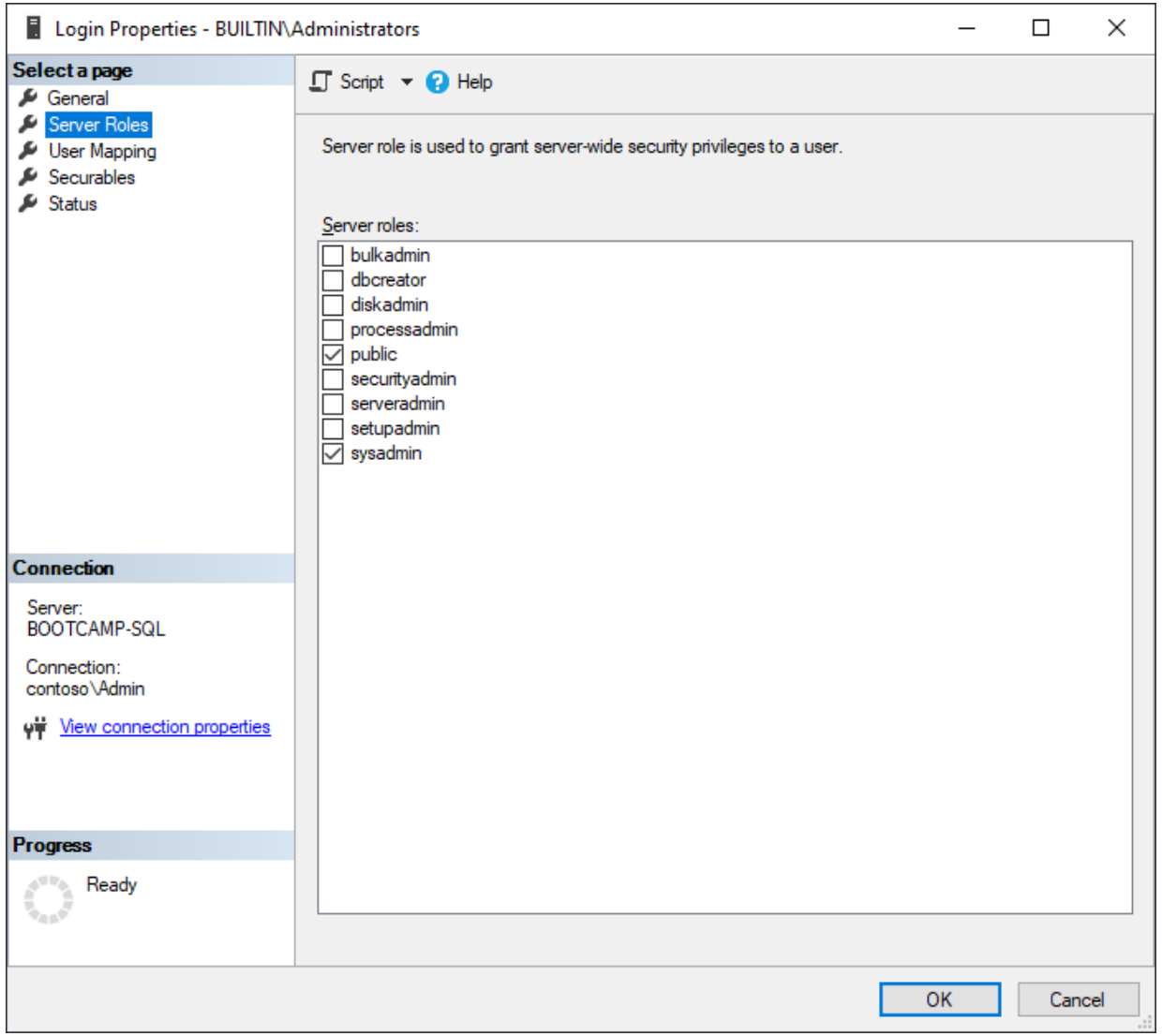
SQL Server Logins



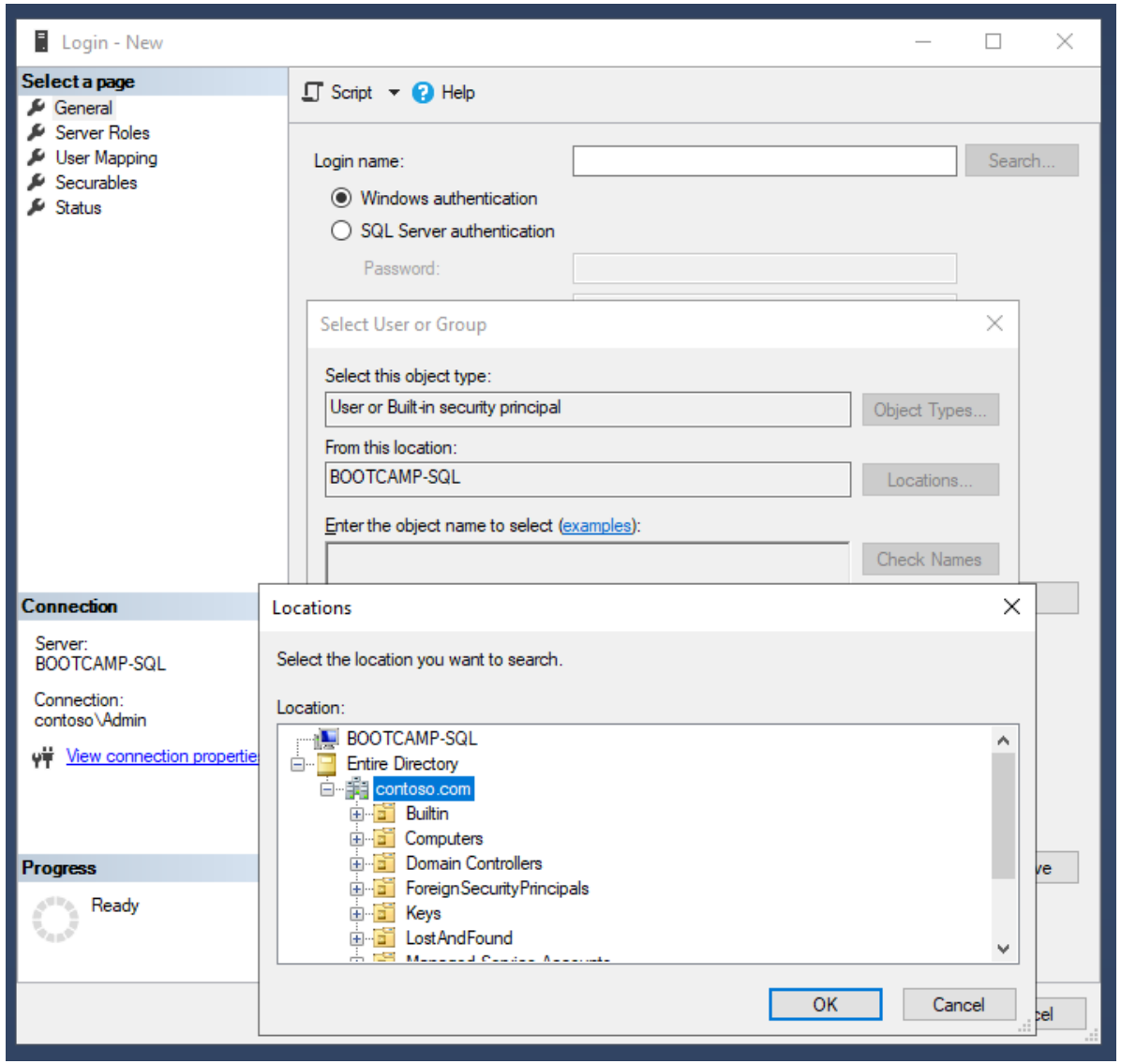
SQL Server Logins – Users/Groups



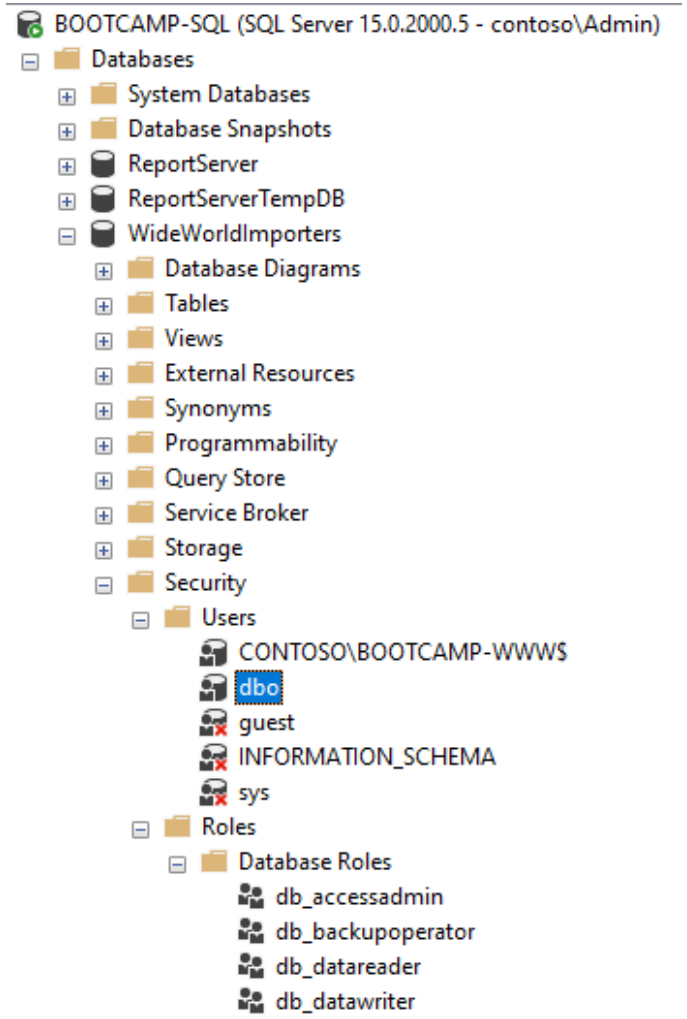
SQL Server Logins – Server Roles



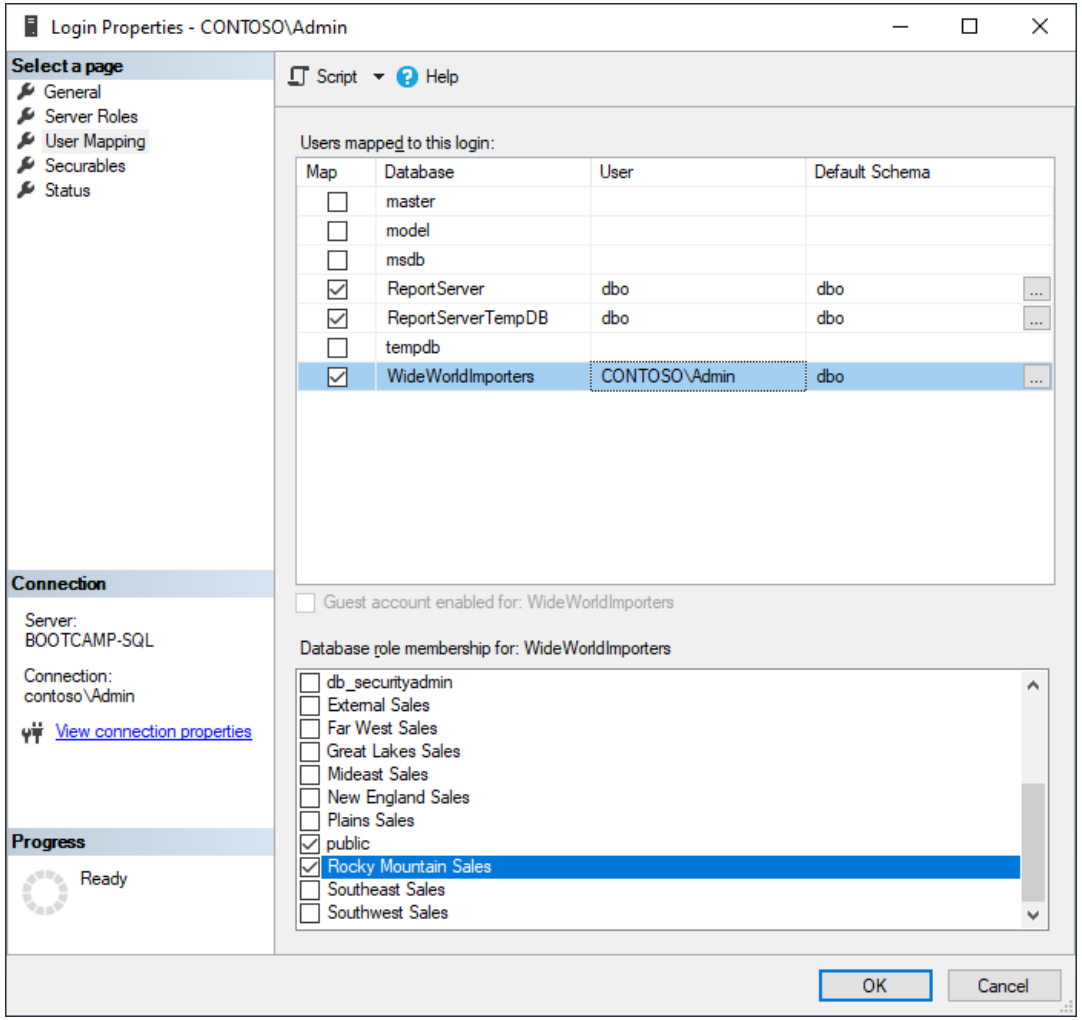
Creating New Logins



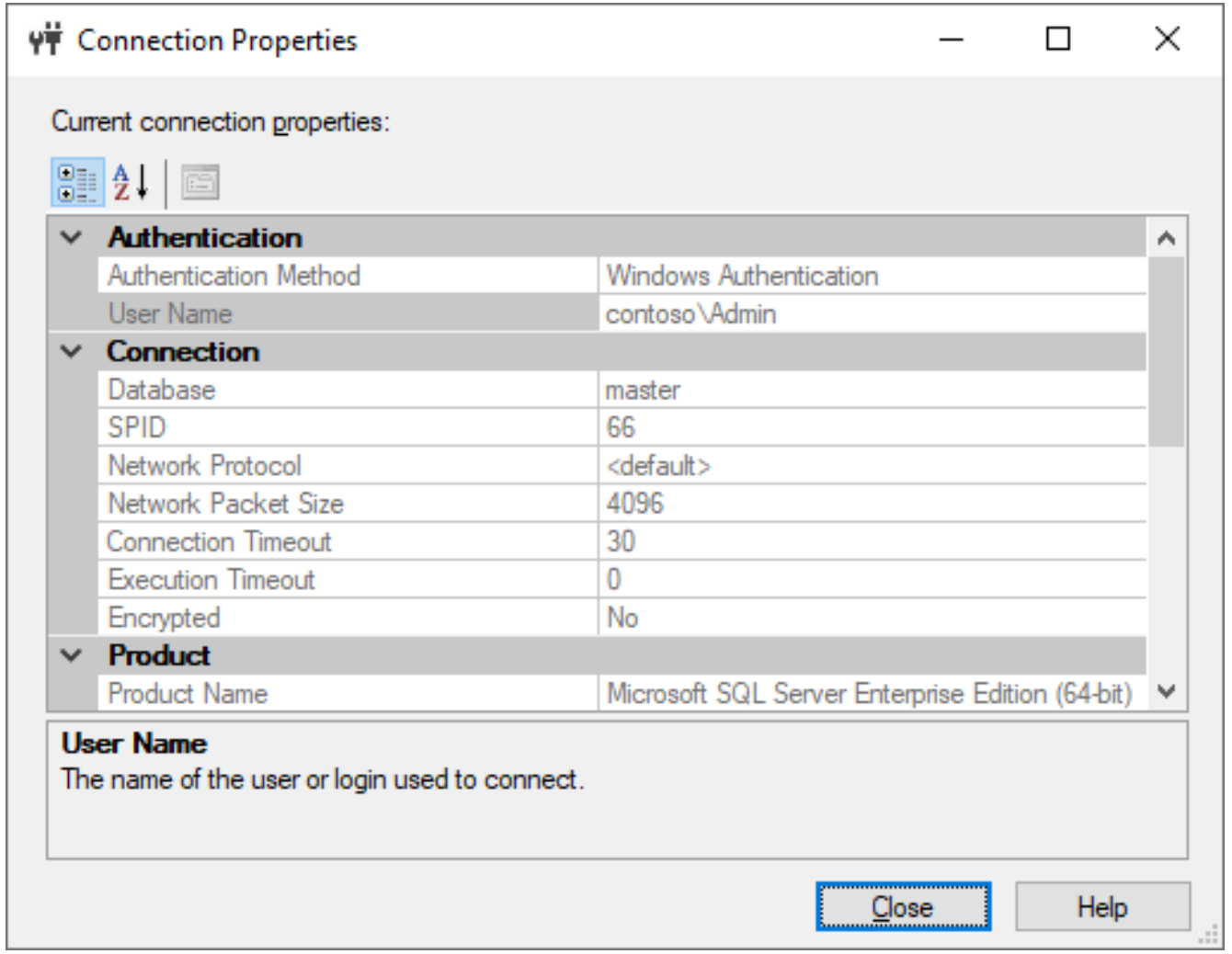
Database Users



Mapping Database Users to Roles



Current Connection Properties



View master.sys.login_token – Local Logon

SQLQuery3.sql - B...ontoso\Admin (63))*

```
SELECT * FROM sys.login_token
```

214 %

Results | Messages

	principal_id	sid	name	type	usage
1	268	0x0105000000000005150000000C9B214024D63B80A36452E...	CONTOSO\Admin	WINDOWS LOGIN	GRANT OR DENY
2	2	0x02	public	SERVER ROLE	GRANT OR DENY
3	3	0x03	sysadmin	SERVER ROLE	GRANT OR DENY
4	259	0x0102000000000005200000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
5	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Domain Users	WINDOWS GROUP	GRANT OR DENY
6	0	0x0101000000000000100000000	\Everyone	WINDOWS GROUP	GRANT OR DENY
7	0	0x0102000000000005200000021020000	BUILTIN\Users	WINDOWS GROUP	GRANT OR DENY
8	259	0x0102000000000005200000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
9	0	0x0101000000000000504000000	NT AUTHORITY\INTERACTIVE	WINDOWS GROUP	GRANT OR DENY
10	0	0x0101000000000000201000000	\CONSOLE LOGON	WINDOWS GROUP	GRANT OR DENY
11	0	0x010100000000000050B000000	NT AUTHORITY\Authenticated Users	WINDOWS GROUP	GRANT OR DENY
12	0	0x010100000000000050F000000	NT AUTHORITY\This Organization	WINDOWS GROUP	GRANT OR DENY
13	0	0x0101000000000000200000000	\LOCAL	WINDOWS GROUP	GRANT OR DENY
14	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Domain Admins	WINDOWS GROUP	GRANT OR DENY
15	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Enterprise Admins	WINDOWS GROUP	GRANT OR DENY
16	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Schema Admins	WINDOWS GROUP	GRANT OR DENY
17	0	0x0101000000000001201000000	\Authentication authority asserted identity	WINDOWS GROUP	GRANT OR DENY
18	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Denied RODC Password Replication Group	WINDOWS GROUP	GRANT OR DENY

View master.sys.login_token – Network Logon

SQLQuery1.sql - B...ontoso\Admin (68))*

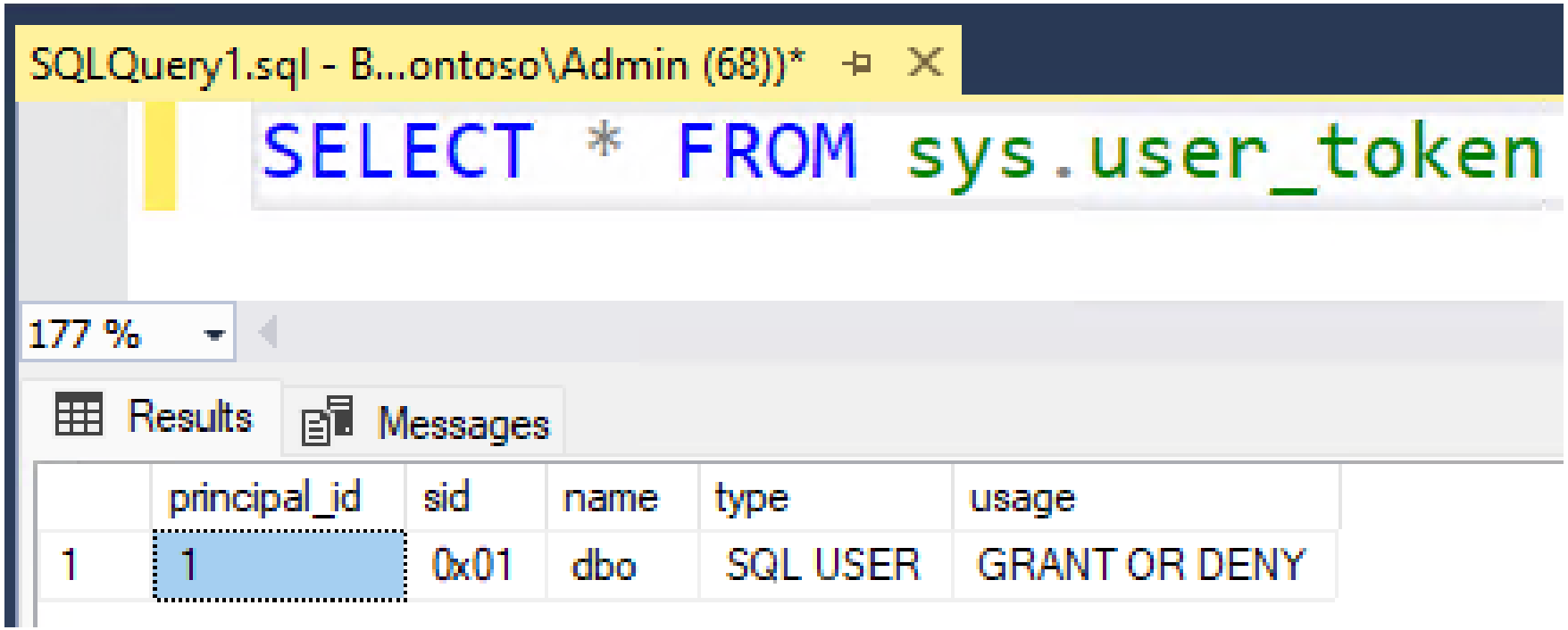
```
SELECT * FROM sys.login_token
```

177 %

Results | Messages

	principal_id	sid	name	type	usage
1	268	0x0105000000000005150000000C9B214024D63B80A36452E...	CONTOSO\Admin	WINDOWS LOGIN	GRANT OR DENY
2	2	0x02	public	SERVER ROLE	GRANT OR DENY
3	3	0x03	sysadmin	SERVER ROLE	GRANT OR DENY
4	259	0x0102000000000005200000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
5	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Domain Users	WINDOWS GROUP	GRANT OR DENY
6	0	0x0101000000000000100000000	\Everyone	WINDOWS GROUP	GRANT OR DENY
7	0	0x0102000000000005200000021020000	BUILTIN\Users	WINDOWS GROUP	GRANT OR DENY
8	259	0x0102000000000005200000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
9	0	0x0101000000000000502000000	NT AUTHORITY\NETWORK	WINDOWS GROUP	GRANT OR DENY
10	0	0x010100000000000050B000000	NT AUTHORITY\Authenticated Users	WINDOWS GROUP	GRANT OR DENY
11	0	0x010100000000000050F000000	NT AUTHORITY\This Organization	WINDOWS GROUP	GRANT OR DENY
12	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Domain Admins	WINDOWS GROUP	GRANT OR DENY
13	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Enterprise Admins	WINDOWS GROUP	GRANT OR DENY
14	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Schema Admins	WINDOWS GROUP	GRANT OR DENY
15	0	0x0101000000000001201000000	\Authentication authority asserted identity	WINDOWS GROUP	GRANT OR DENY
16	0	0x0105000000000005150000000C9B214024D63B80A36452E...	contoso\Denied RODC Password Replication Group	WINDOWS GROUP	GRANT OR DENY

View master.sys.user_token



WIA Under the Hood

Windows Integrated Authentication

- WIA = IWA = Negotiate = SPNEGO = NEGO

- Authentication Packages
  - Kerberos
  - MSV1_0
    - NTLMv2
    - NTLM
    - ~~LM~~

