

SQL KONFERENZ 2026

SQL KONFERENZ 2026



Unveiling the new security features in SQL Server 2025

Pieter Vanhove

Senior Product Manager - Microsoft

SQL KONFERENZ 2026

Agenda



- Entra Authentication
- Crypto Updates
- Other Security Enhancements

Entra Authentication

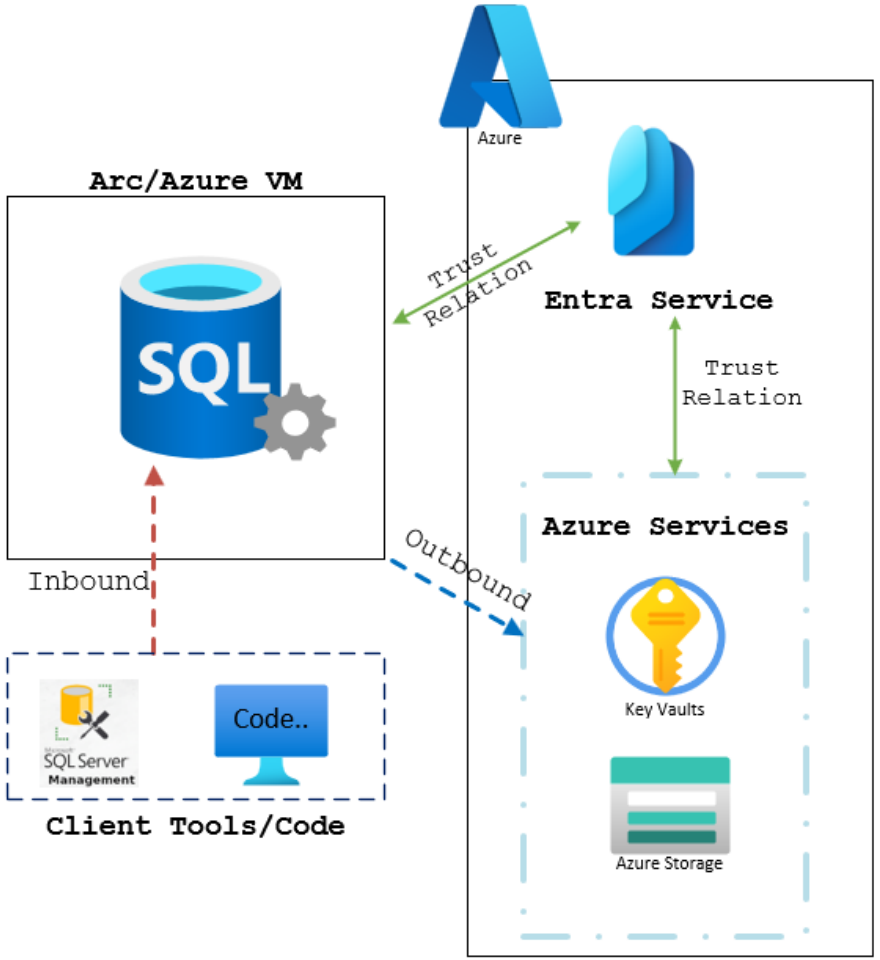
Entra Features in SQL Server 2025 on Arc (Windows)

Inbound

- Simplifying setup with primary managed identity
- Use of Object_Id for duplicate Entra names

Outbound

- Create Credential T-SQL can support ‘managed Identity’
- Backup to URL & TDE with EKM, using managed identity



Entra Features in SQL Server 2025 on Arc (Windows)

Users/Logins

```
-- login creation for Microsoft Entra user
CREATE LOGIN [user@contoso.com] FROM EXTERNAL PROVIDER;
GO
-- login creation for Microsoft Entra group
CREATE LOGIN [my_group_name] FROM EXTERNAL PROVIDER;
GO
-- login creation for Microsoft Entra application
CREATE LOGIN [my_app_name] FROM EXTERNAL PROVIDER;
GO
```