The Bigger Picture

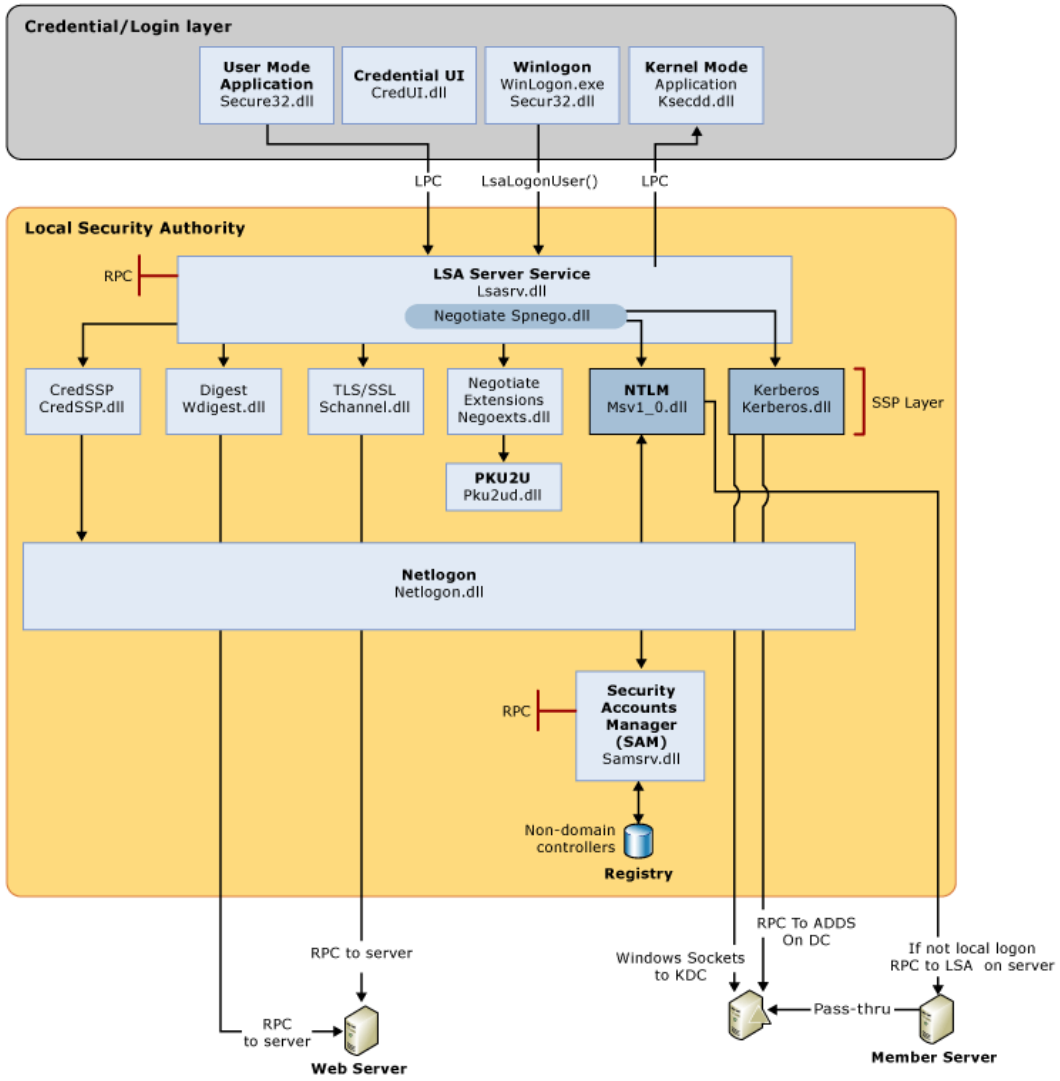


Image Source: https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication

NTLM Authentication – Challenge-Response

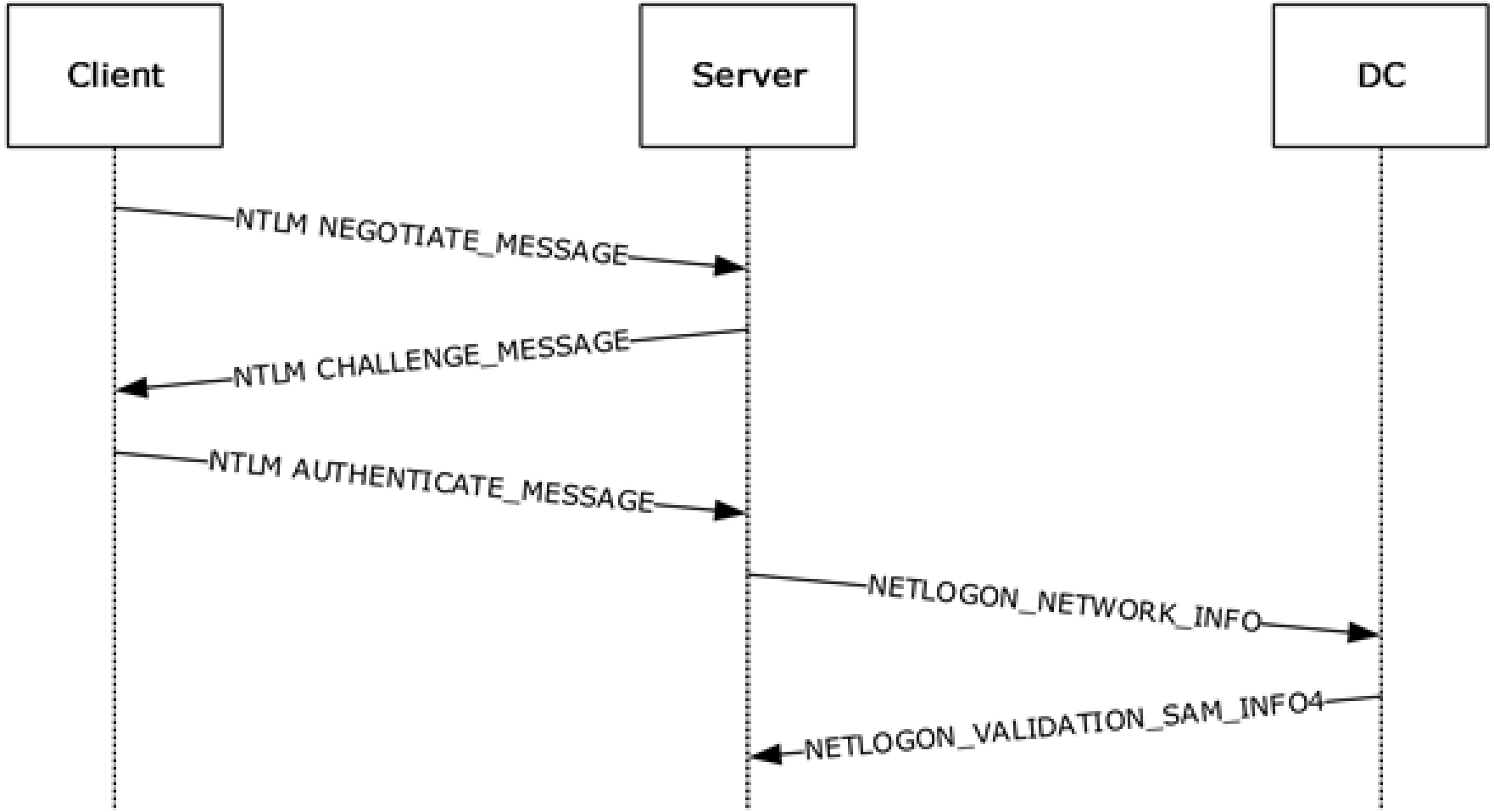
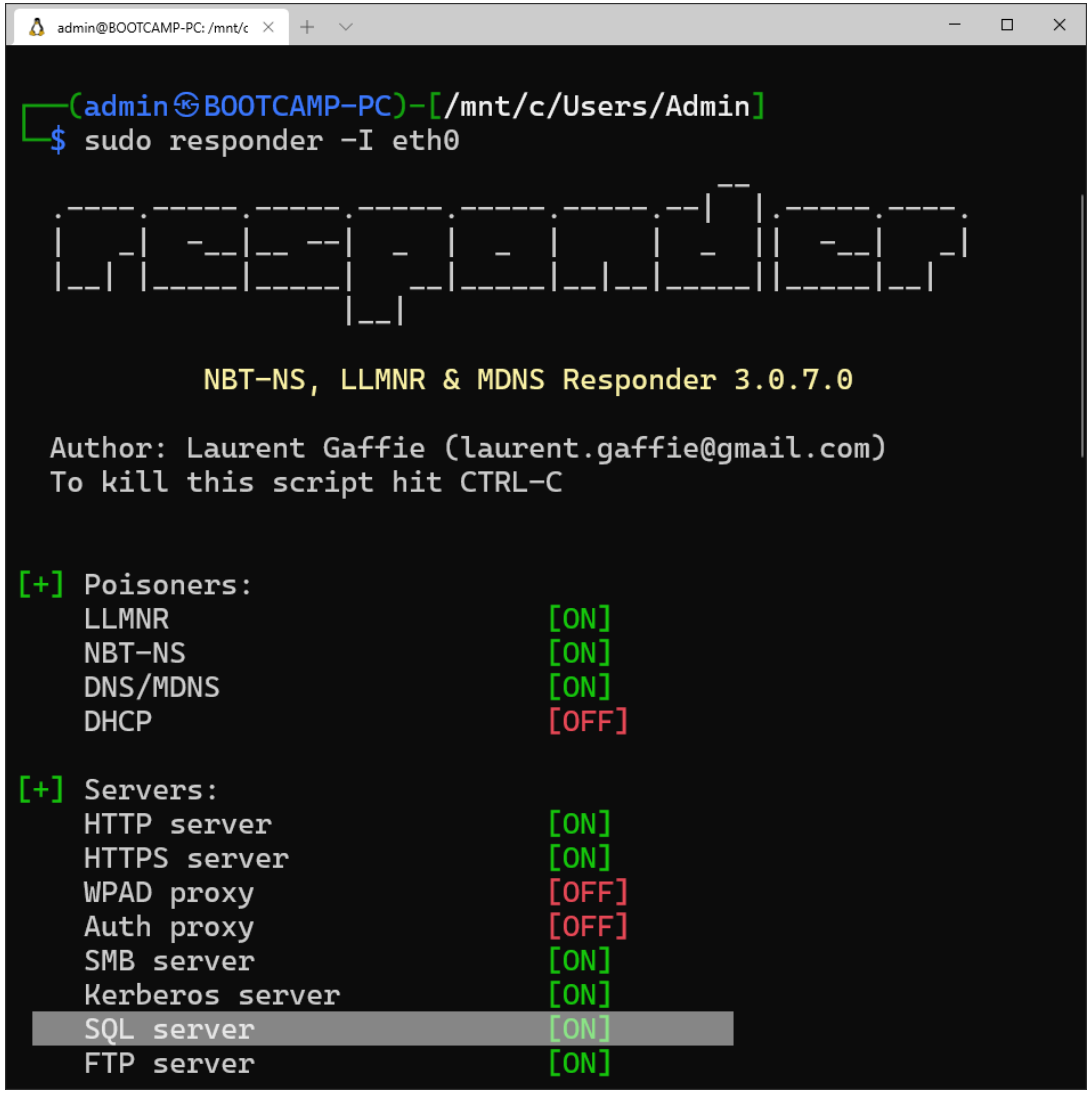


Image Source: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-apds/5bfd942e-7da5-494d-a640-f269a0e3cc5d

NTLM Weaknesses

- Legacy Password Hash Function (MD4)
- Deprecated Encryption (HMAC-MD5, DES)
- Lacks Mutual Authentication

NTLM MITM – Traffic Capture



NTLM MITM – Traffic Capture

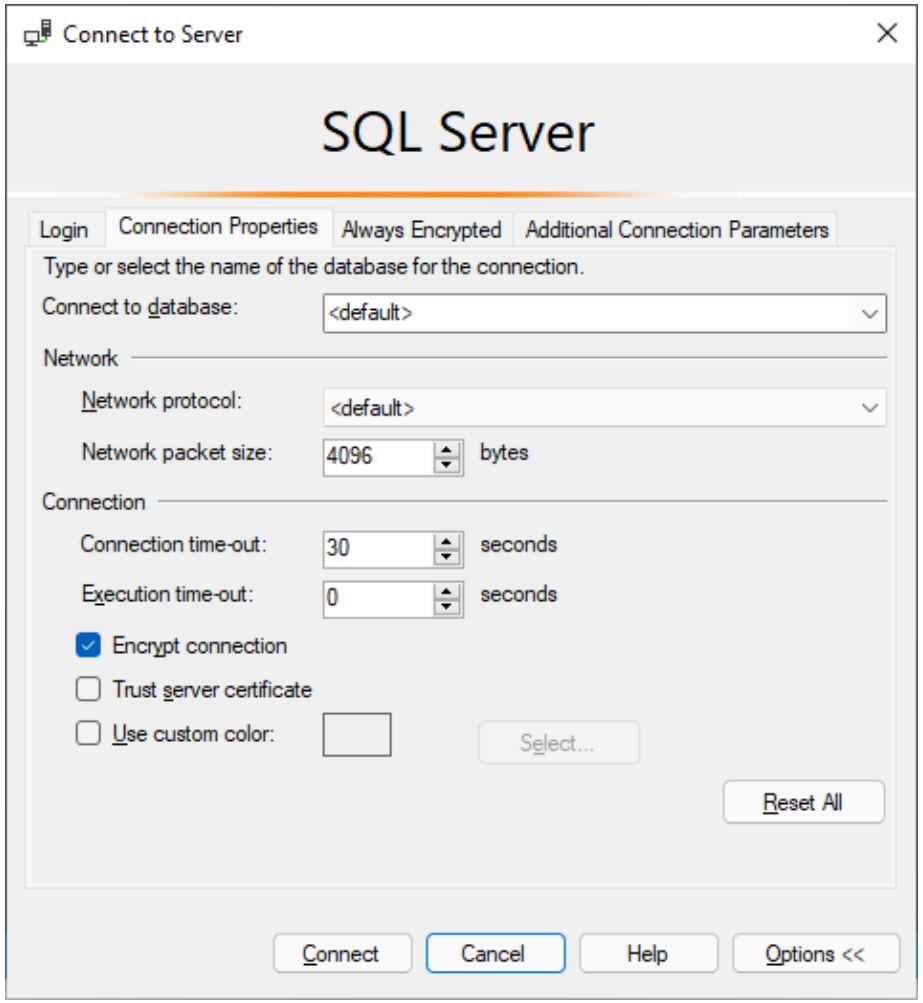
```
[*] [MDNS] Poisoned answer sent to 172.22.0.1      for name contoso-sql.□local
[MSSQL] NTLMv2 Client   : 172.22.0.1
[MSSQL] NTLMv2 Username : contoso\Admin
[MSSQL] NTLMv2 Hash     : Admin::contoso:265f3903183967ec:A70BAB60ECAB3C5148A99D4549326923:01010000000000
00C1E2D9F055D1D701BFF5E8A66031A9A3000000002000800 4D0054004100440001001E00570049004E002D00370034004700 4B0
04B00430032005A00460035005500040014004D0054004100440 02E004C004F00430041004C0003003400570049004E002D003700
34004700 4B004B00430032005A00460035005500 2E004D0054004100440 02E004C004F00430041004C0005001400 4D0054004100 4
4002E004C004F00430041004C0008003000300000000000000000000000300000C15C7EE7DD0FFE1D5F5F84F6E2257F816BC1B6
E4D30B385FF0FA80A93FA5E0000A00100000000000000000000000000000000000009003E004D0053005300510 04C0053007600630
02F0063006F006E0074006F0073006F002D00730071006C002E006C006F00630061006C003A00310034003300330000000000000
0000
```

NTLM Traffic Cracking

```
┌──(admin㉿BOOTCAMP-PC)-[/mnt/c/Users/Admin]
└─$ sudo john --format=netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt /usr/share/responder/logs/MSSQL-NTLMv2-172.22.0.1.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Pa$$w0rd         (Admin)
Pa$$w0rd         (Admin)
Pa$$w0rd         (Admin)
3g 0:00:00:00 DONE (2021-11-04 10:07) 4.411g/s 117458p/s 352376c/s 352376C/s jasonf..Bulldog
```

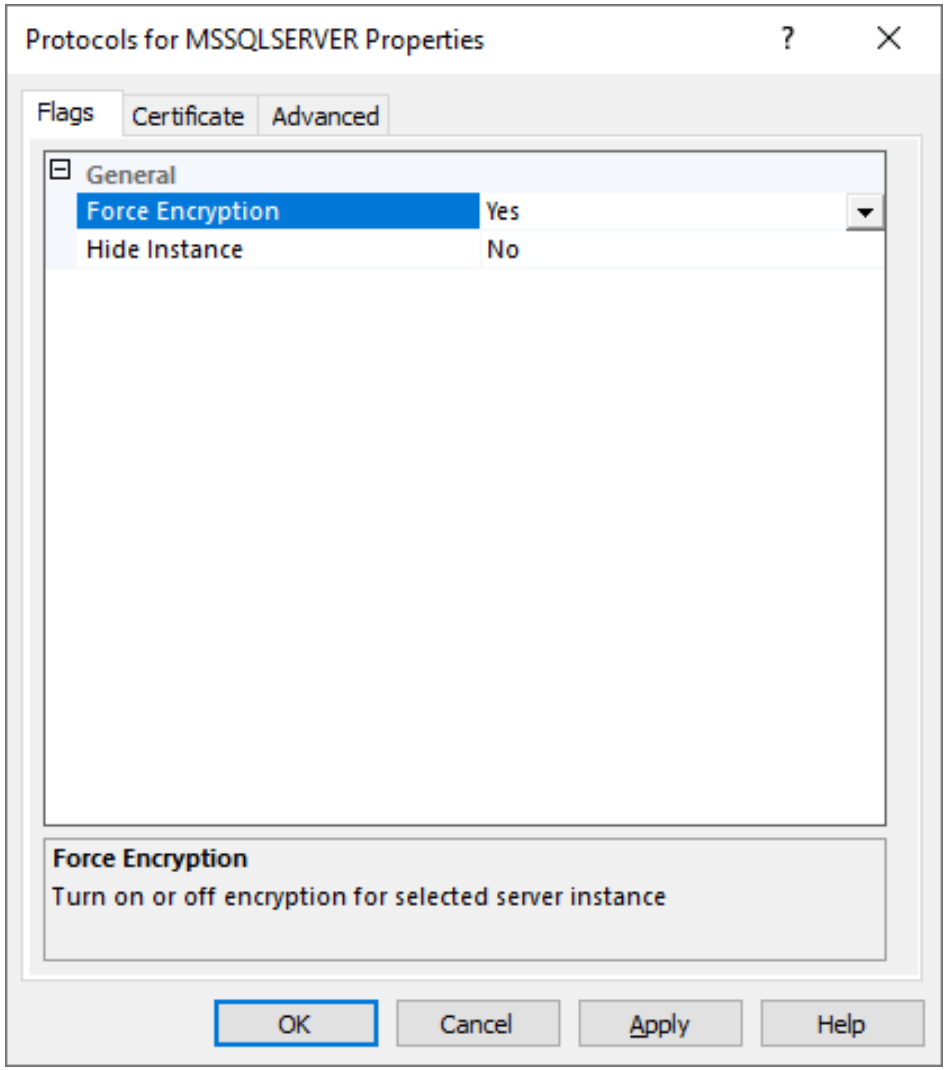
DEMO: SQL Server MITM with Responder

Solution: Enforce Encryption on Client

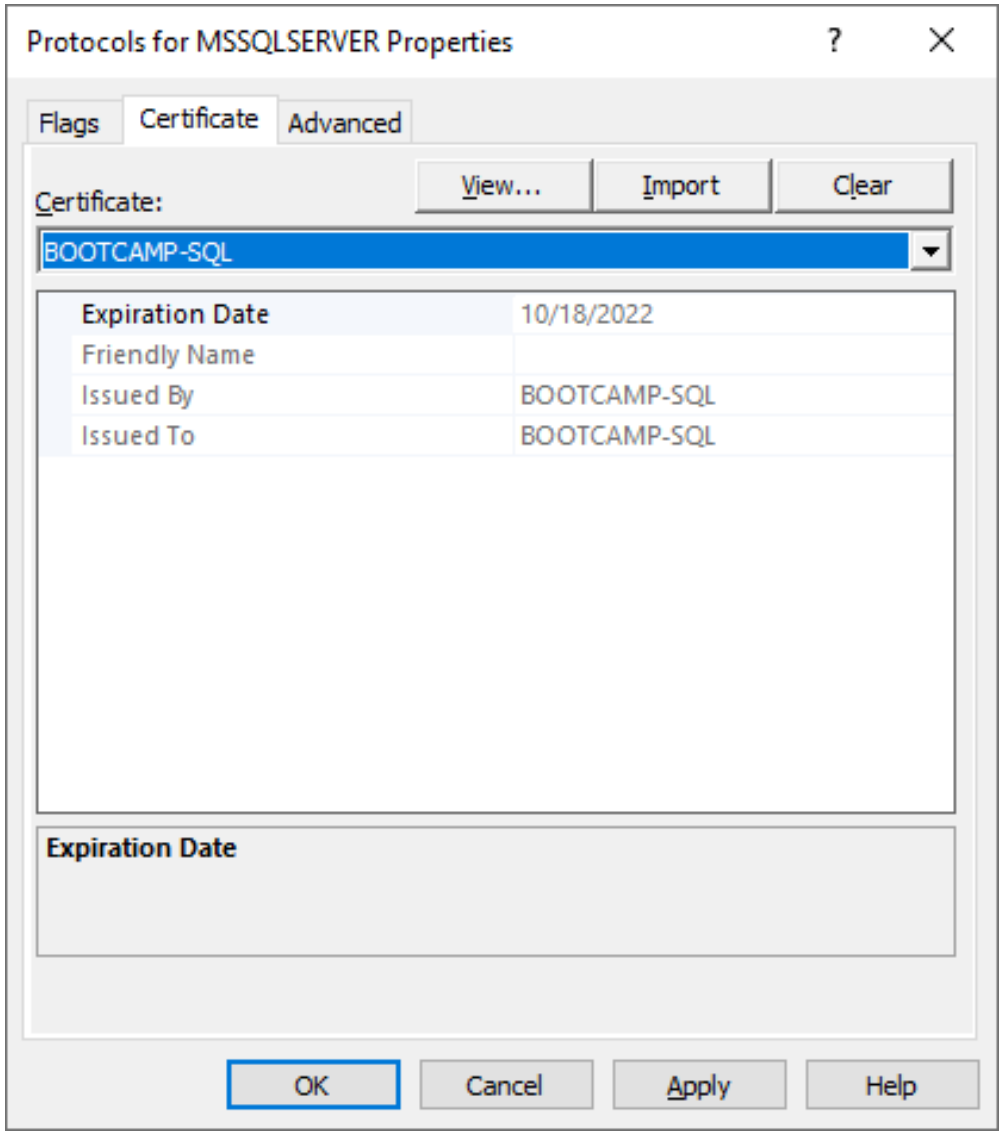


Connection String: **Encrypt=True**;**TrustServerCertificate=True**

Server-Side Enforcement Insufficient



Deploy a Proper Certificate



NTLM Relay Attack

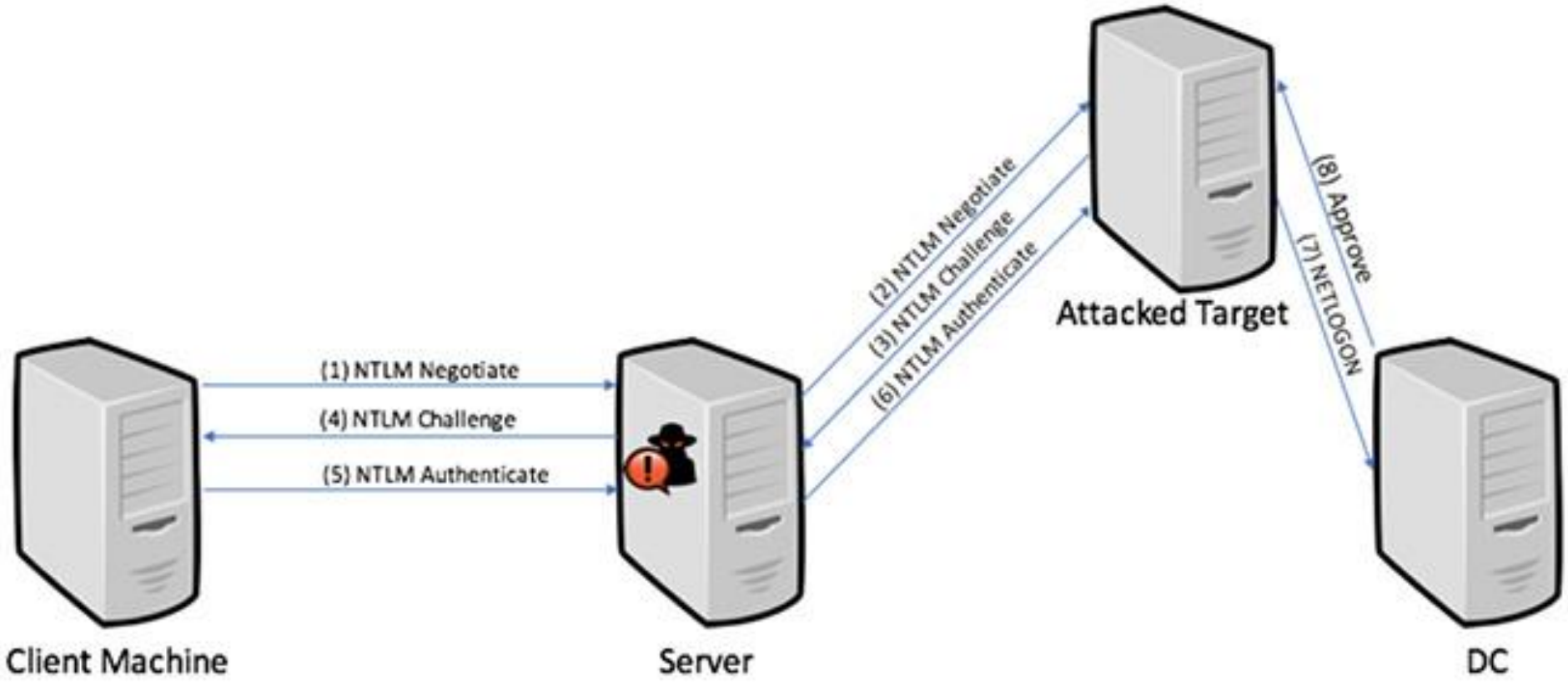
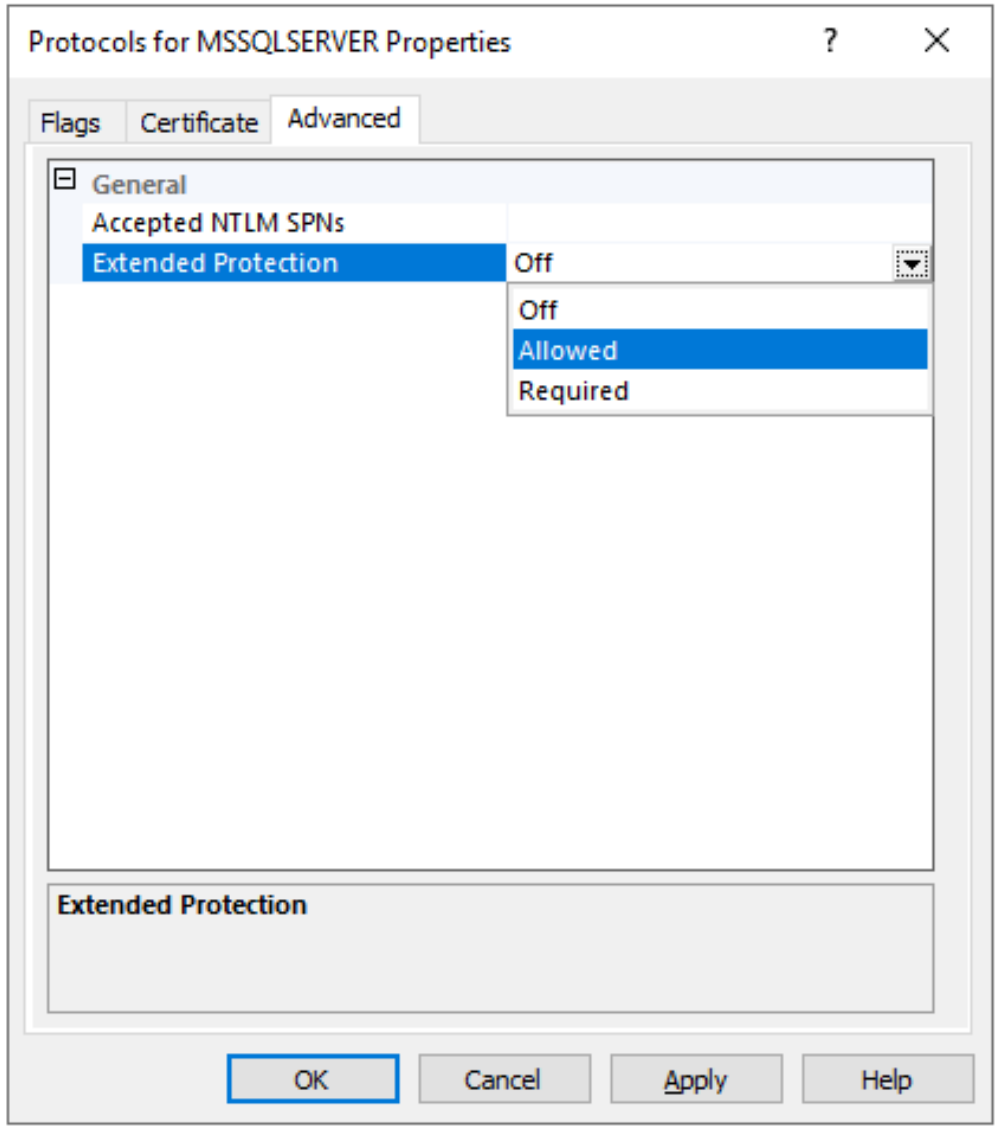


Image Source: https://www.helpnetsecurity.com/2019/06/11/microsoft-ntlm-vulnerabilities/

Extended Protection for Authentication



Kerberos Authentication

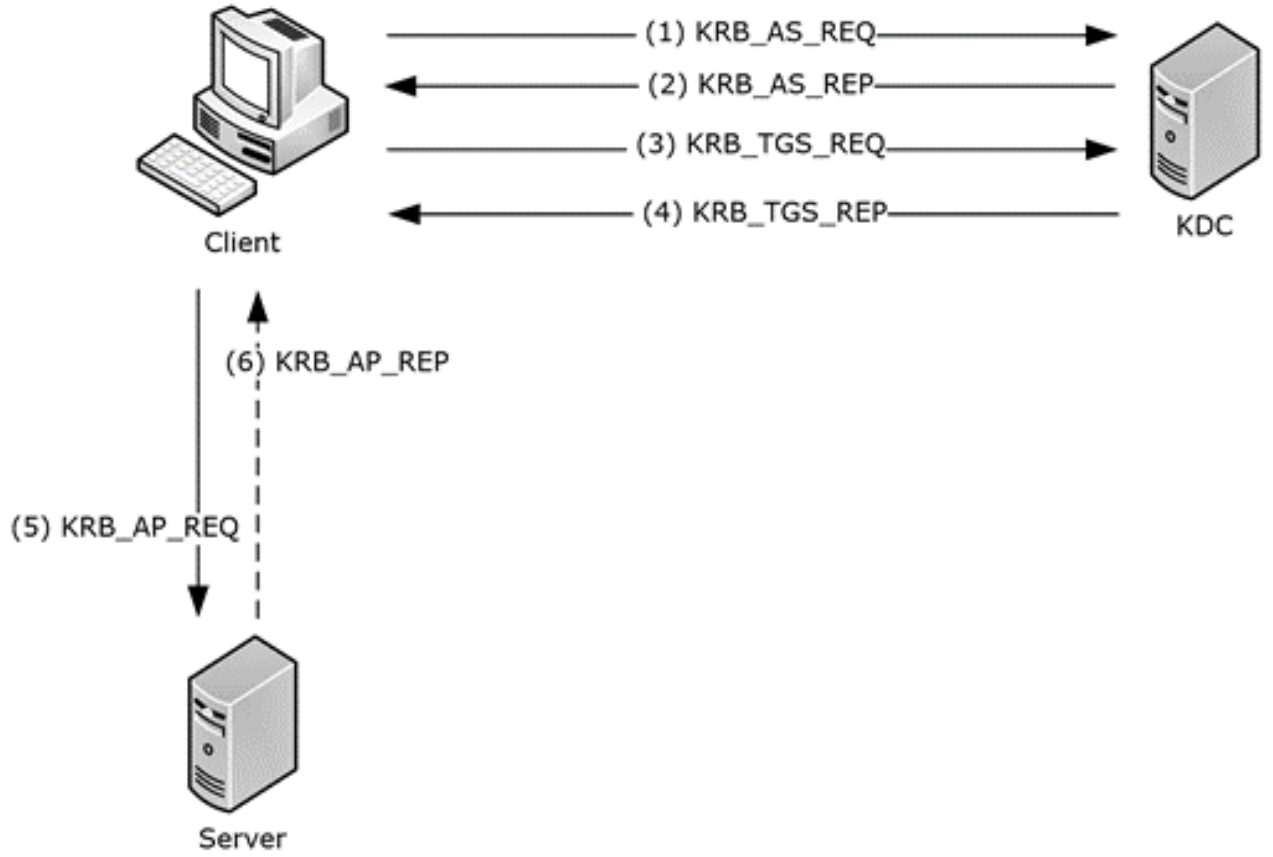
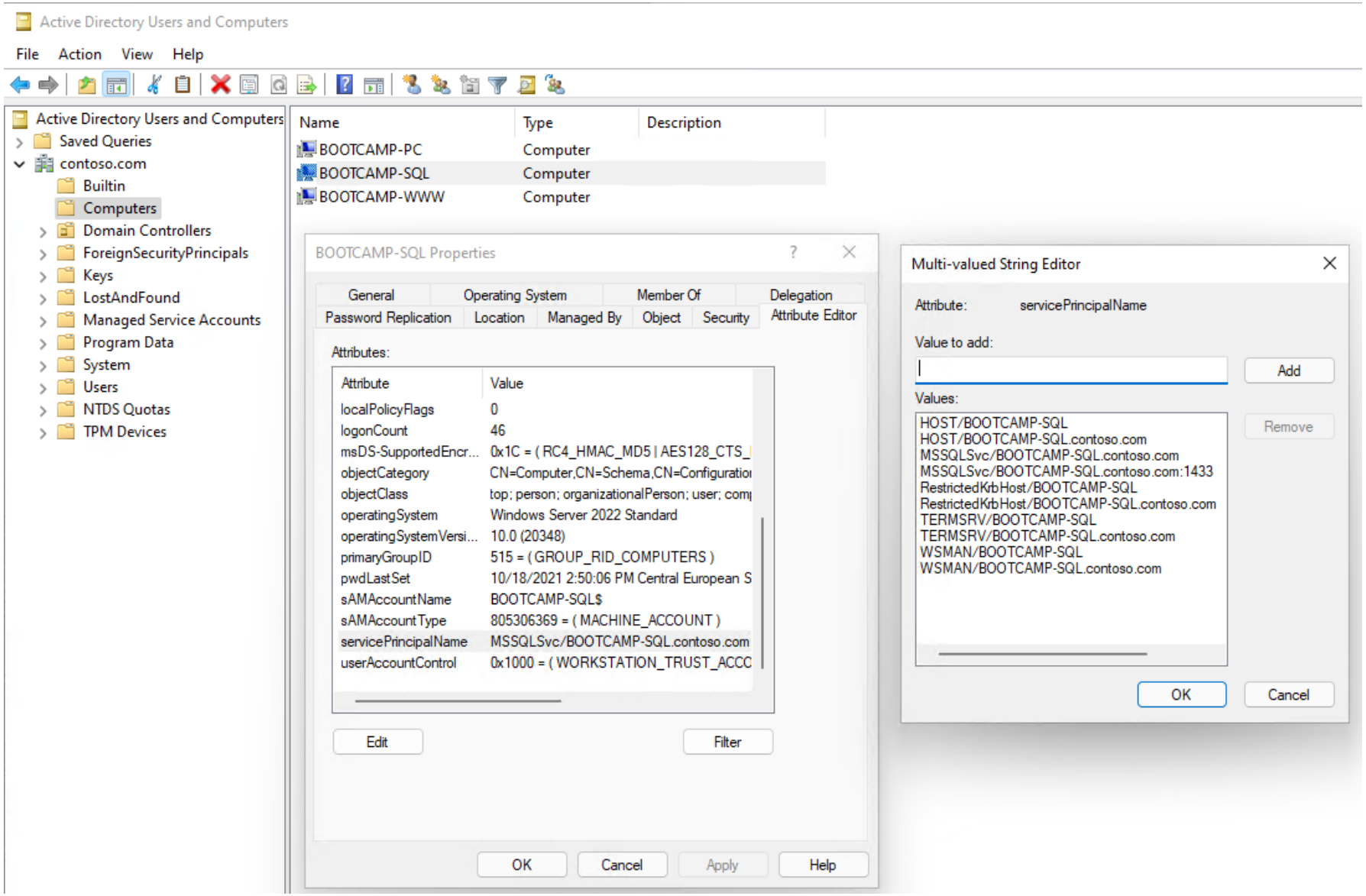


Image Source: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13

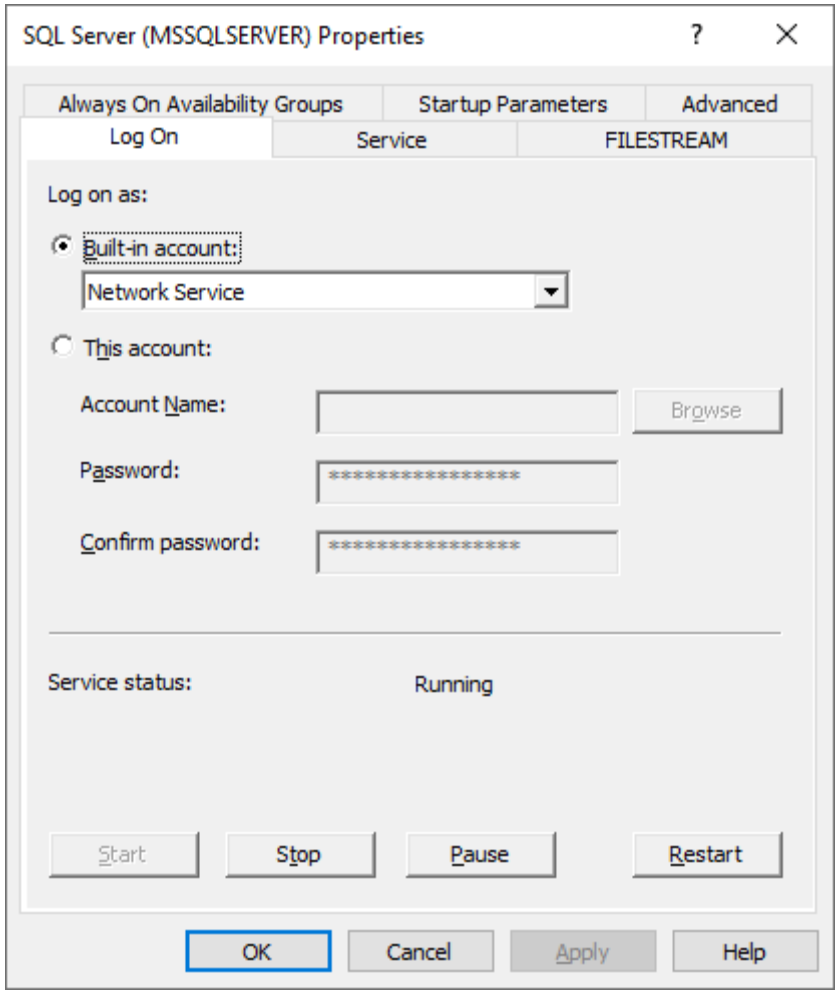
Kerberos Ticket Cache in Windows

DEMO: Kerberos Ticket Cache

Enabling Kerberos for SQL Server in AD

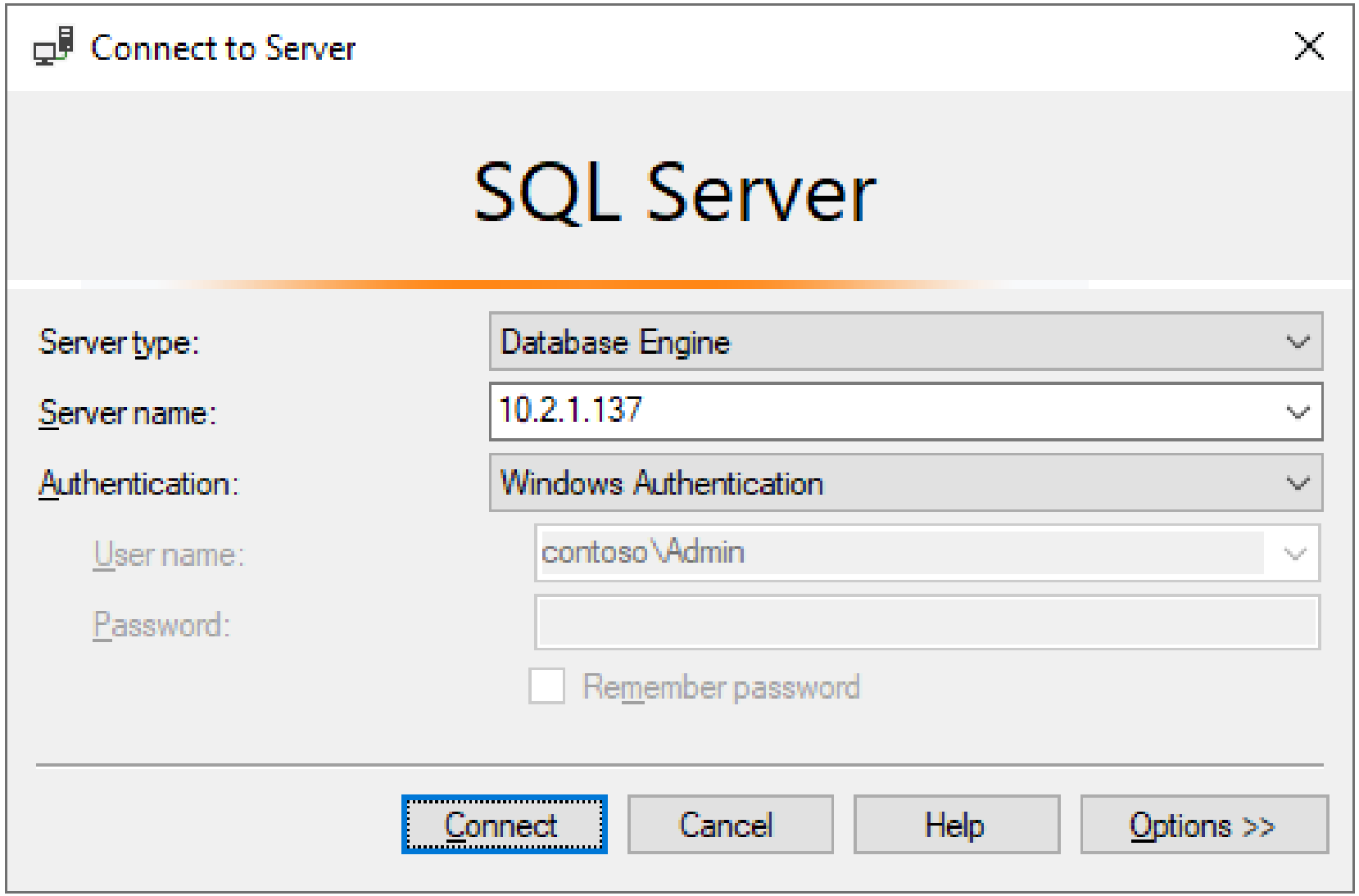


Enabling Kerberos for SQL Server in AD

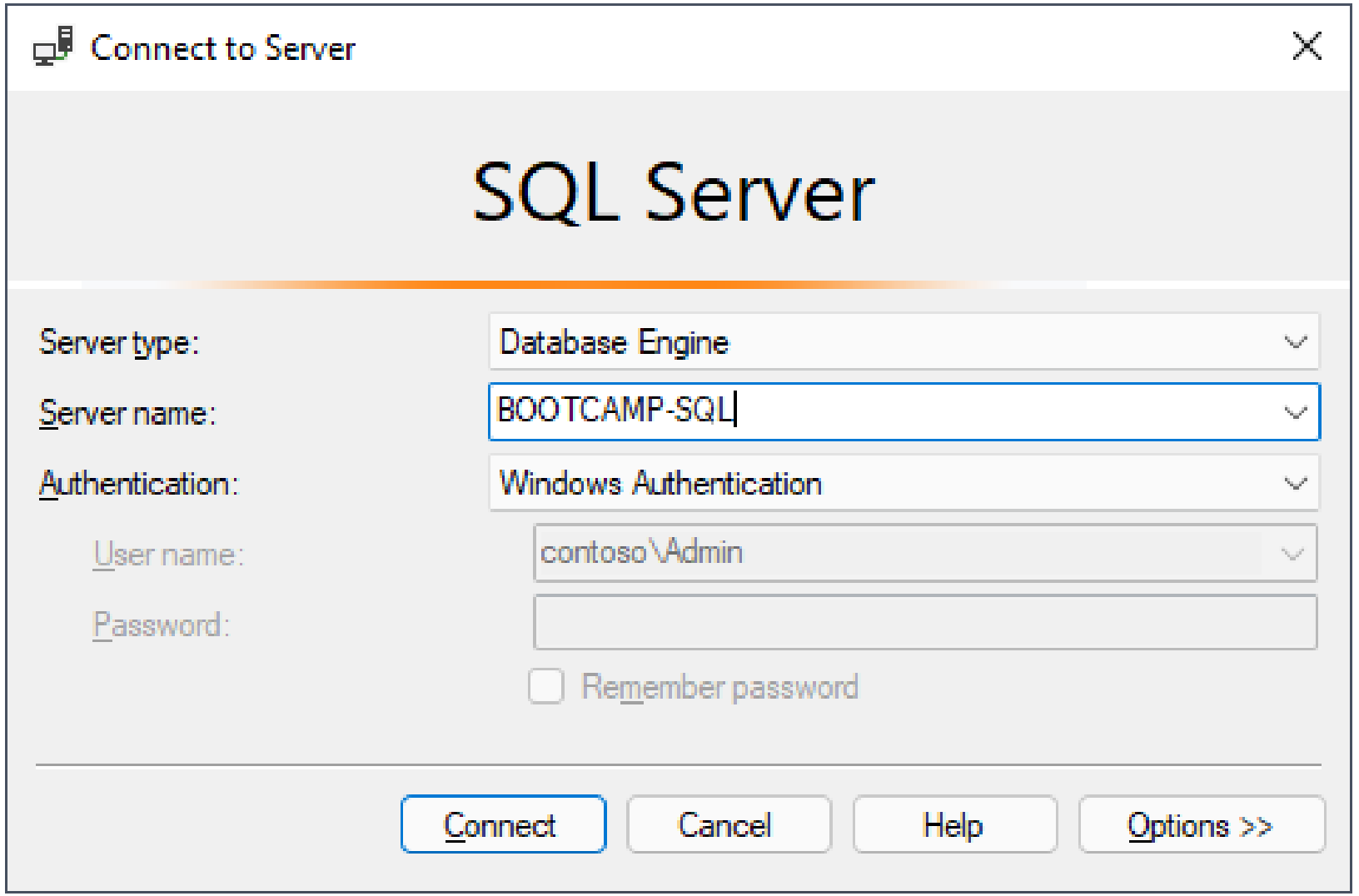


DEMO: Configuring SPNs for SQL Server

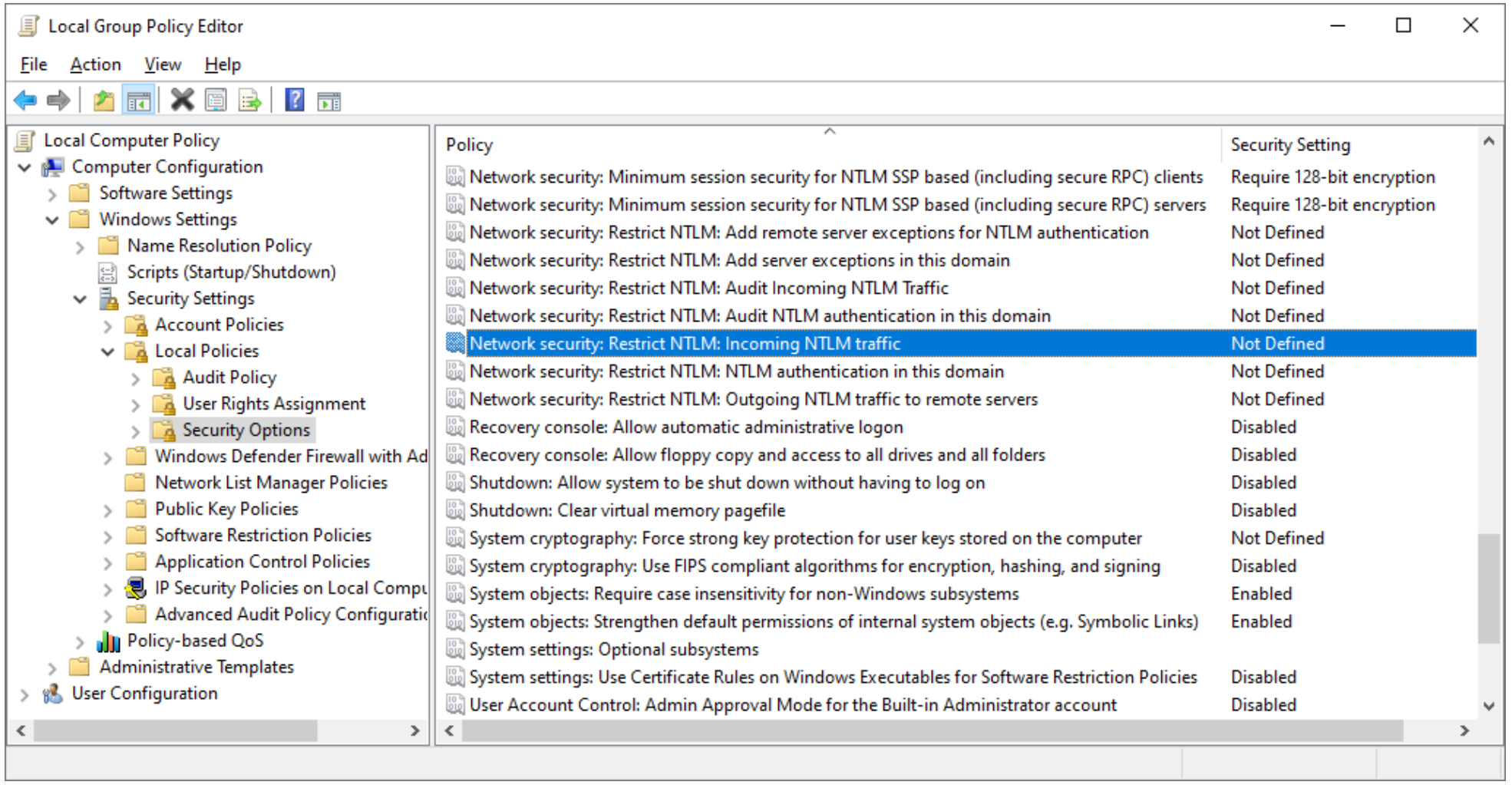
IP Address NTLM Fallback (99% Cases)



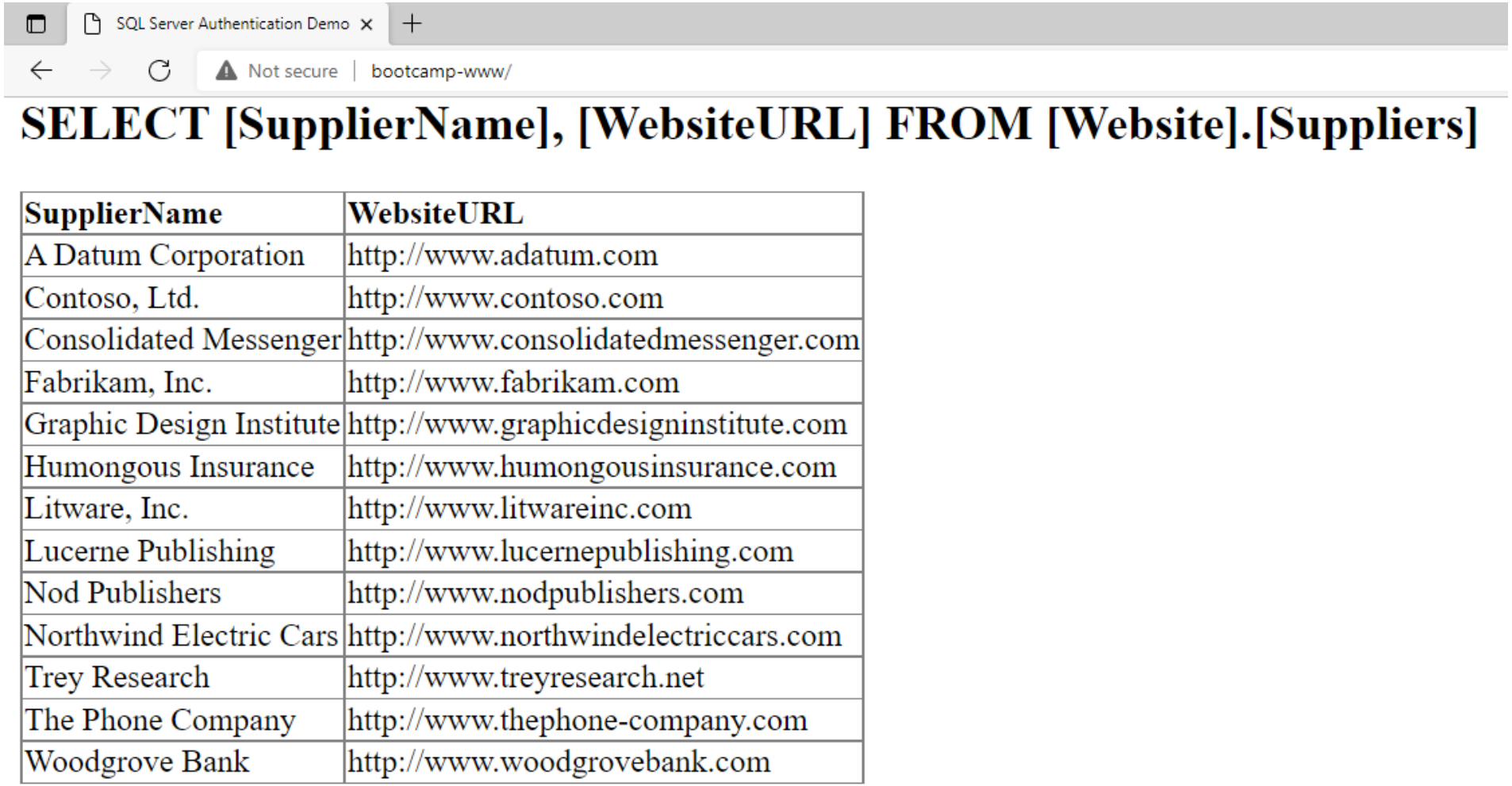
NetBIOS Name NTLM Fallback (Sometimes)



Restricting NTLM Traffic



Web App Authentication



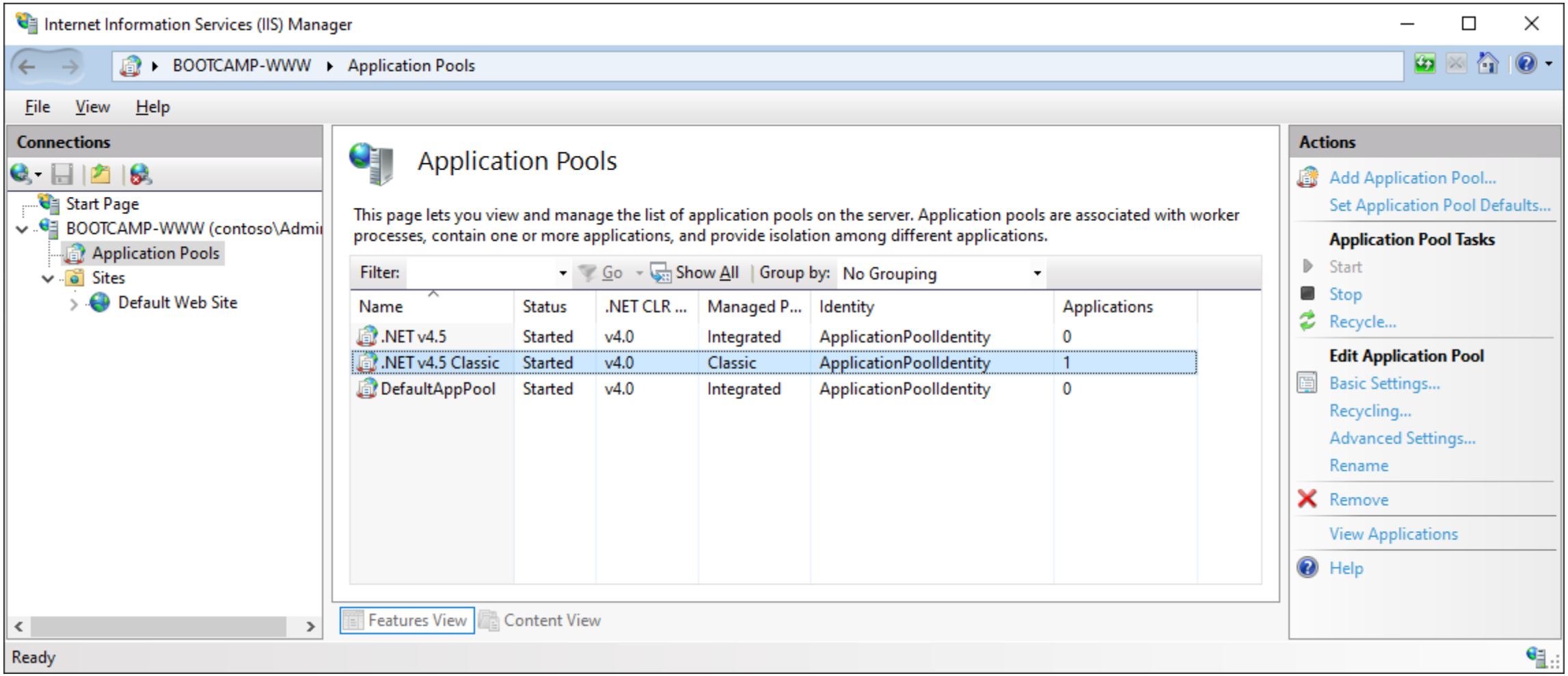
SupplierName	WebsiteURL
A Datum Corporation	http://www.adatum.com
Contoso, Ltd.	http://www.contoso.com
Consolidated Messenger	http://www.consolidatedmessenger.com
Fabrikam, Inc.	http://www.fabrikam.com
Graphic Design Institute	http://www.graphicdesigninstitute.com
Humongous Insurance	http://www.humongousinsurance.com
Litware, Inc.	http://www.litwareinc.com
Lucerne Publishing	http://www.lucernepublishing.com
Nod Publishers	http://www.nodpublishers.com
Northwind Electric Cars	http://www.northwindelectriccars.com
Trey Research	http://www.treyresearch.net
The Phone Company	http://www.thephone-company.com
Woodgrove Bank	http://www.woodgrovebank.com