Use, **Object_Id** for non-unique Entra names

```
CREATE LOGIN [myapp4466e] FROM EXTERNAL PROVIDER
  WITH OBJECT_ID = 'aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb'
```

Outbound – Create Credential

```
CREATE CREDENTIAL [https://<storage-account-name>.blob.core.windows.net/<container-name>]
    WITH IDENTITY = 'Managed Identity'
```

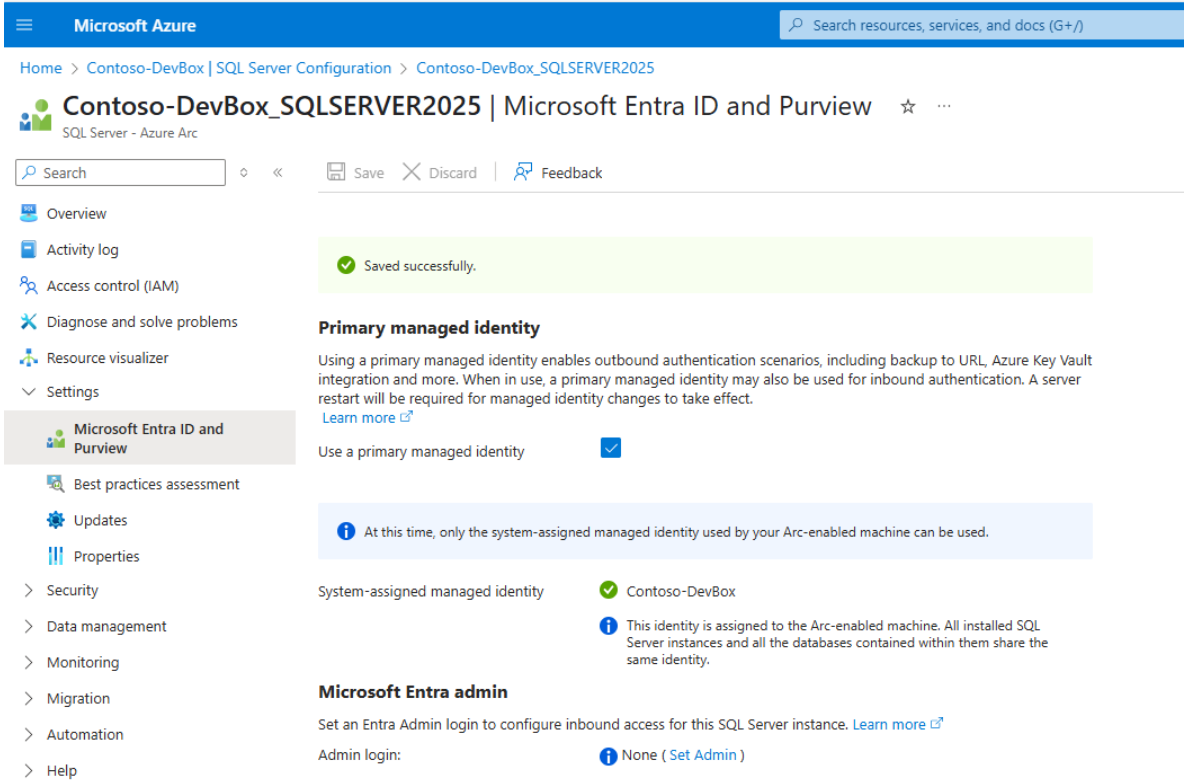
Outbound – Backup & Restore to the Azure storage

```
BACKUP DATABASE [AdventureWorks]
    TO URL = 'https://<storage-account-name>.blob.core.windows.net/<container-name>/AdventureWorks.bak'
```

```
RESTORE DATABASE [AdventureWorks]
    FROM URL = 'https://<storage-account-name>.blob.core.windows.net/<container-name>/AdventureWorks.bak'
```