Using WIA in Connection Strings

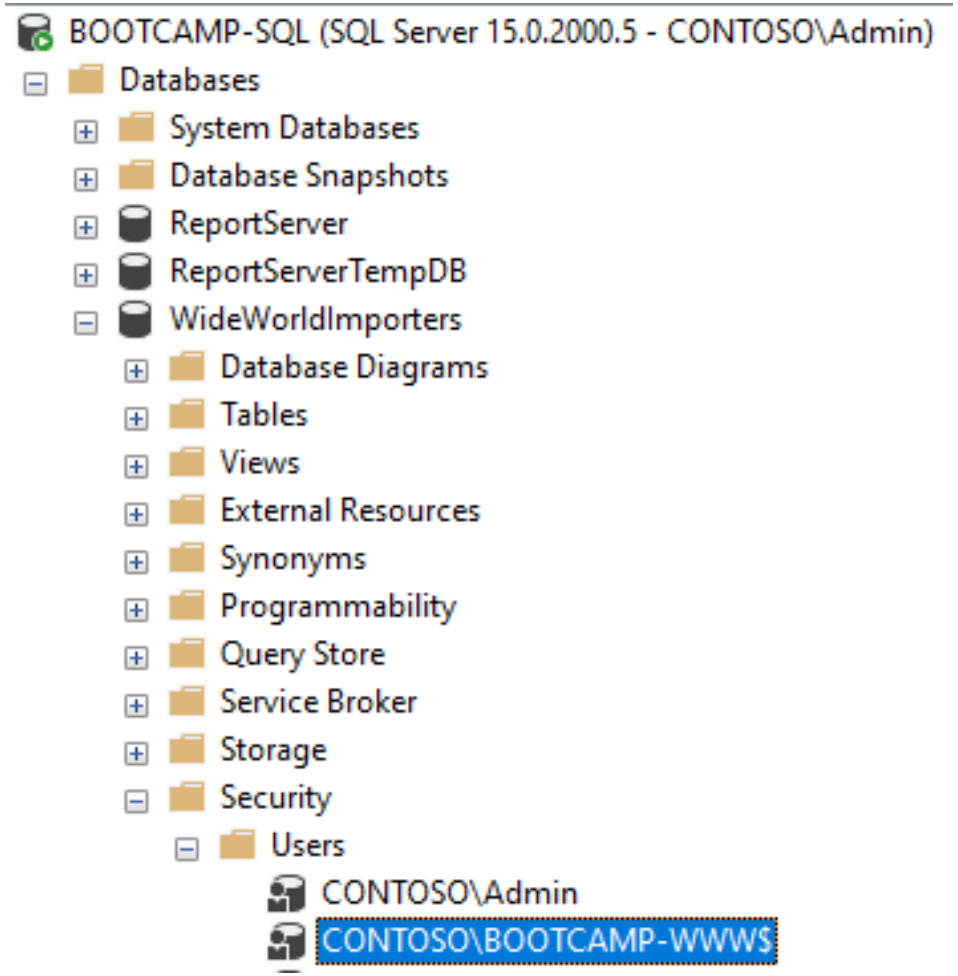
web.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <connectionStrings>
        <clear />
        <add name="WideWorldImporters" connectionString="Server=bootcamp-sql.contoso.com;Database=WideWorldImporters;Integrated Security=SSPI" />
    </connectionStrings>
    <system.webServer>
      <security>
```

Application Identity

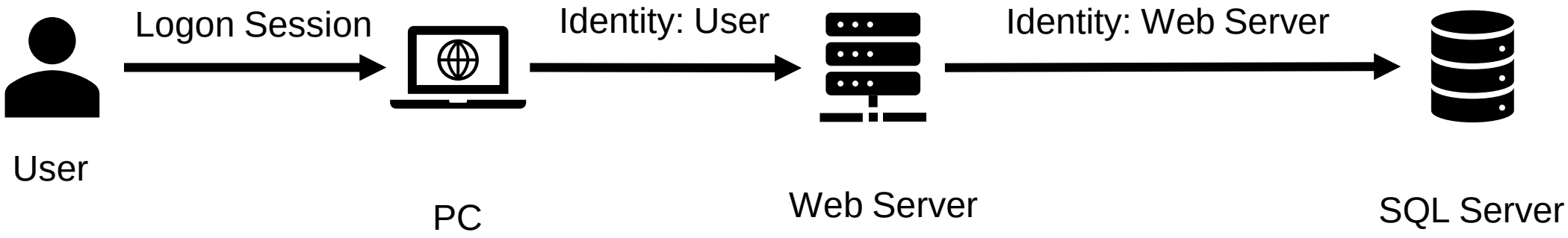


Granting Application Access

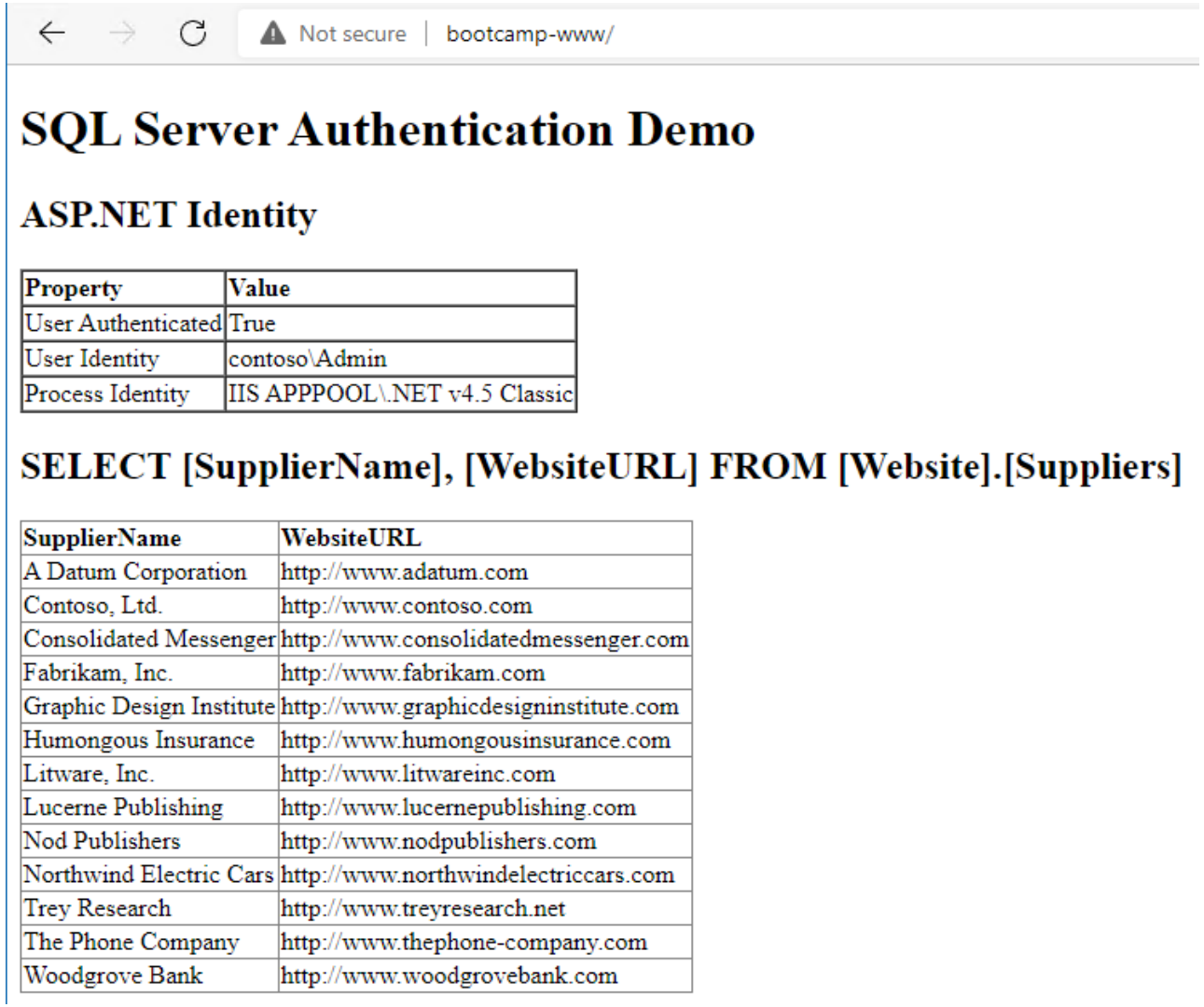


Kerberos Delegation

WIA Without Delegation



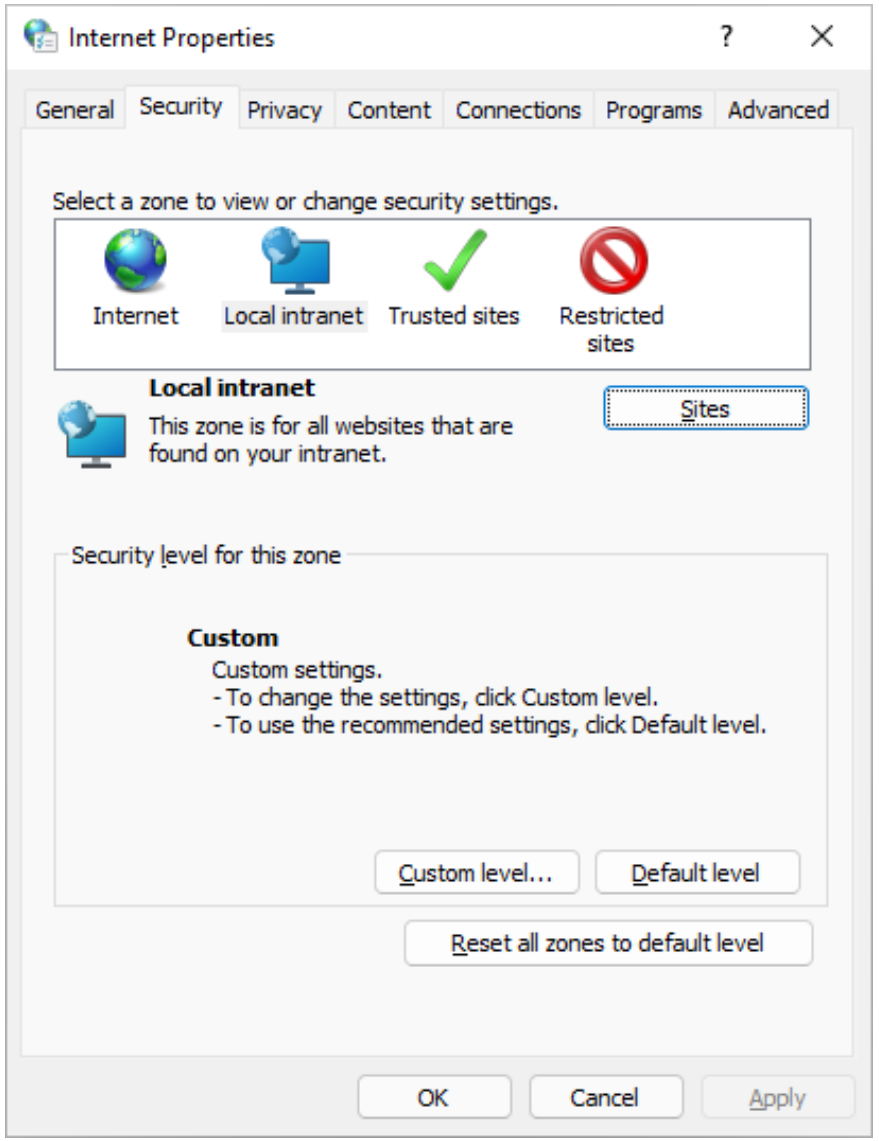
WIA Without Delegation



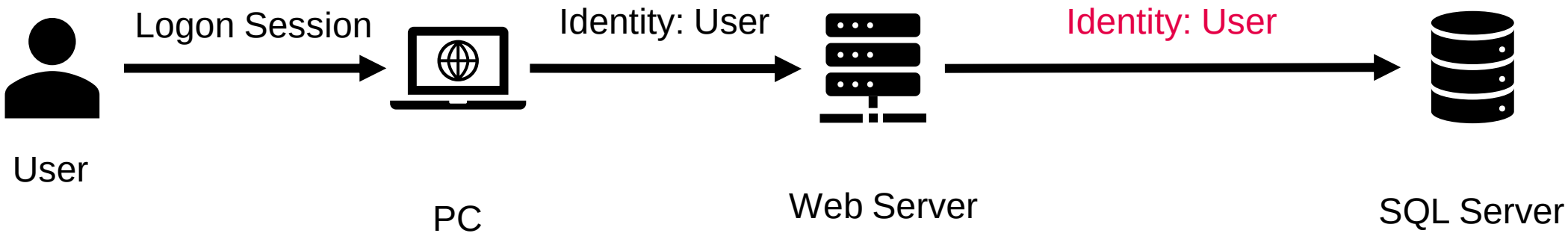
Configuration a Web App for WIA

```
<system.webServer>
  <security>
    <authentication>
      <anonymousAuthentication enabled="false" />
      <windowsAuthentication enabled="true" />
    </authentication>
  </security>
</system.webServer>
```

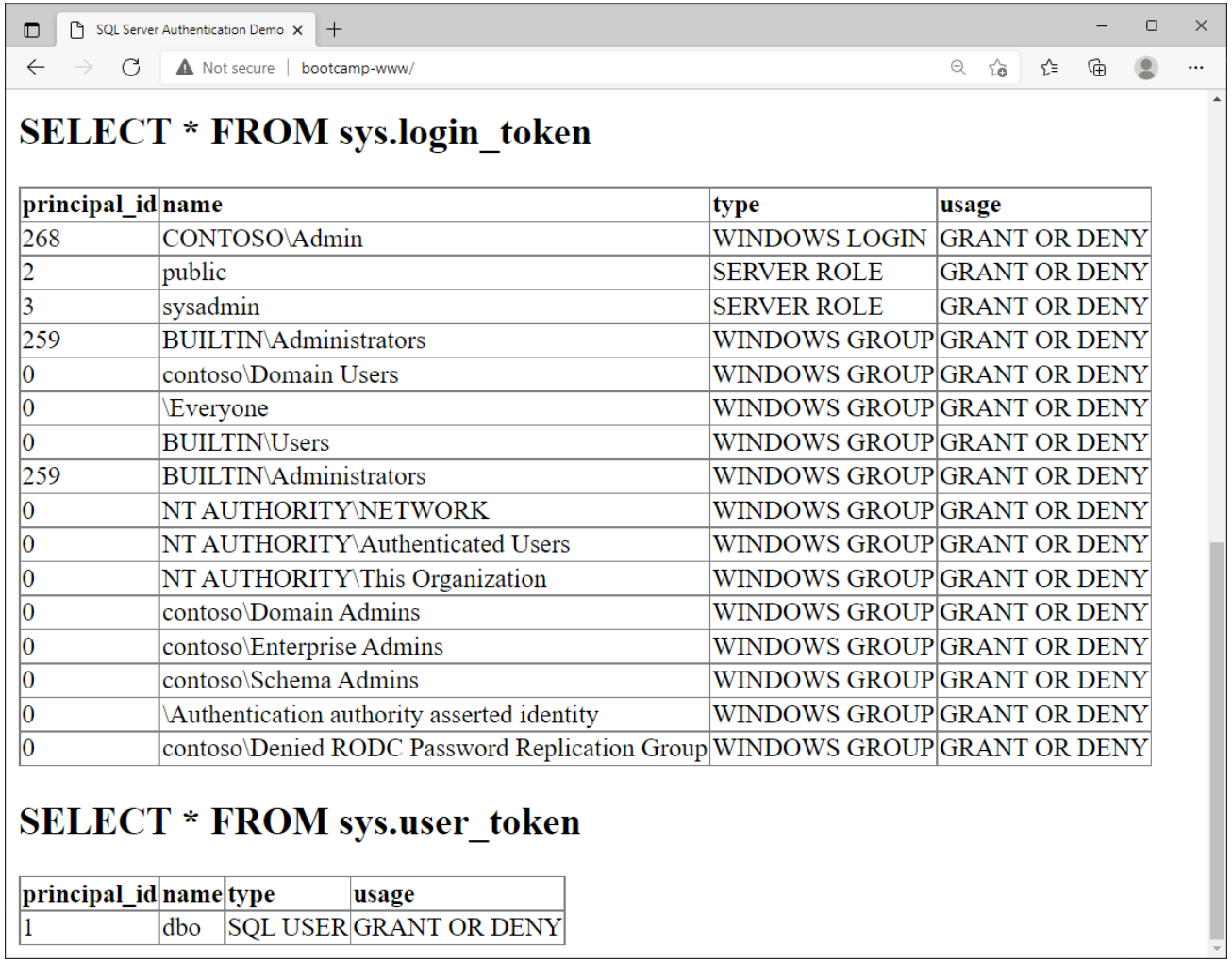
Requirement: Local Intranet Zone



WIA With Delegation/Impersonation



WIA With Delegation/Impersonation



SELECT * FROM sys.login_token

principal_id	name	type	usage
268	CONTOSO\Admin	WINDOWS LOGIN	GRANT OR DENY
2	public	SERVER ROLE	GRANT OR DENY
3	sysadmin	SERVER ROLE	GRANT OR DENY
259	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
0	contoso\Domain Users	WINDOWS GROUP	GRANT OR DENY
0	\Everyone	WINDOWS GROUP	GRANT OR DENY
0	BUILTIN\Users	WINDOWS GROUP	GRANT OR DENY
259	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
0	NT AUTHORITY\NETWORK	WINDOWS GROUP	GRANT OR DENY
0	NT AUTHORITY\Authenticated Users	WINDOWS GROUP	GRANT OR DENY
0	NT AUTHORITY\This Organization	WINDOWS GROUP	GRANT OR DENY
0	contoso\Domain Admins	WINDOWS GROUP	GRANT OR DENY
0	contoso\Enterprise Admins	WINDOWS GROUP	GRANT OR DENY
0	contoso\Schema Admins	WINDOWS GROUP	GRANT OR DENY
0	\Authentication authority asserted identity	WINDOWS GROUP	GRANT OR DENY
0	contoso\Denied RODC Password Replication Group	WINDOWS GROUP	GRANT OR DENY

SELECT * FROM sys.user_token

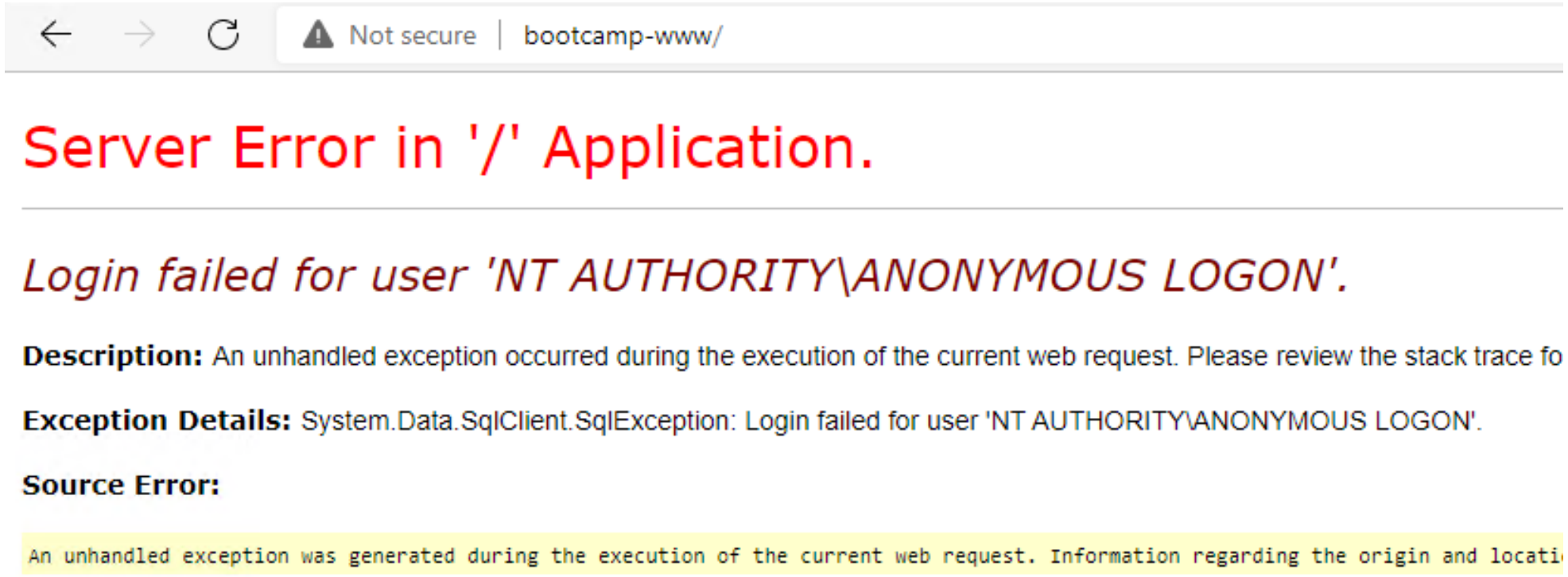
principal_id	name	type	usage
1	dbo	SQL USER	GRANT OR DENY

Configuring a Web App for Delegation

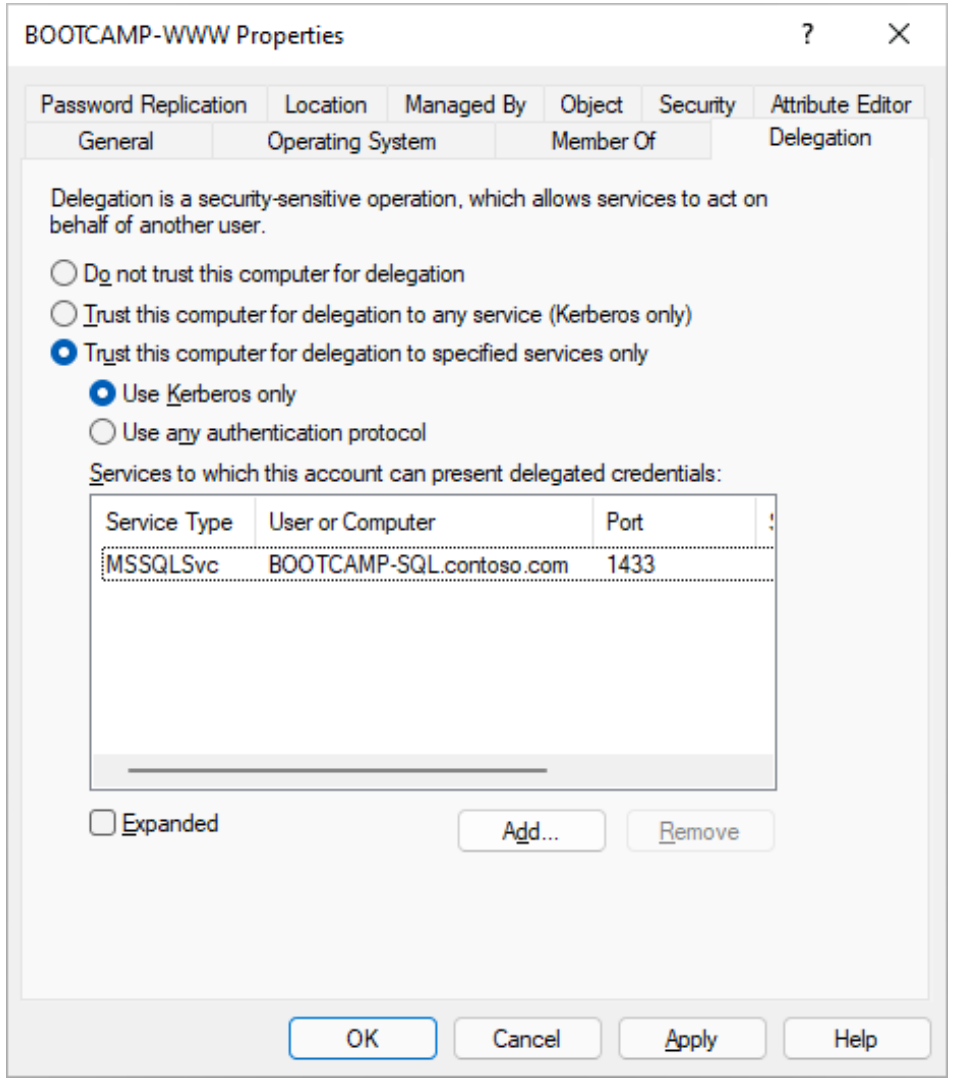
web.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <connectionStrings>
        <clear />
        <add name="WideWorldImporters" connectionString="Server=bootcamp-sql.contoso.com;Database=WideWorldImporters;Integrated Security=SSPI" />
    </connectionStrings>
    <system.webServer>
      <security>
        <authentication>
          <anonymousAuthentication enabled="false" />
          <windowsAuthentication enabled="true" />
        </authentication>
      </security>
    </system.webServer>
    <system.web>
        <identity impersonate="true" />
    </system.web>
</configuration>
```

Not That Simple

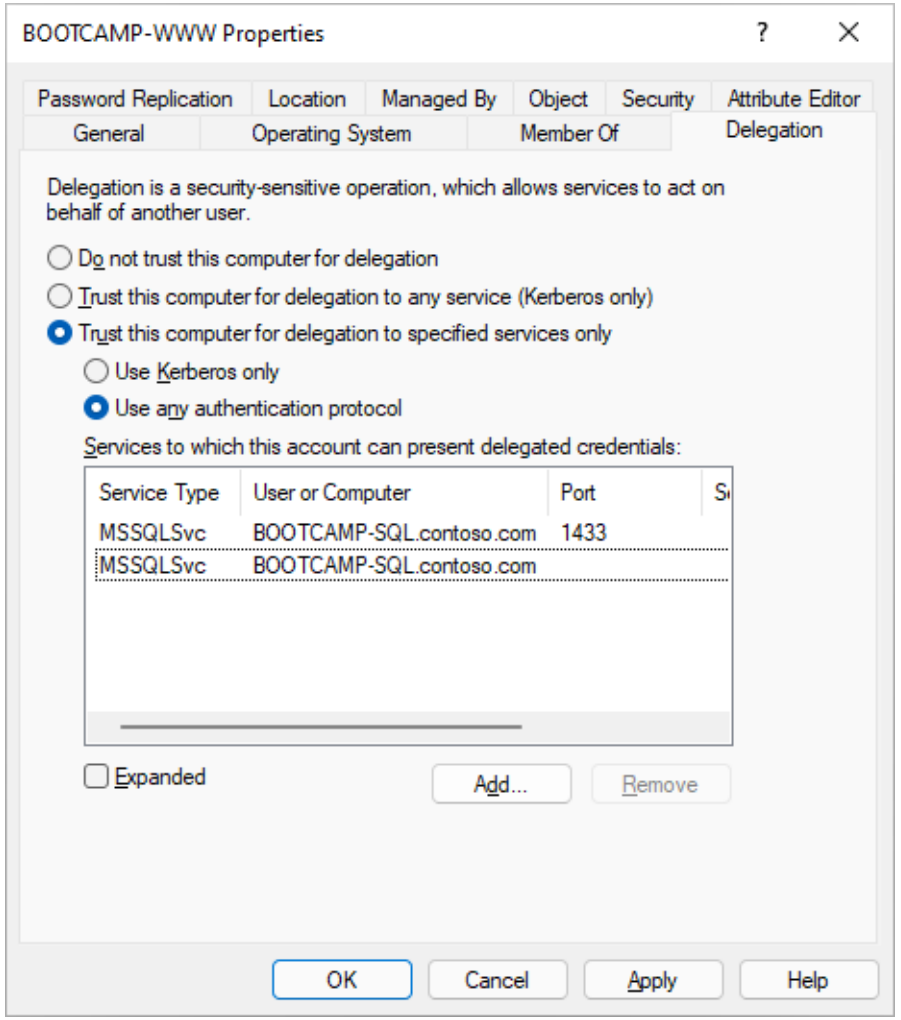


Kerberos Constrained Delegation

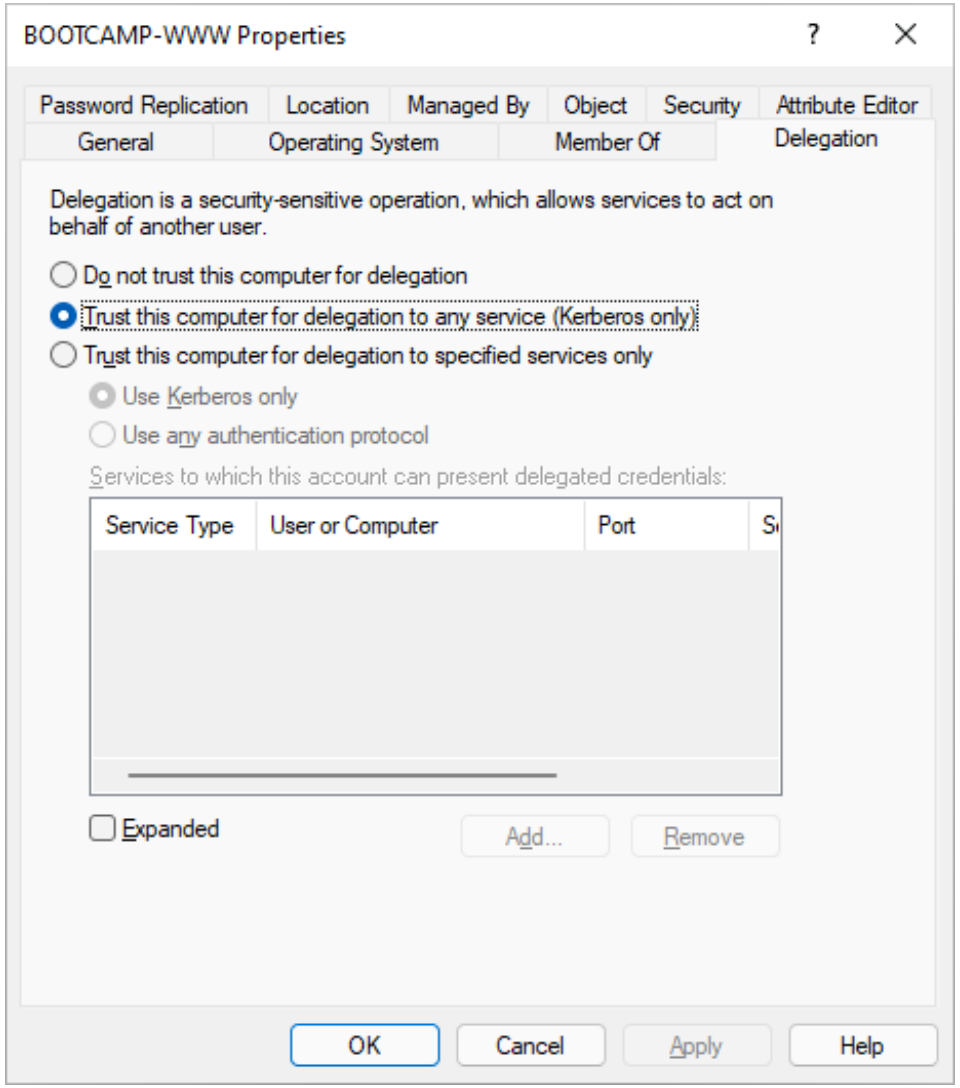


DEMO: Kerberos Delegation

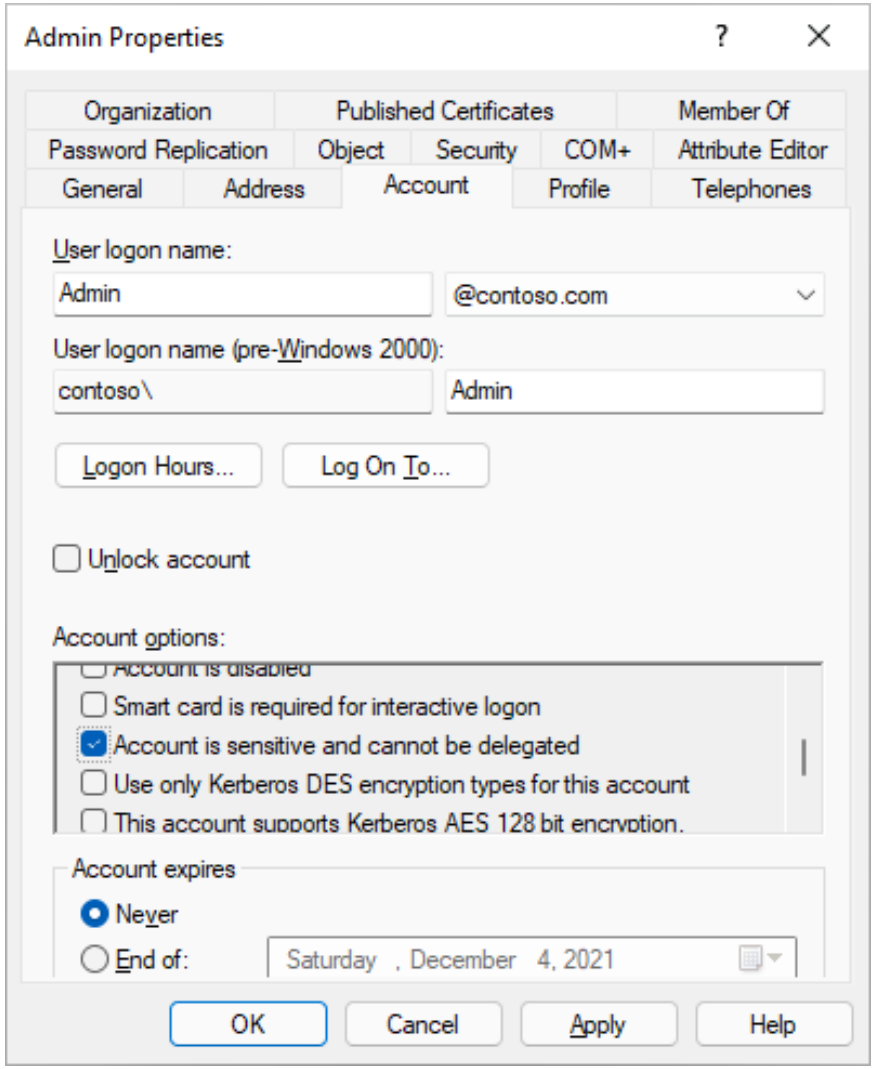
Protocol Transition Security Risks



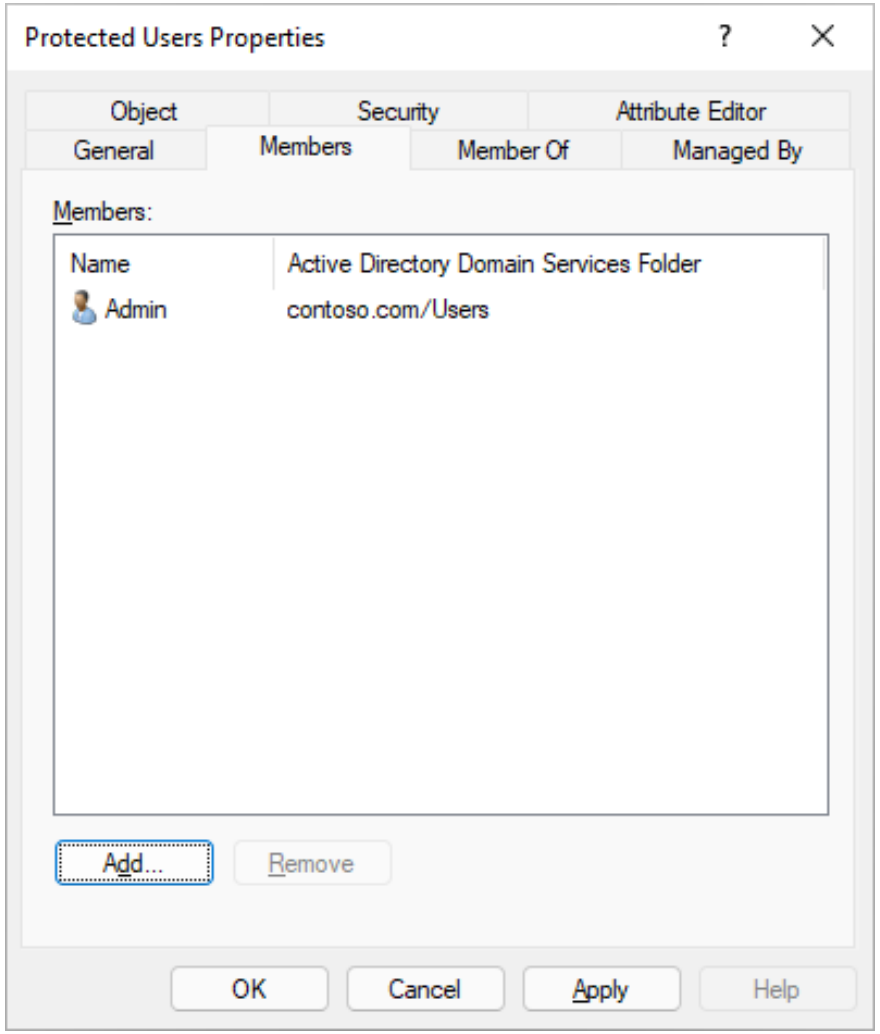
Unconstrained Delegation Security Risks



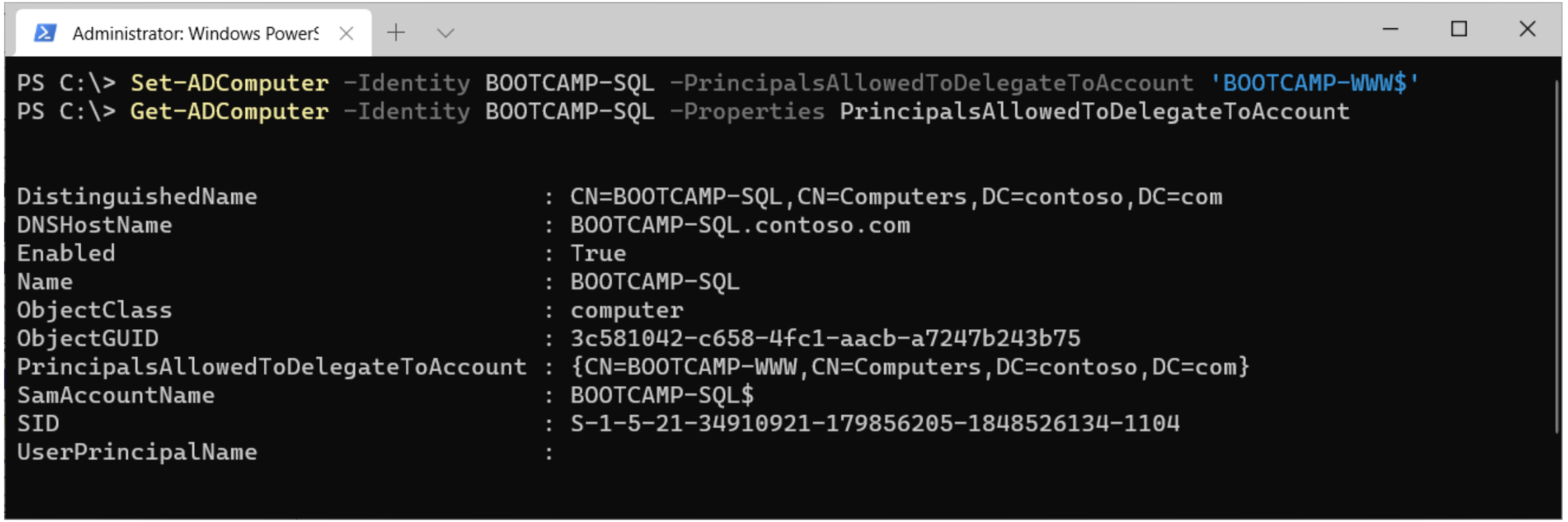
Per-Account Countermeasure



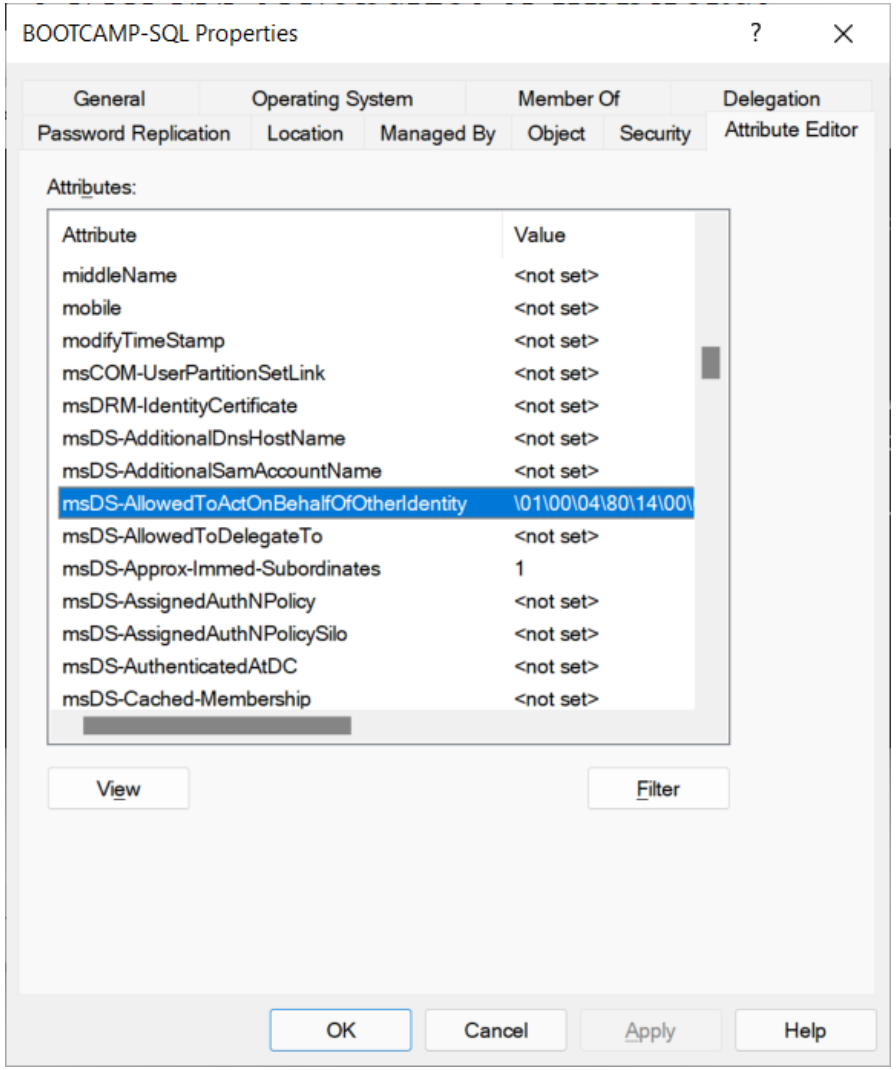
Countermeasure – Windows Server 2012 AD



Resource-Based Constrained Delegation

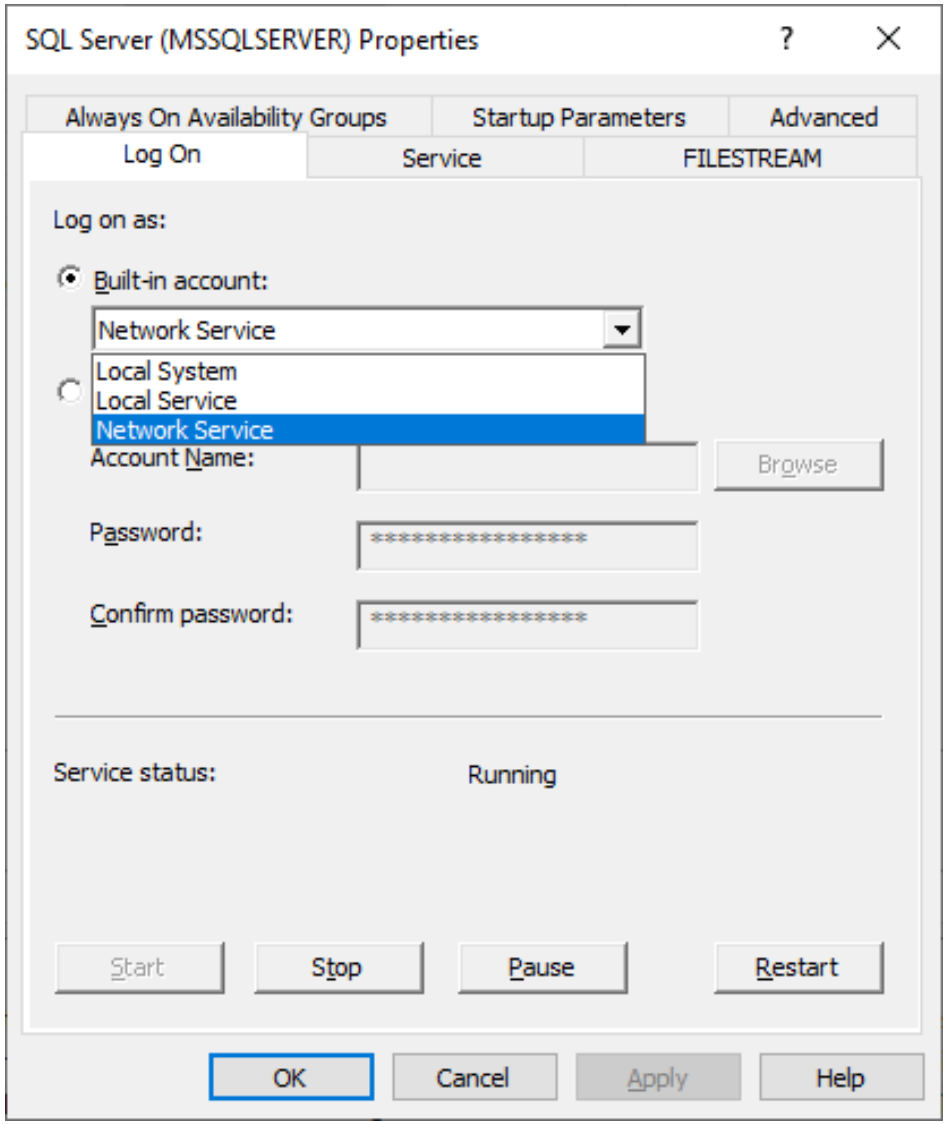


Resource-Based Constrained Delegation

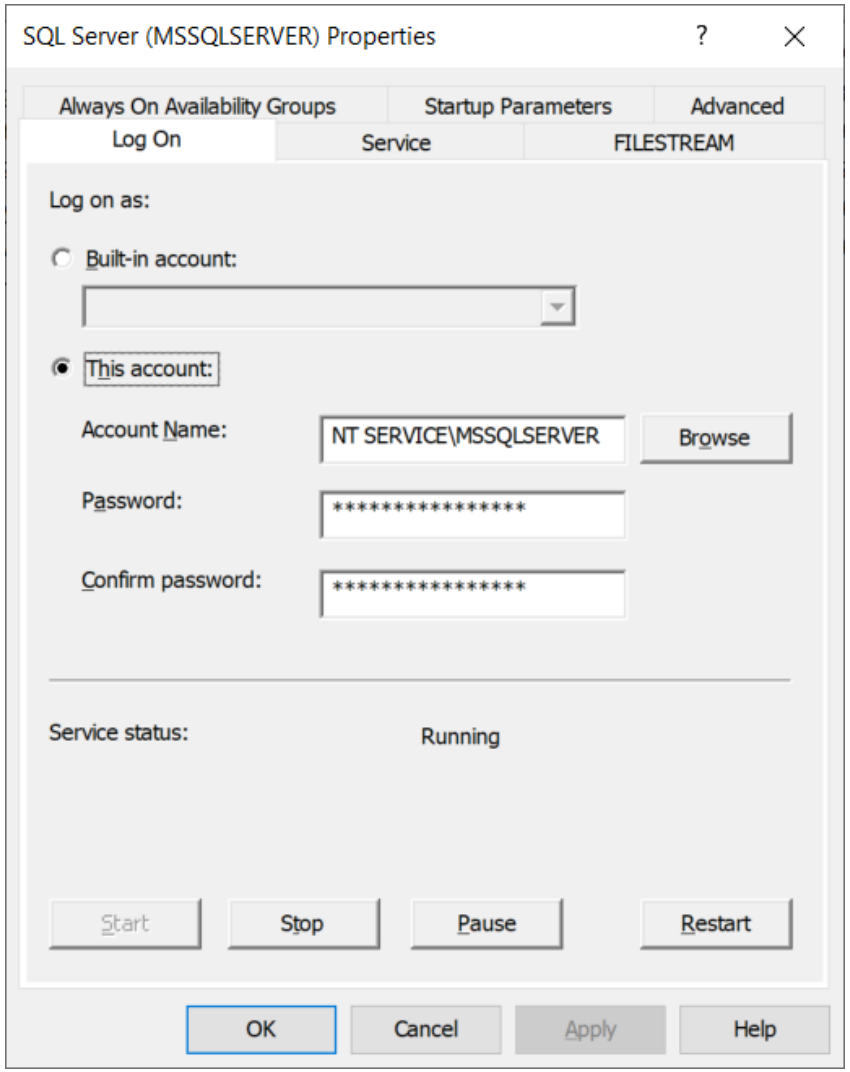


SQL Server Identity

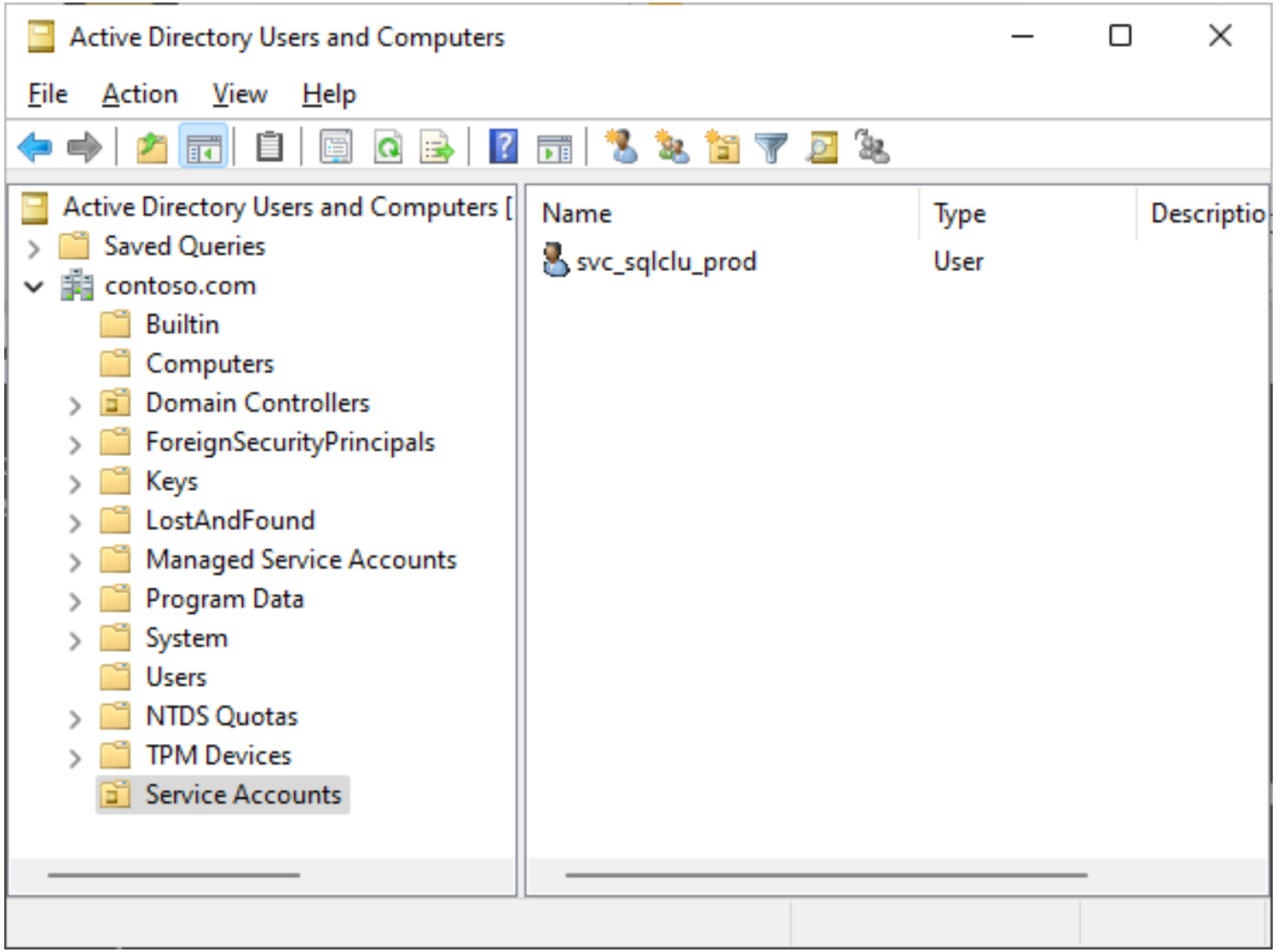
Built-In Identities



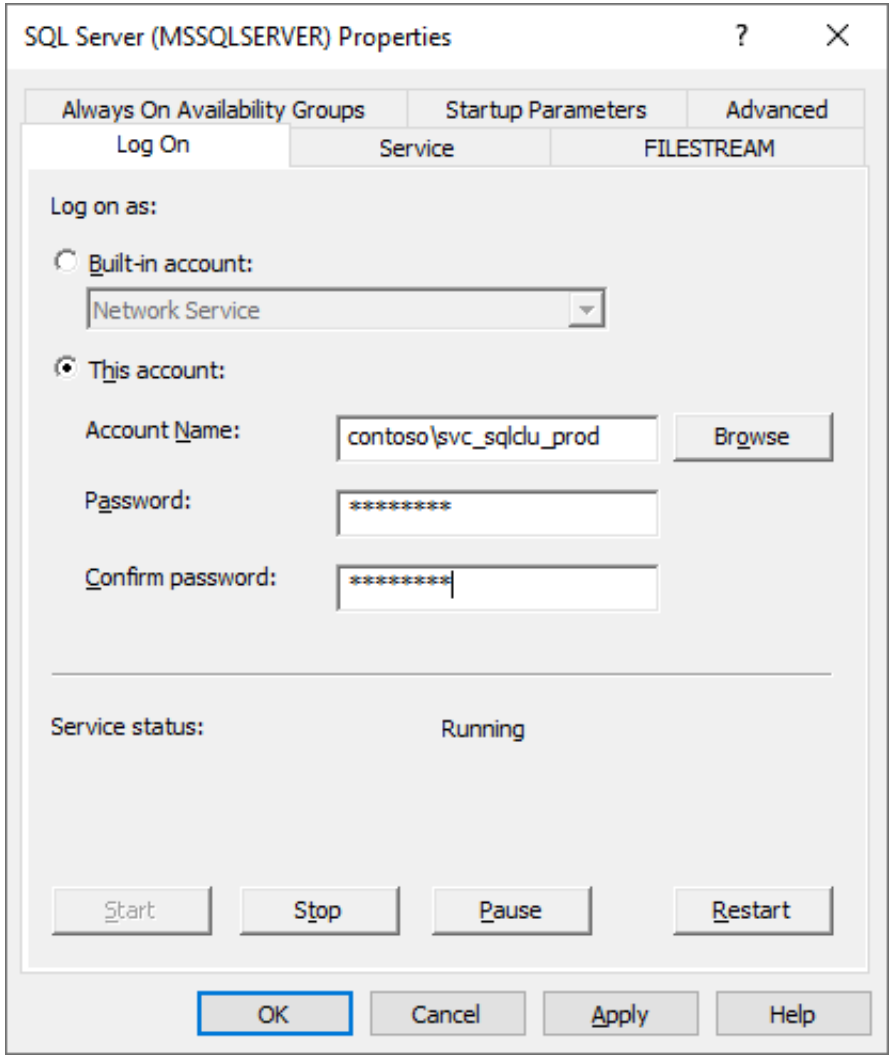
Virtual Service Account



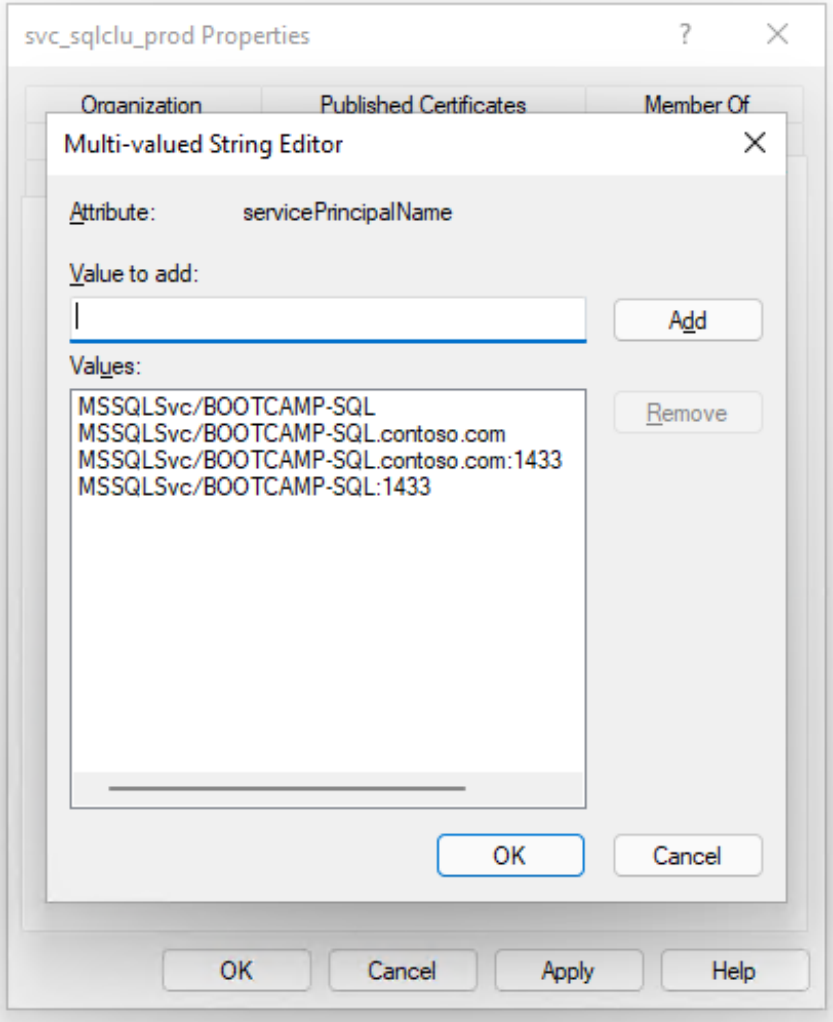
Dedicated Service Accounts



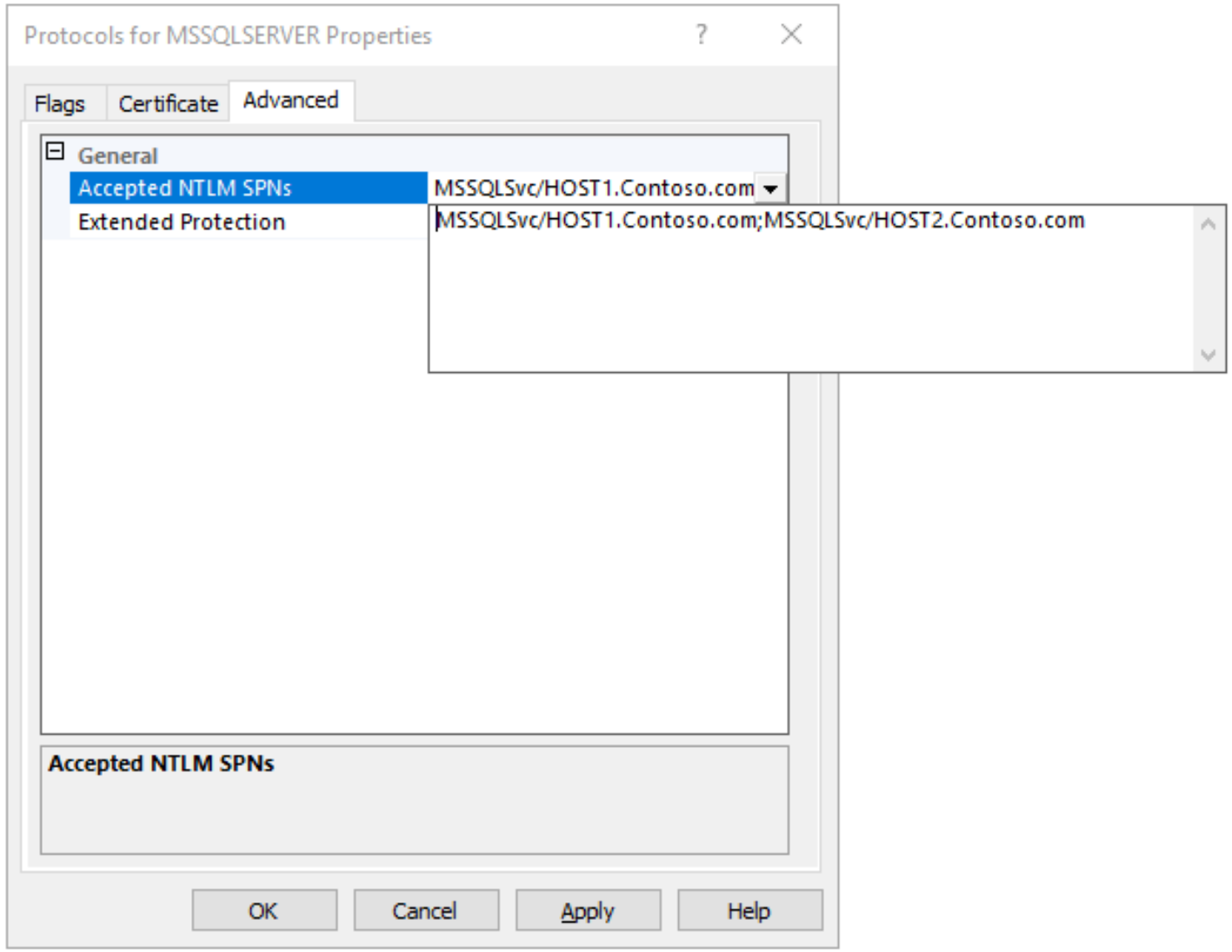
Dedicated Service Accounts



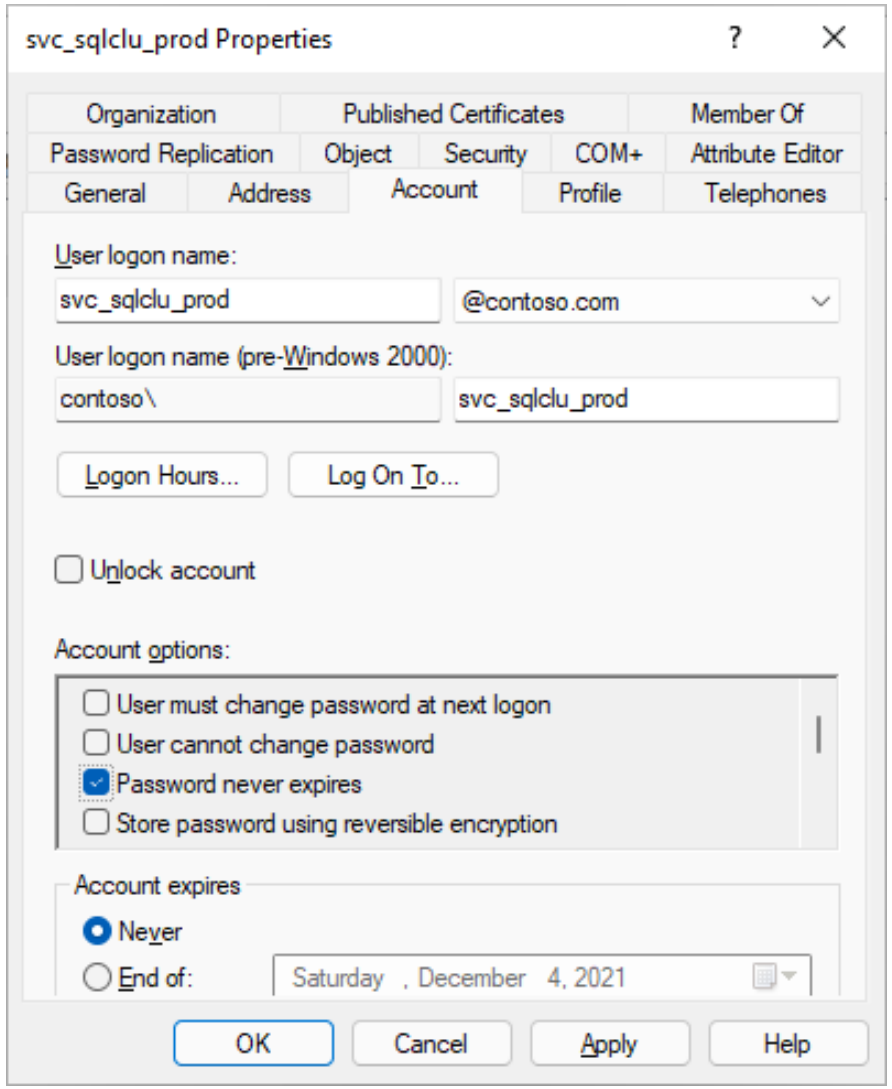
Manual Service Principal Name Management



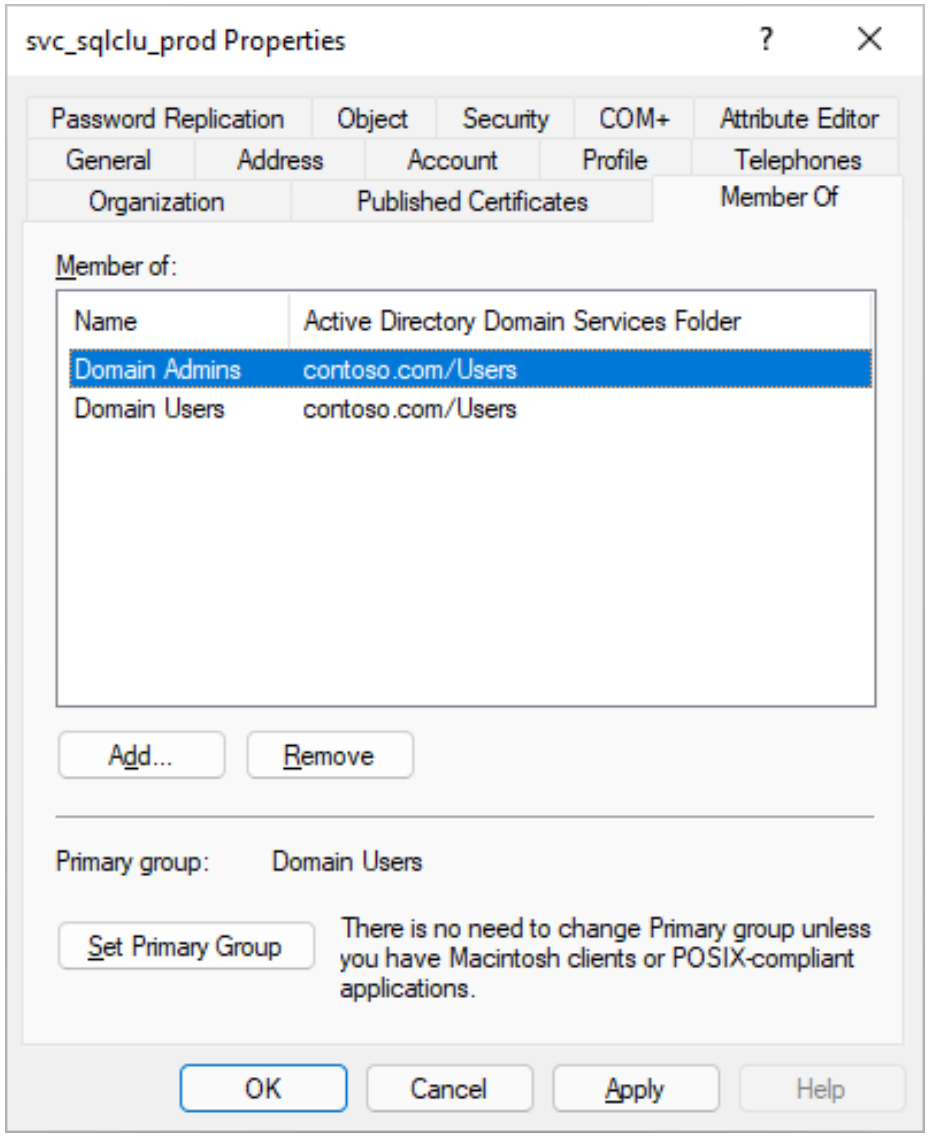
Accepted SPNs



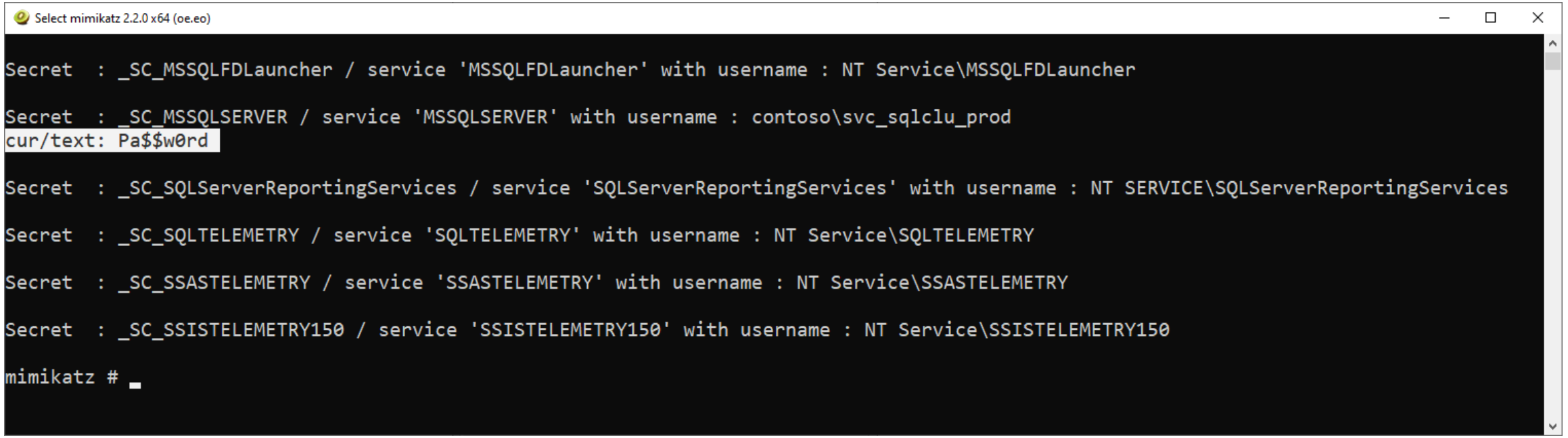
Risk of Permanent Passwords



Risk of Over-Privileged Service Accounts

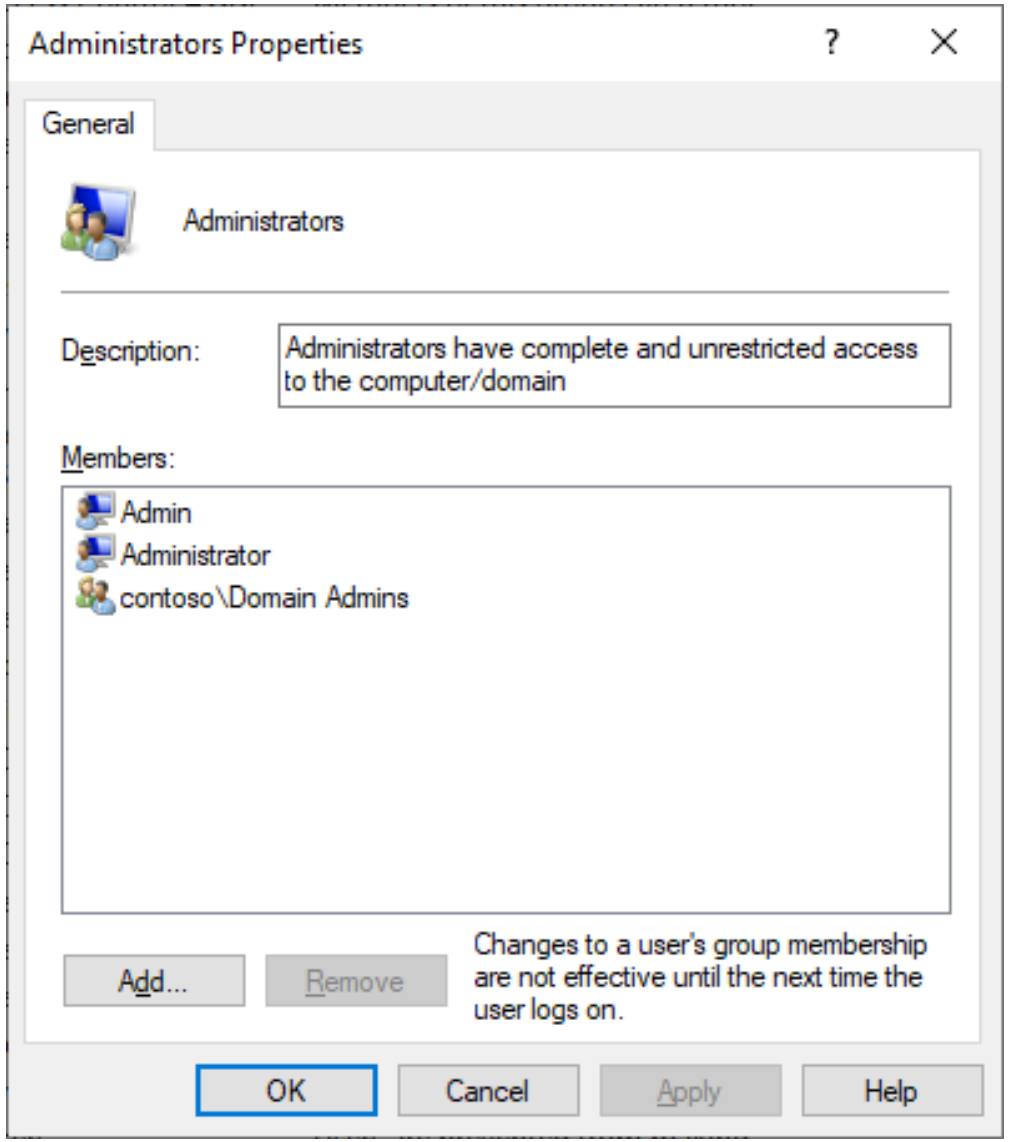


Risk of Credential Harvesting

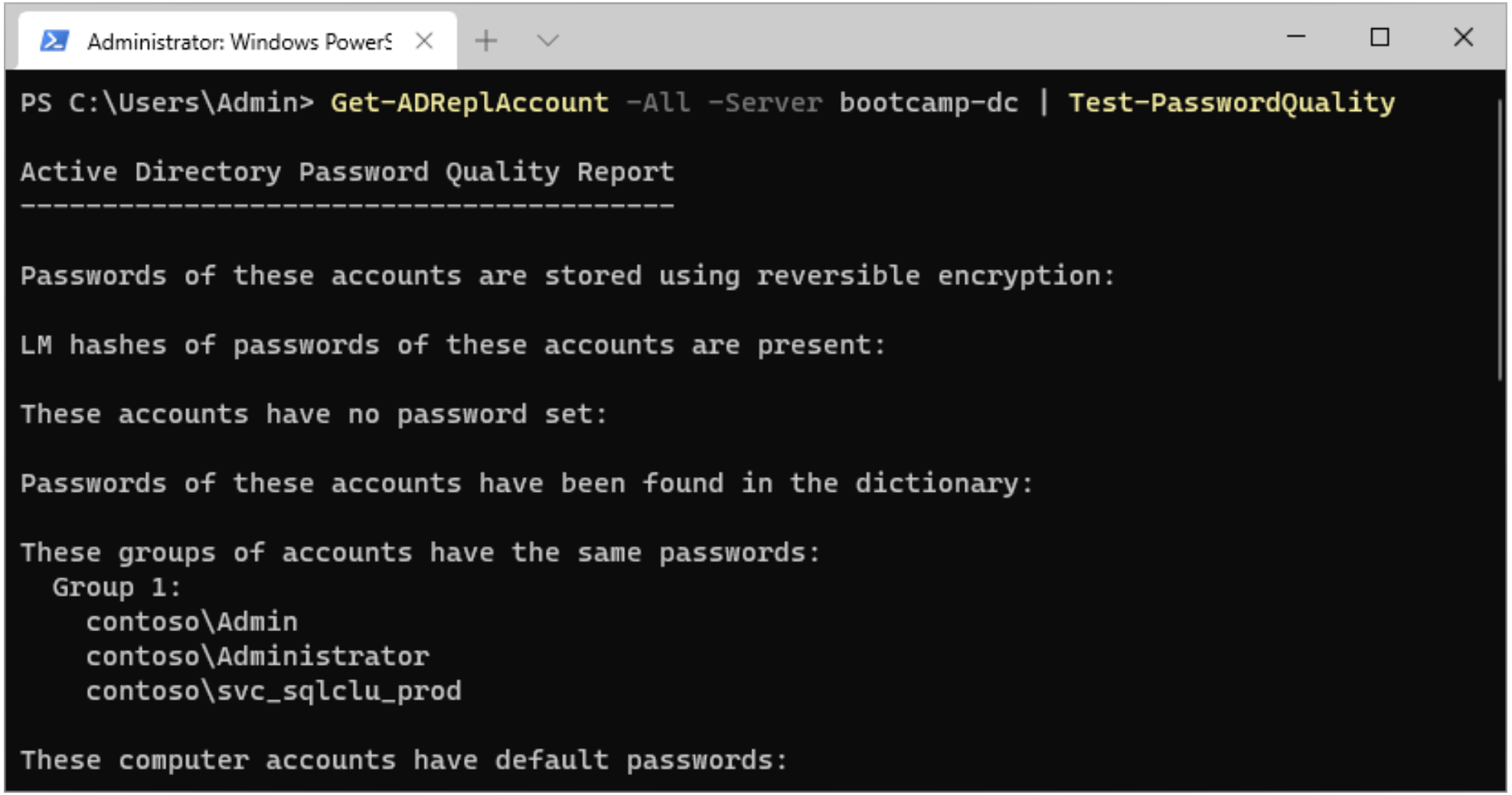


DEMO: Dumping Service Credentials

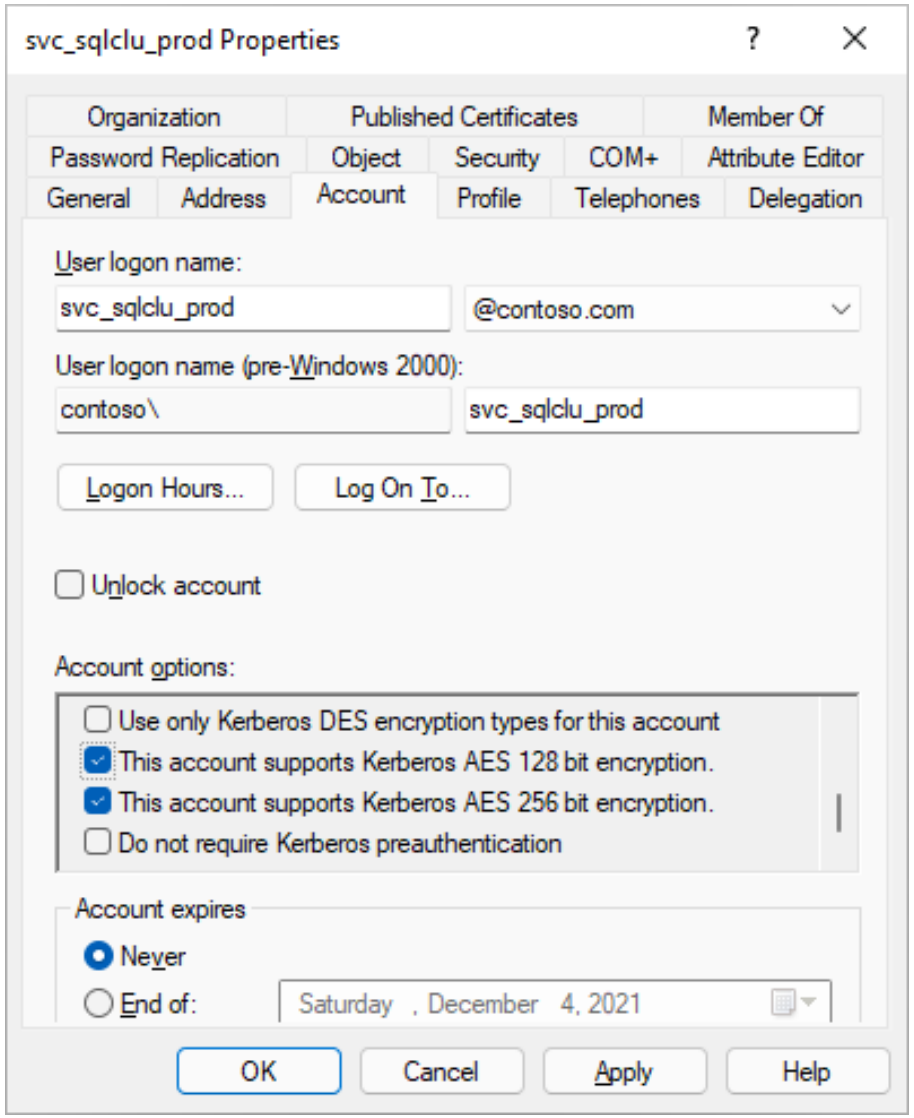
Credential Harvesting Permissions



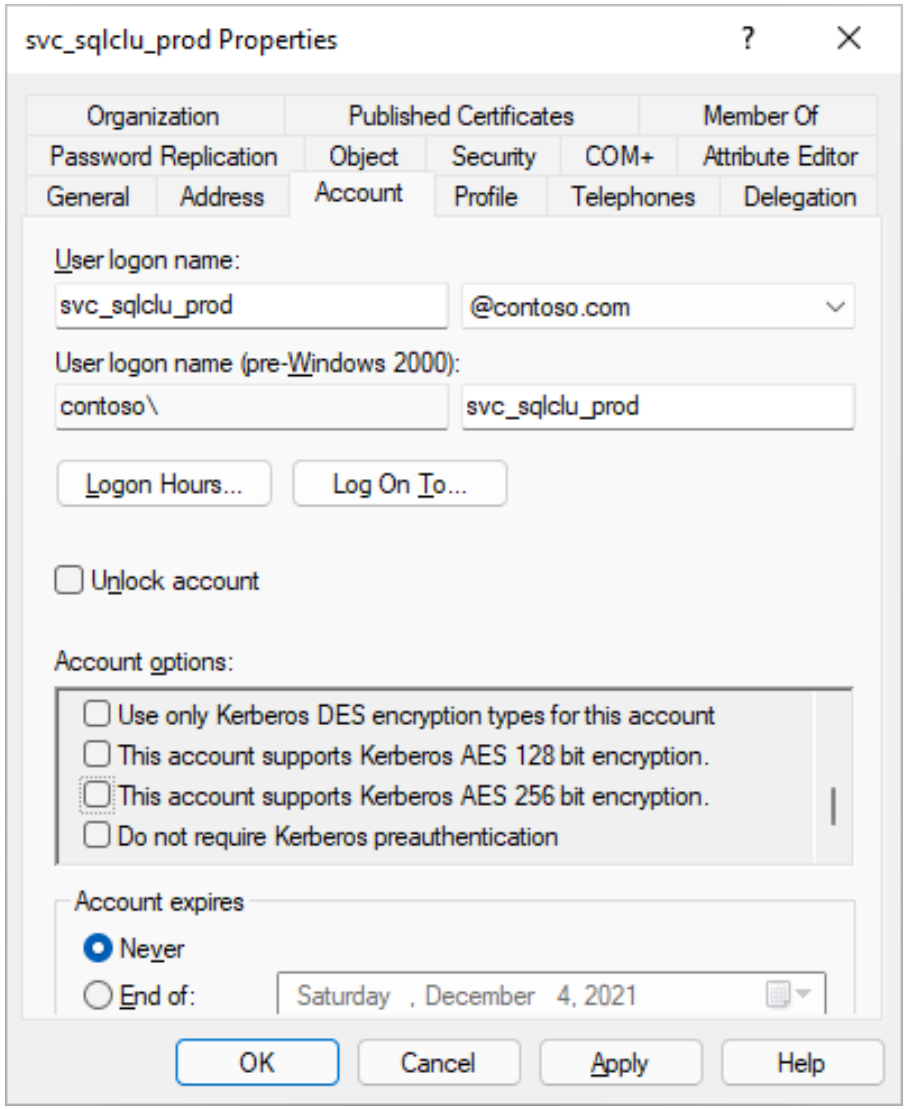
Risk of Credential Reuse



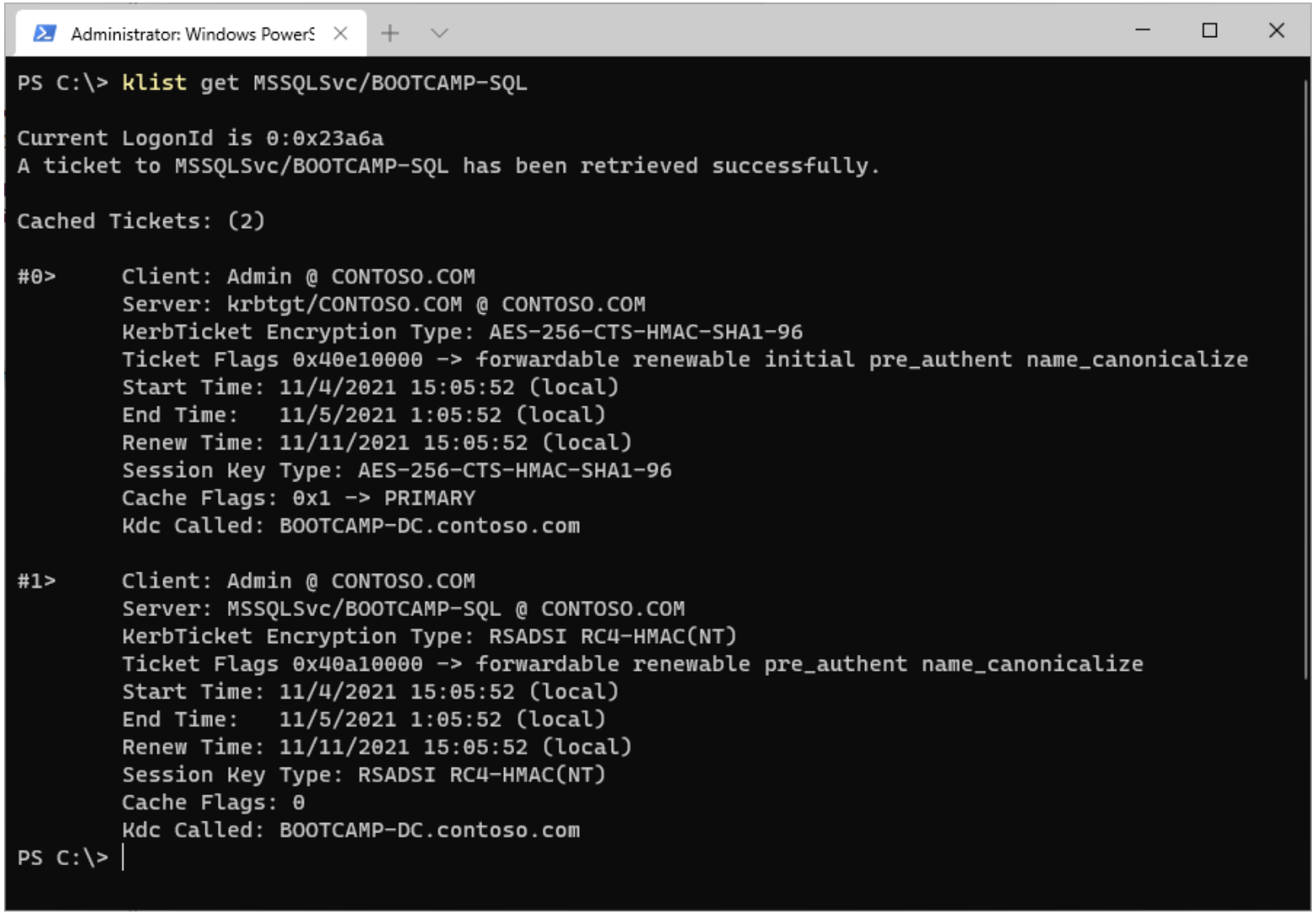
Configuring Kerberos Encryption Types



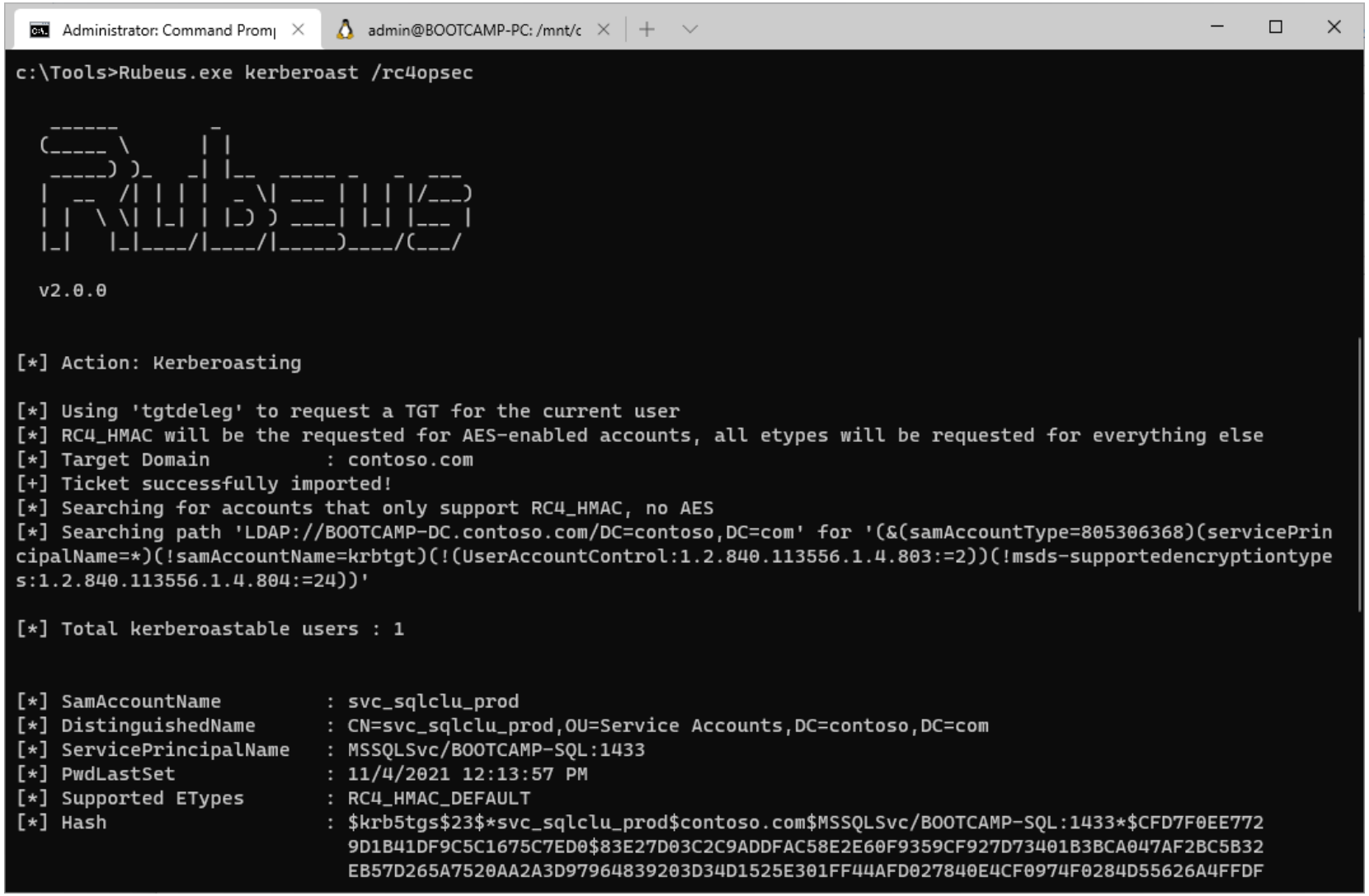
Misconfigured Kerberos Encryption Types



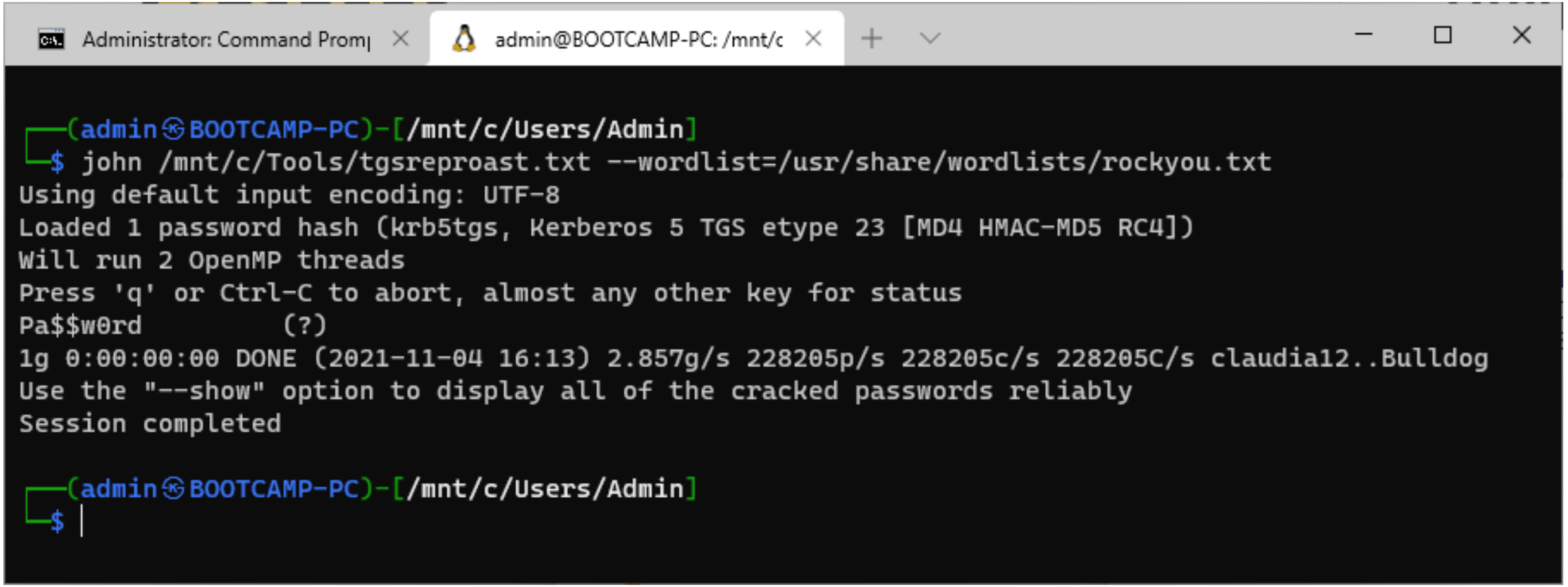
Kerberos RC4 Encryption



Kerberoasting Attack

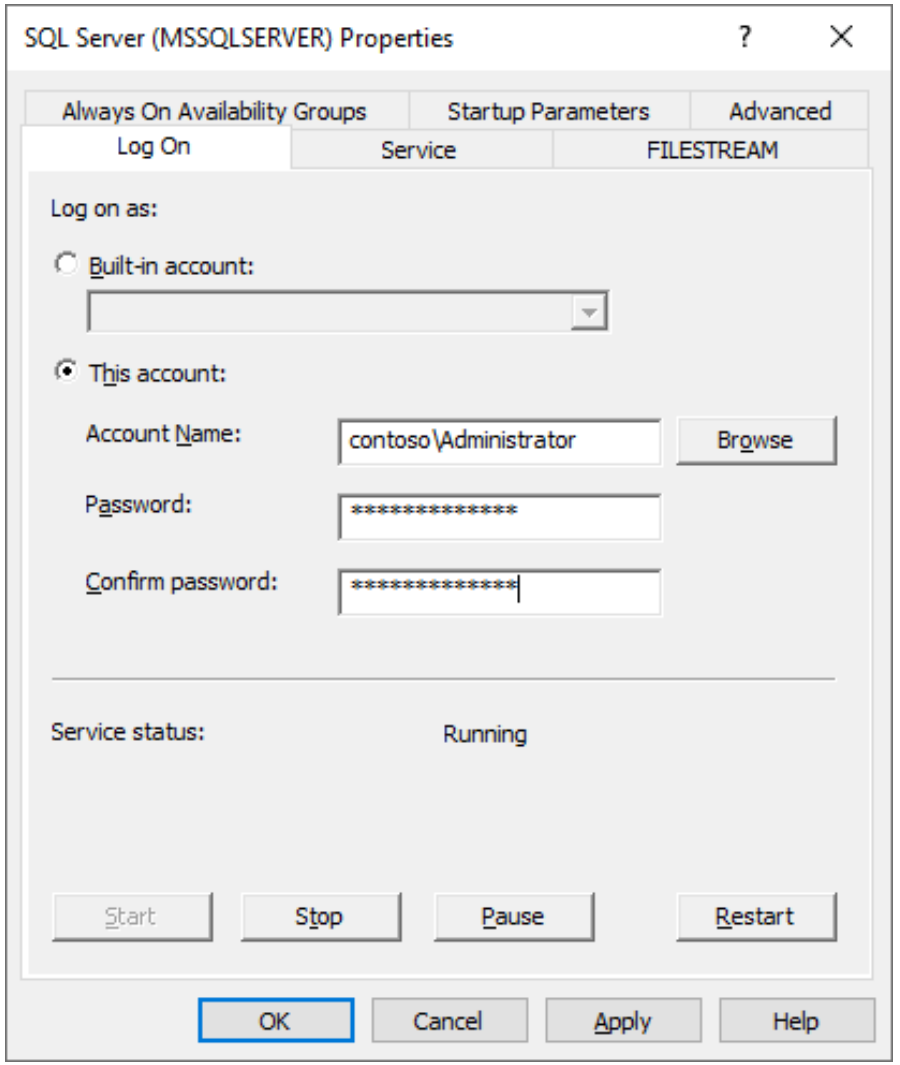


Kerberoasting Attack

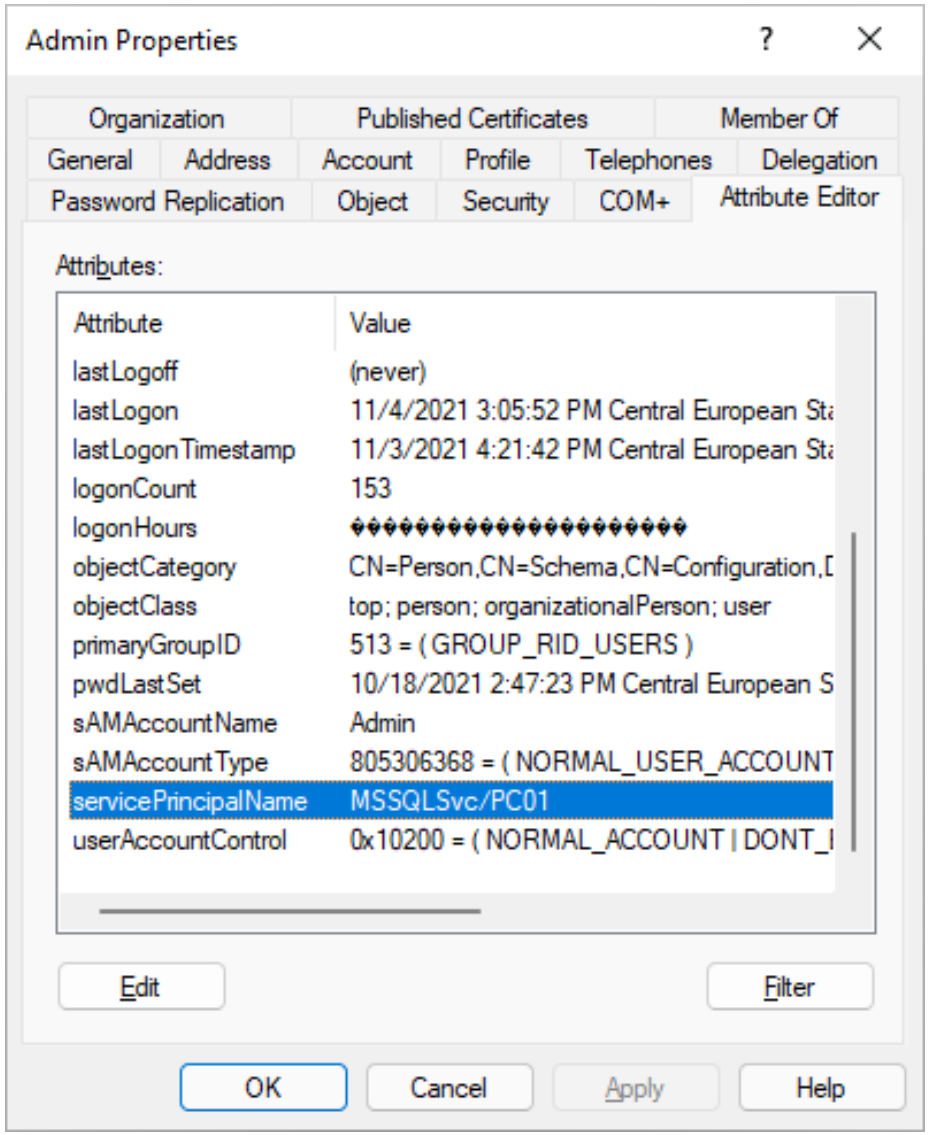


DEMO: Kerberoasting

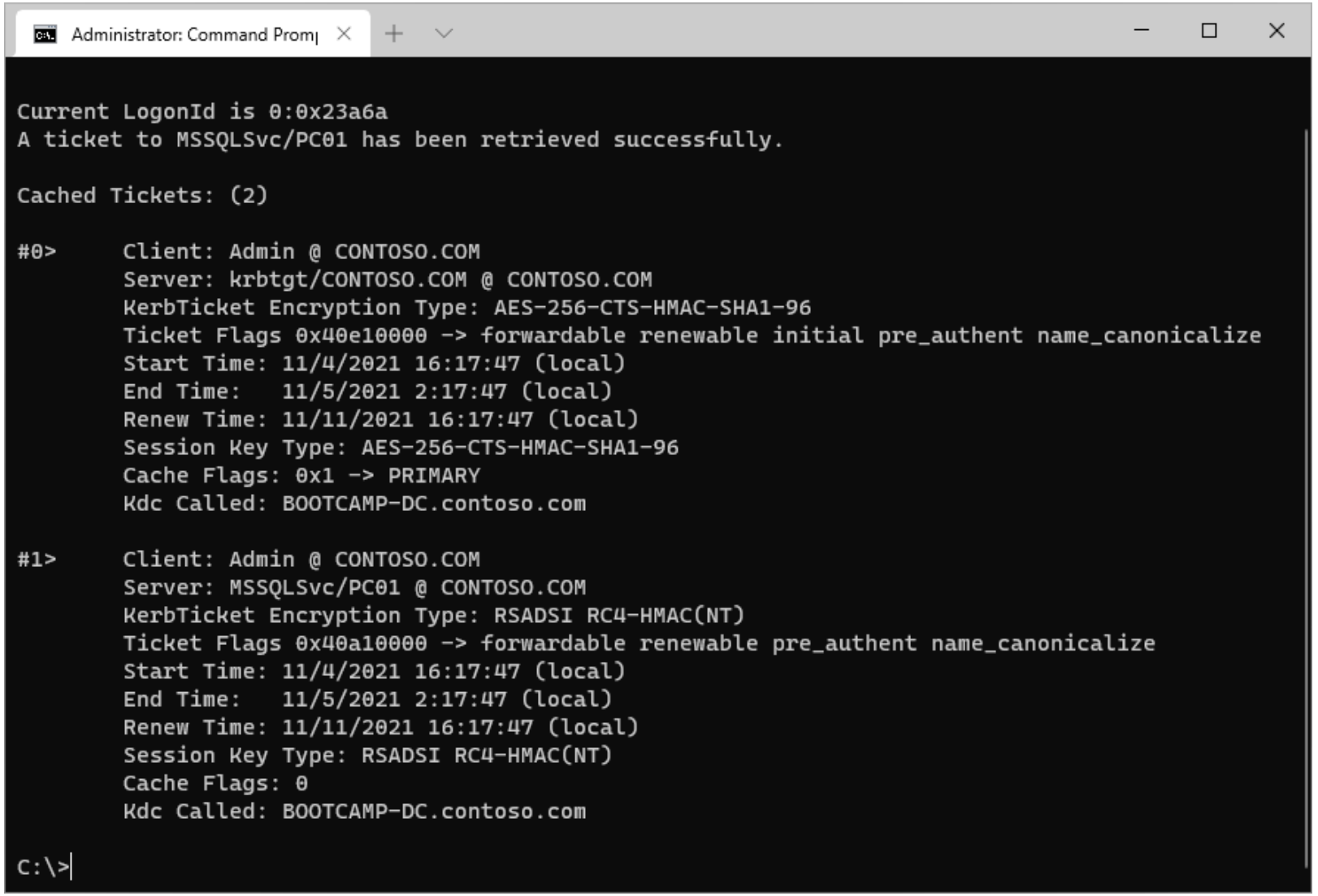
Mayhem: Misconfigured Service Identity



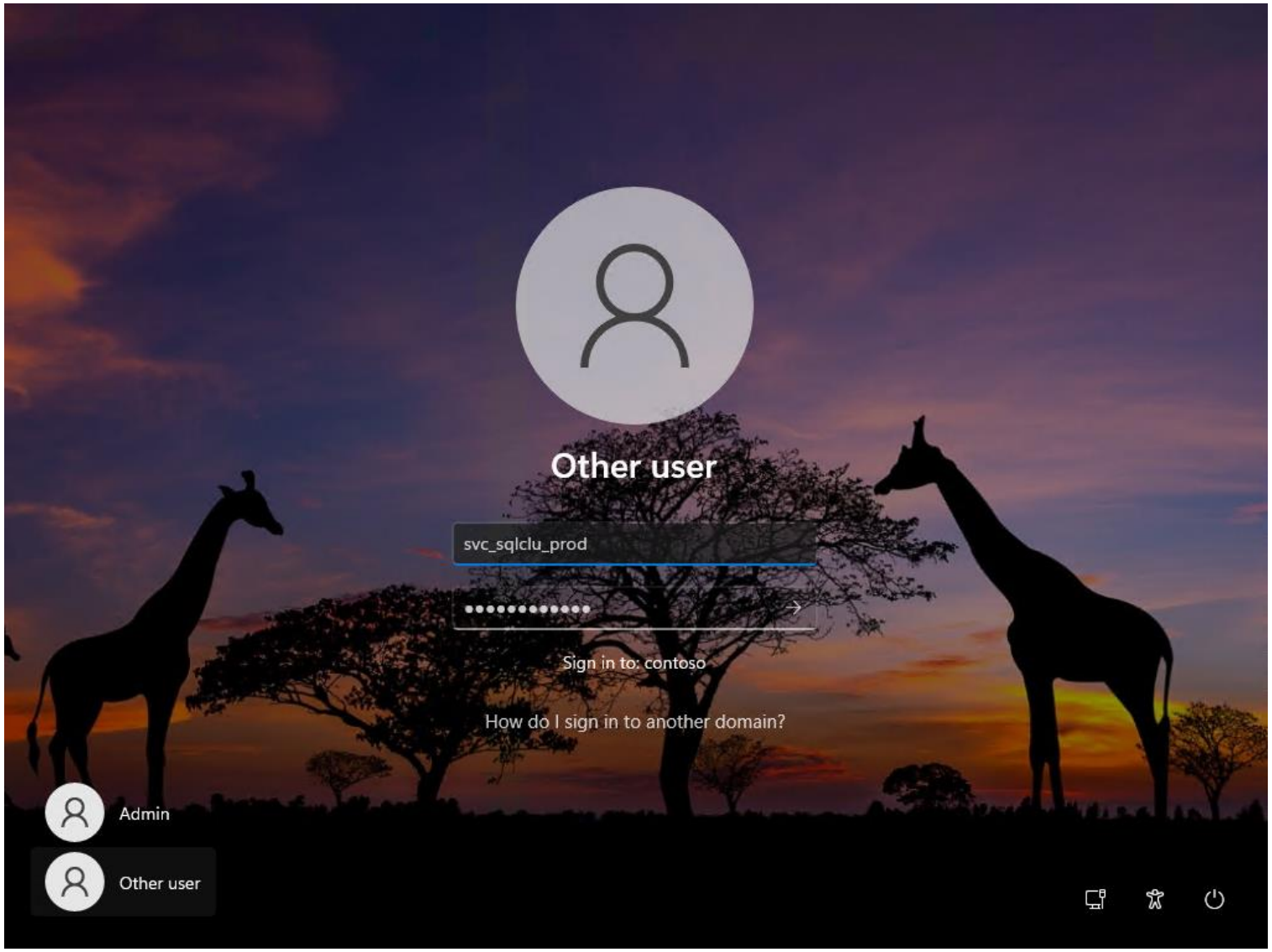
Mayhem: Misconfigured Service Identity



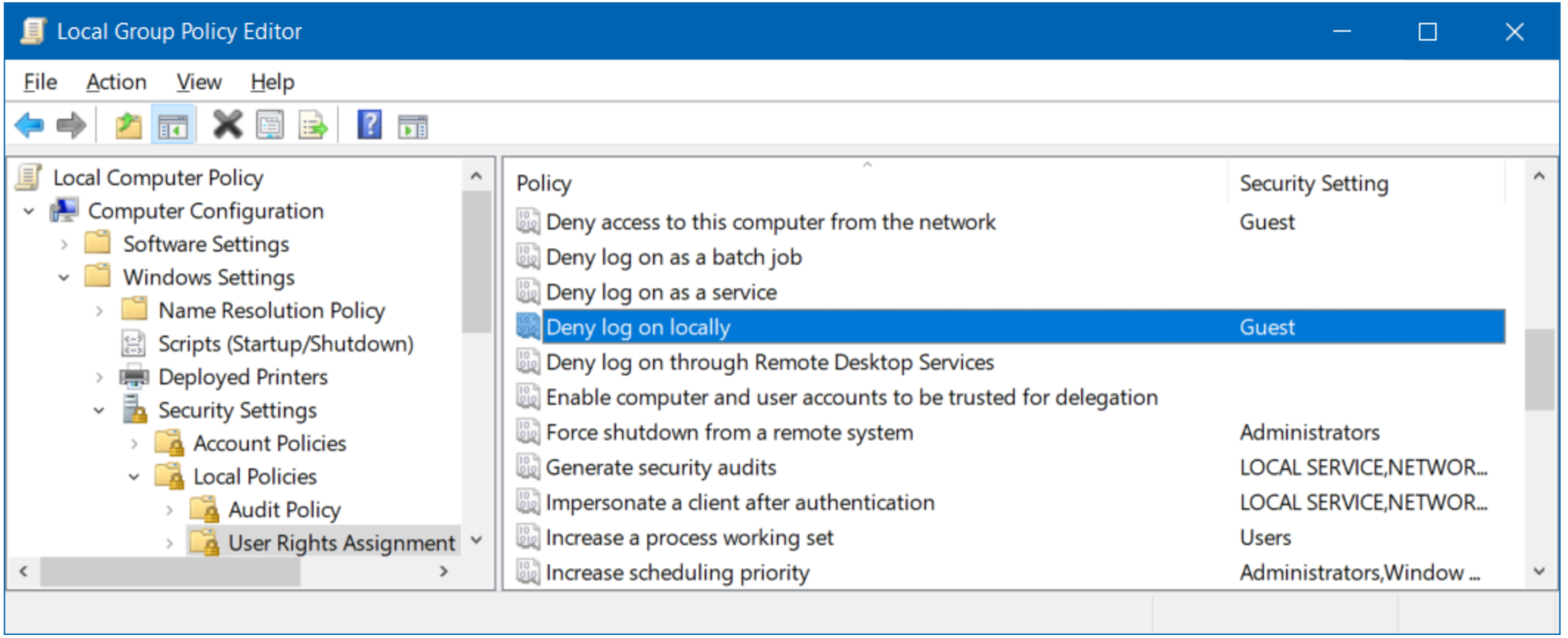
Mayhem: Misconfigured Admins



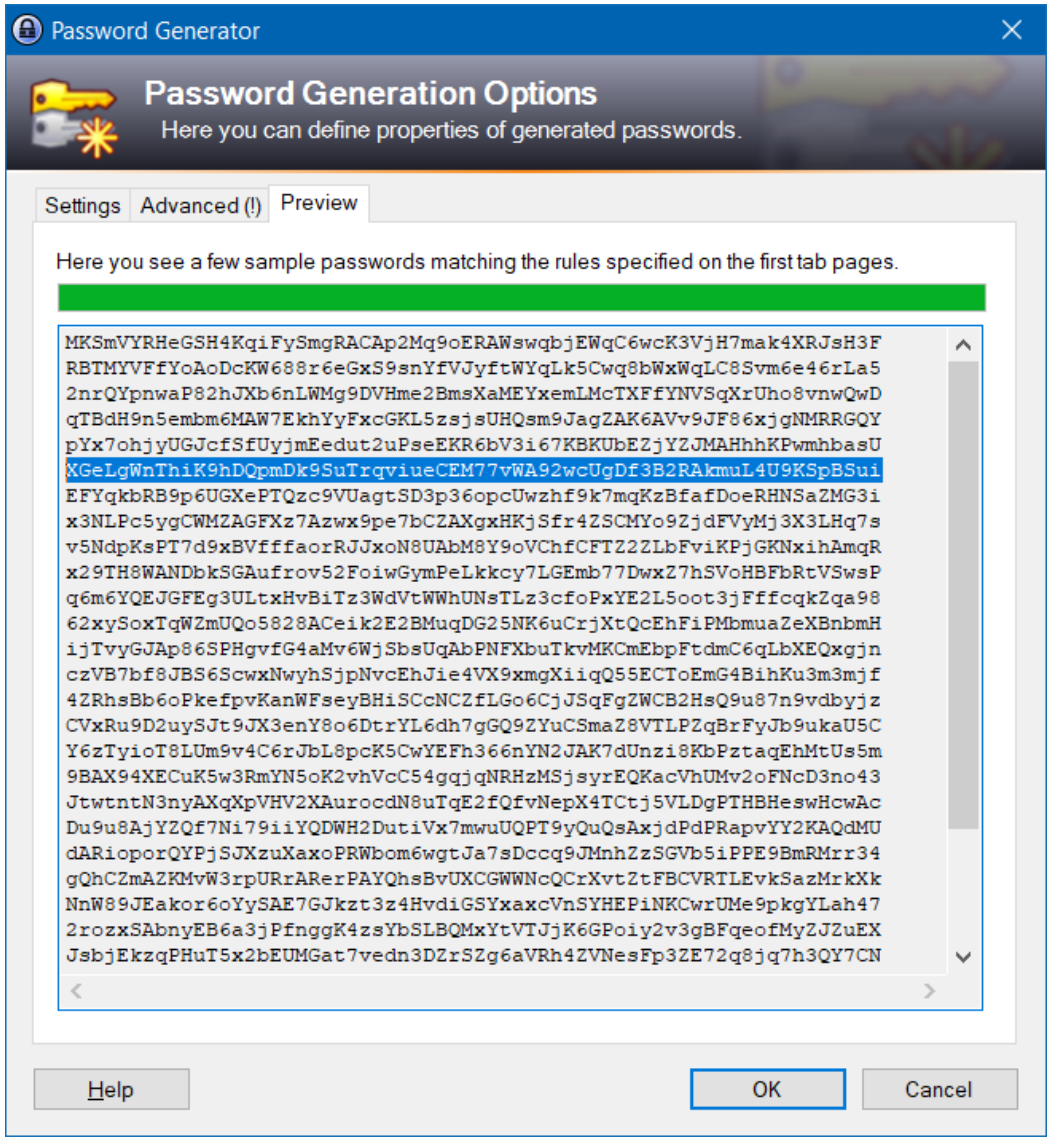
Risk of Interactive Logon



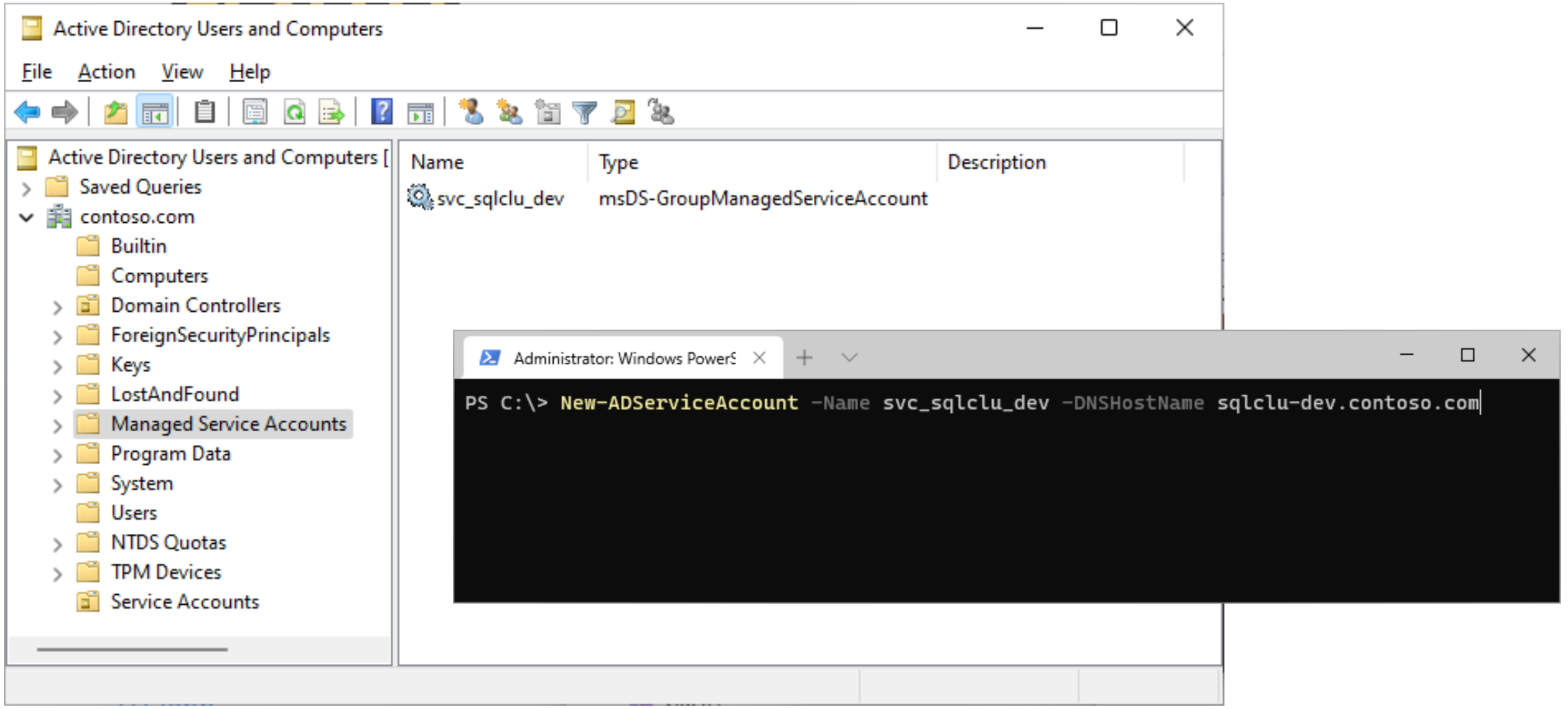
Countermeasure: Deny Logon



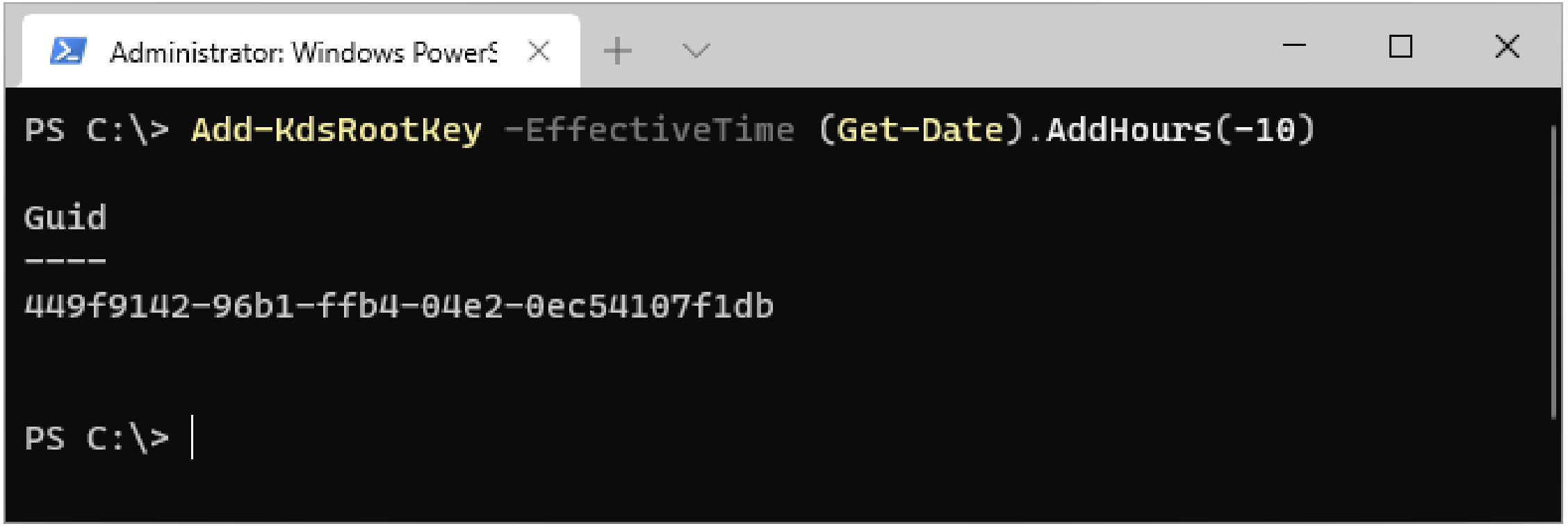
Always Use Password Generators



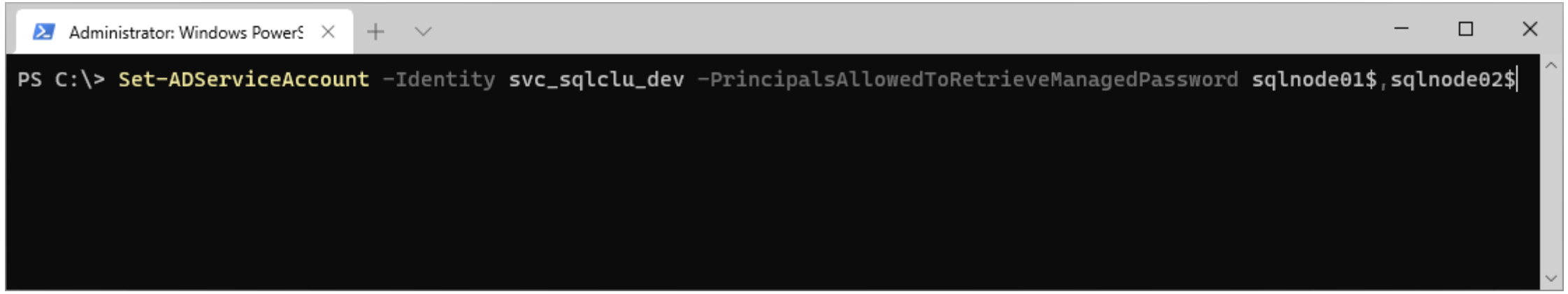
Group Managed Service Accounts



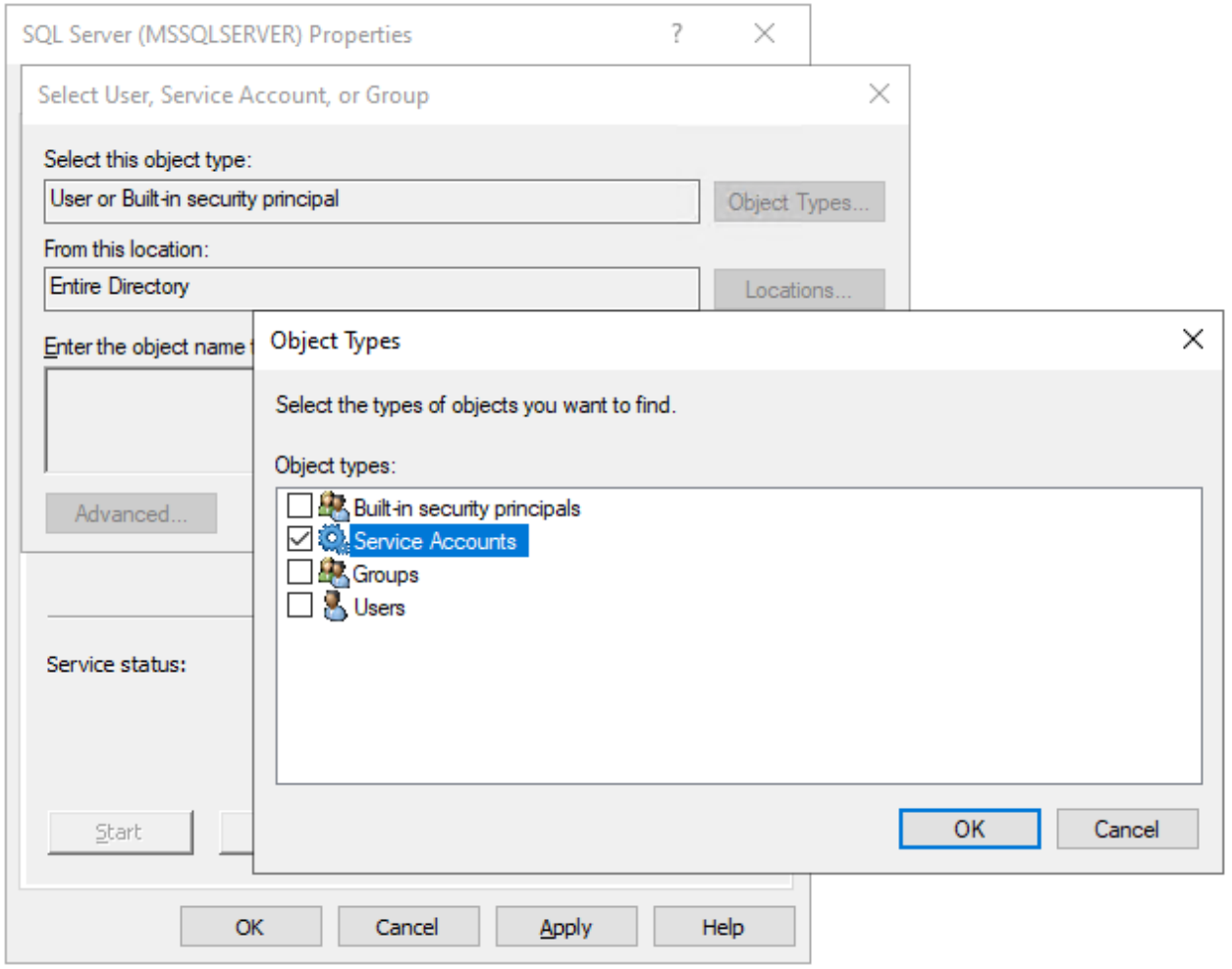
GMSA Requirement: KDS Root Keys



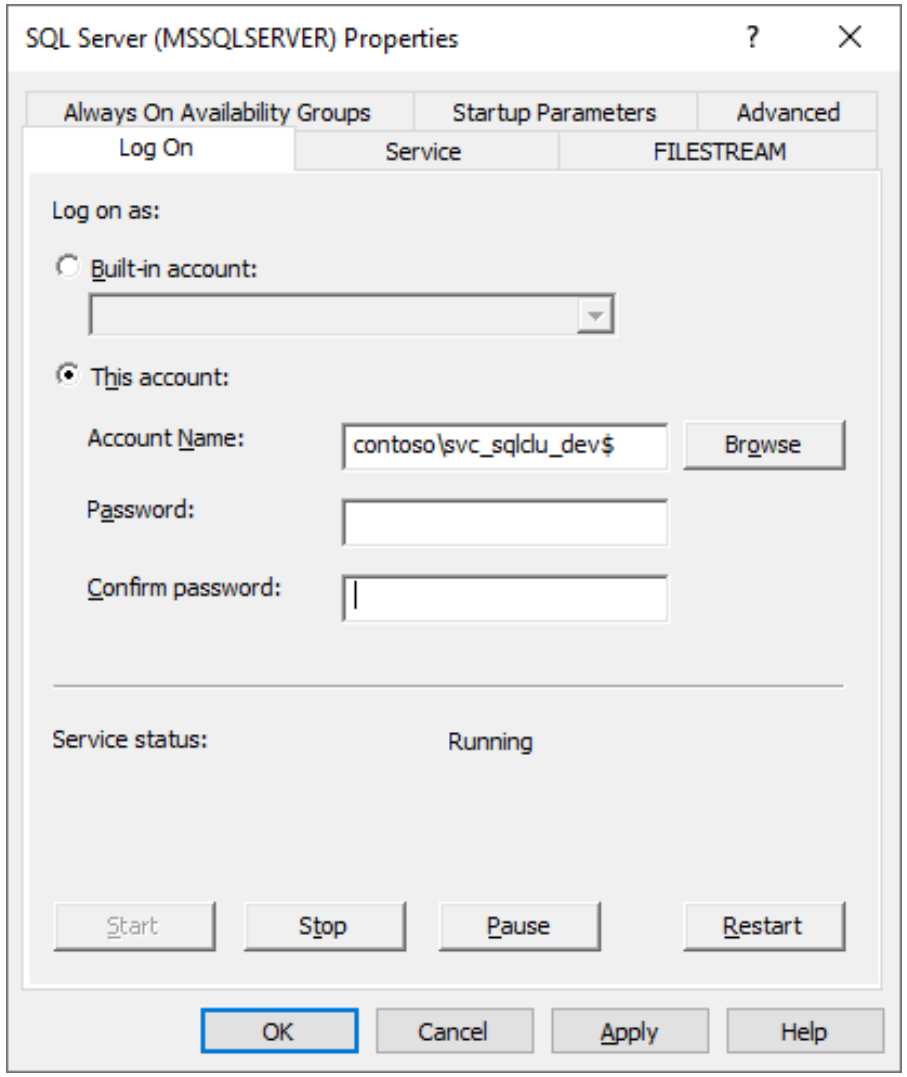
Managed Password Retrieval



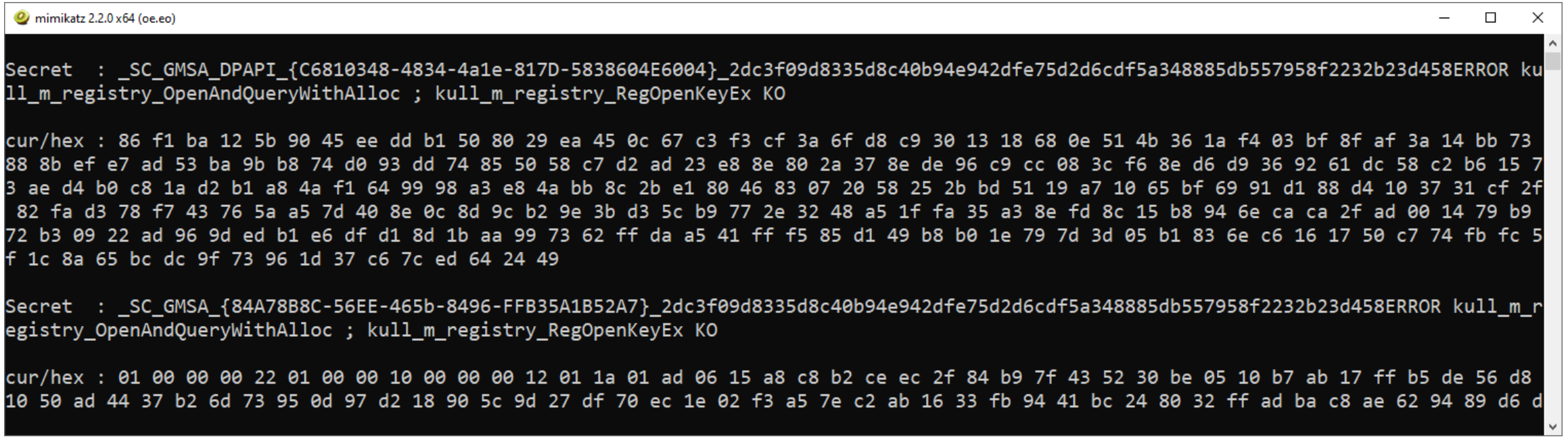
Configuring SQL Server for GMSA



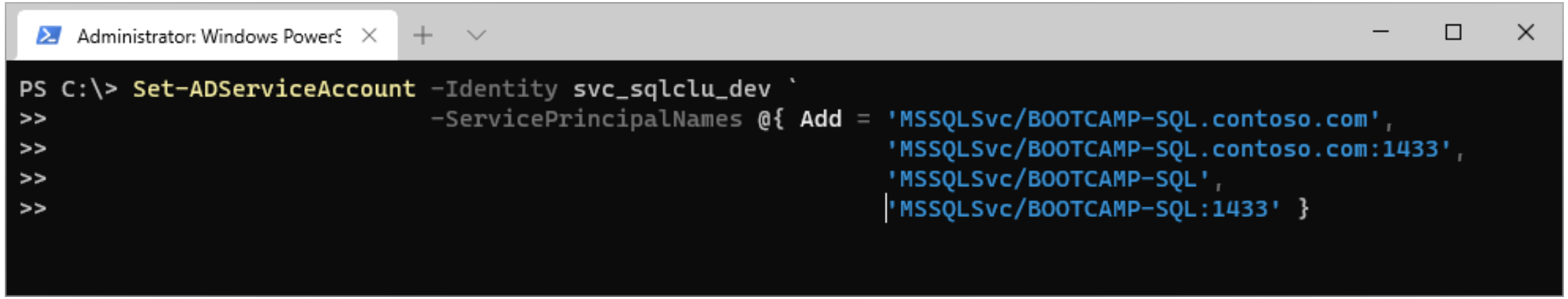
Automatic Password Management



Password Still There



Service Principal Names



DEMO: GMSA

Note: Linked Servers

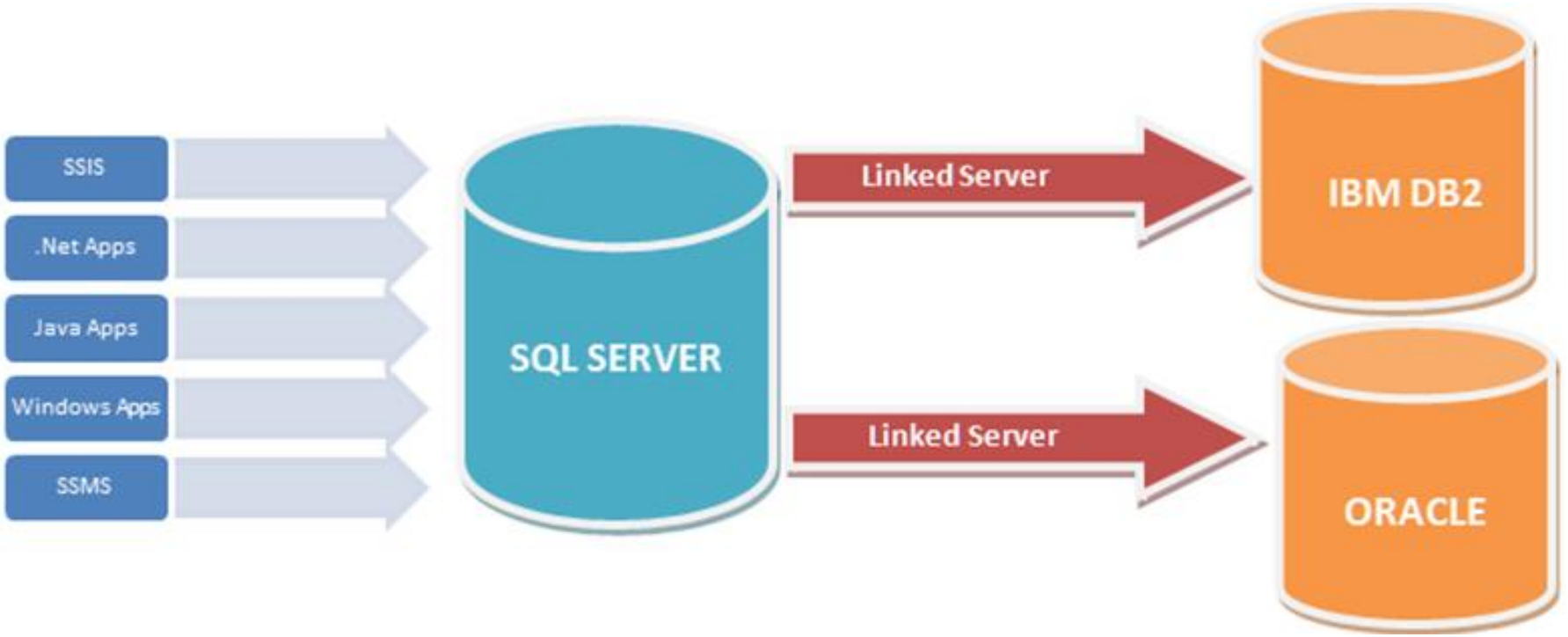
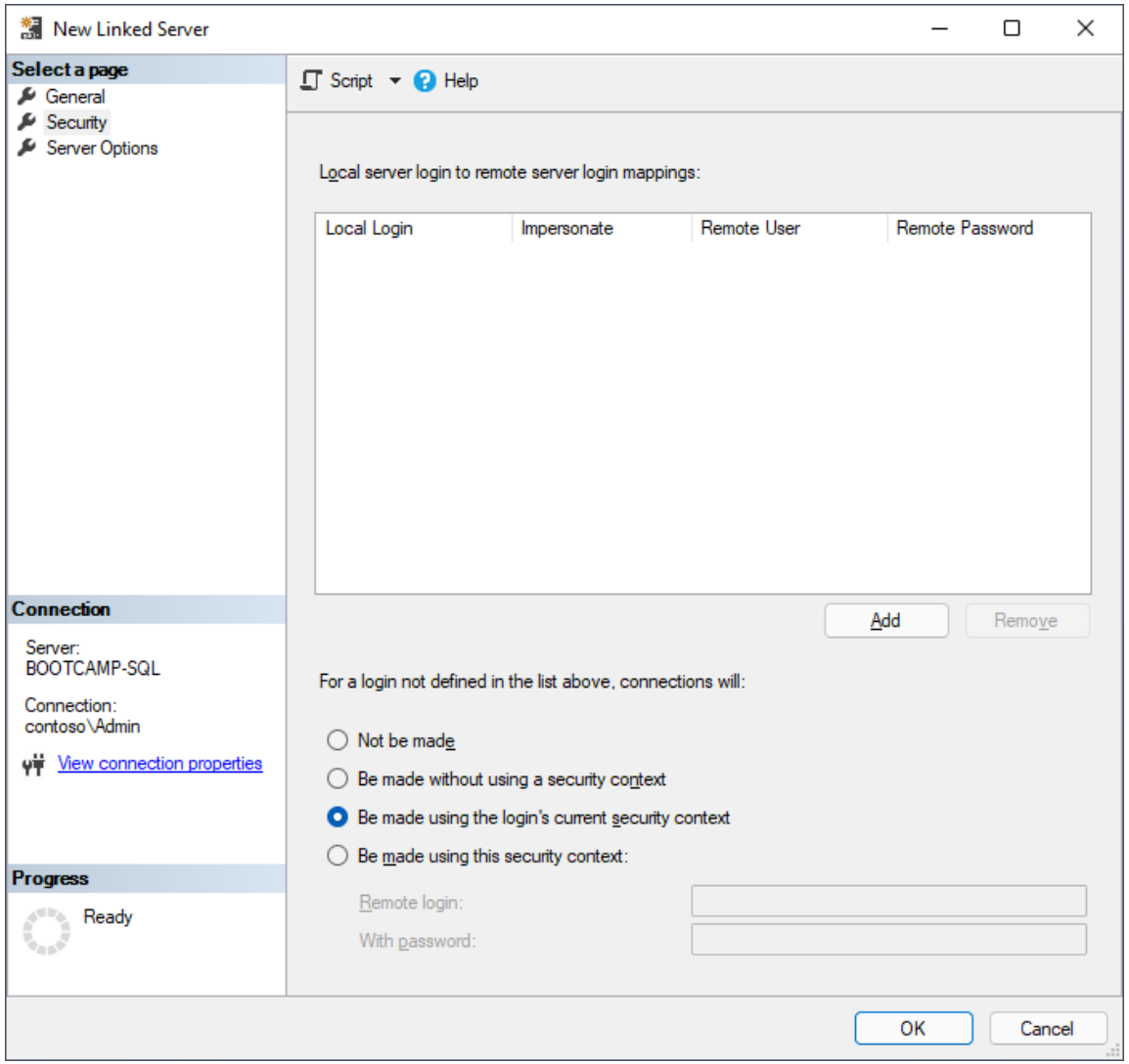


Image Source: https://techcommunity.microsoft.com/t5/sql-server-support/linked-server-performance-heterogeneous-databases/ba-p/316167

Note: Linked Servers



SQL Server
Windows Authentication Internals

Mgr. Michael Grafnetter
MVP | MCT
michael.grafnetter@outlook.com
@MGrafnetter