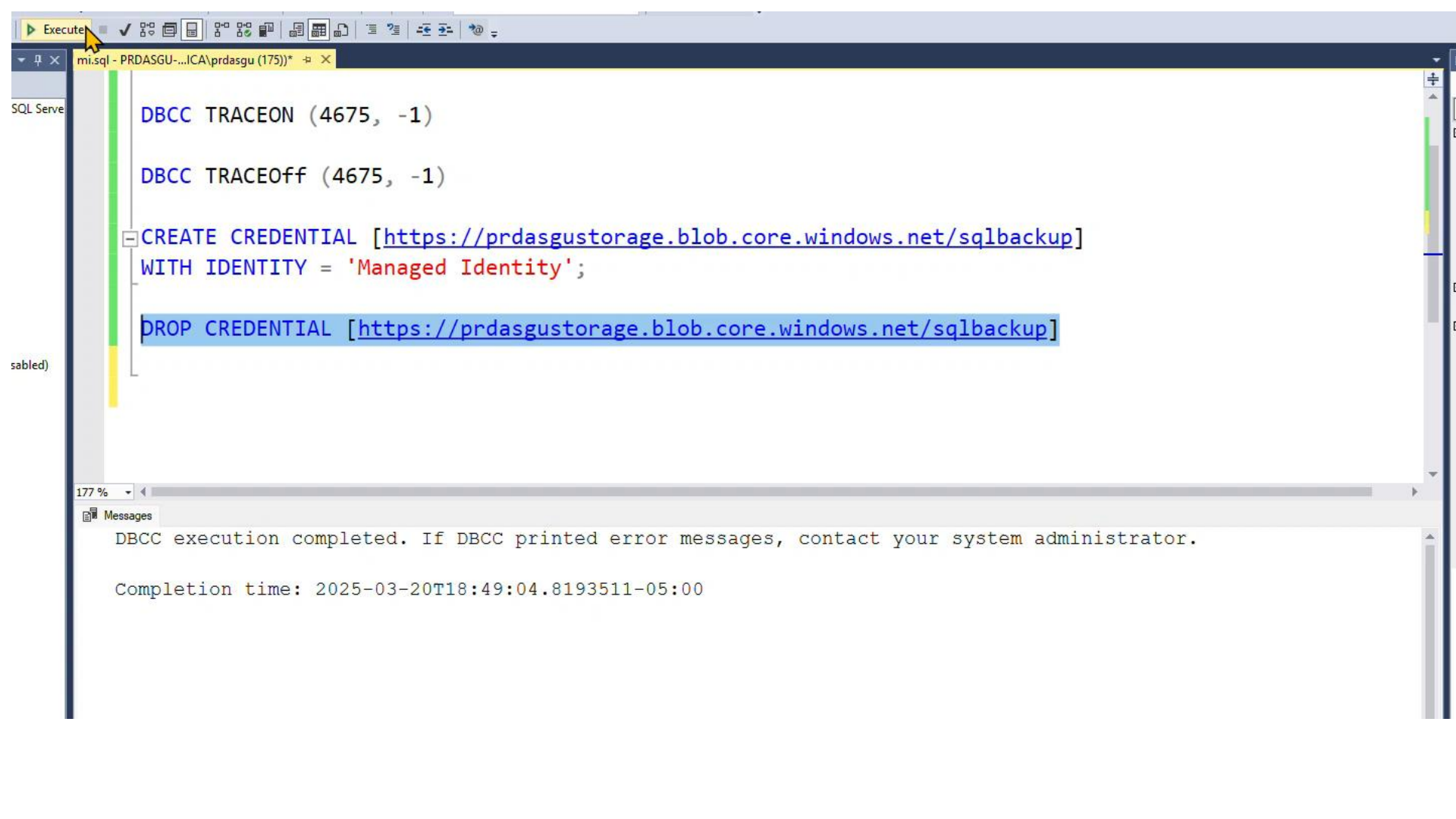
How to get started

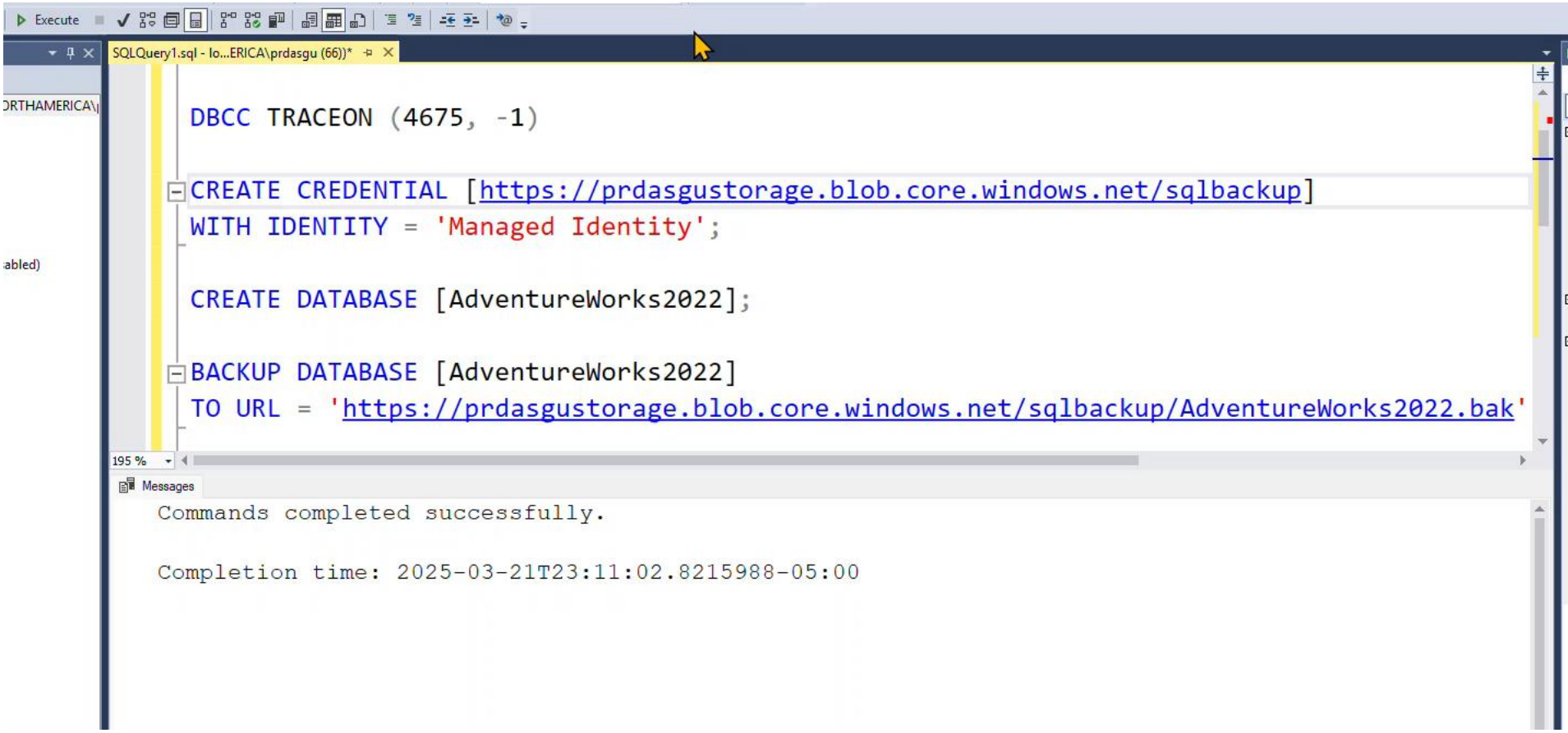
- Associate a “Primary managed identity” to the SQL Server
- Grant graph API permissions
  - User.Read.All,
  - GroupMember.Read.All, and
  - Application.Read.All





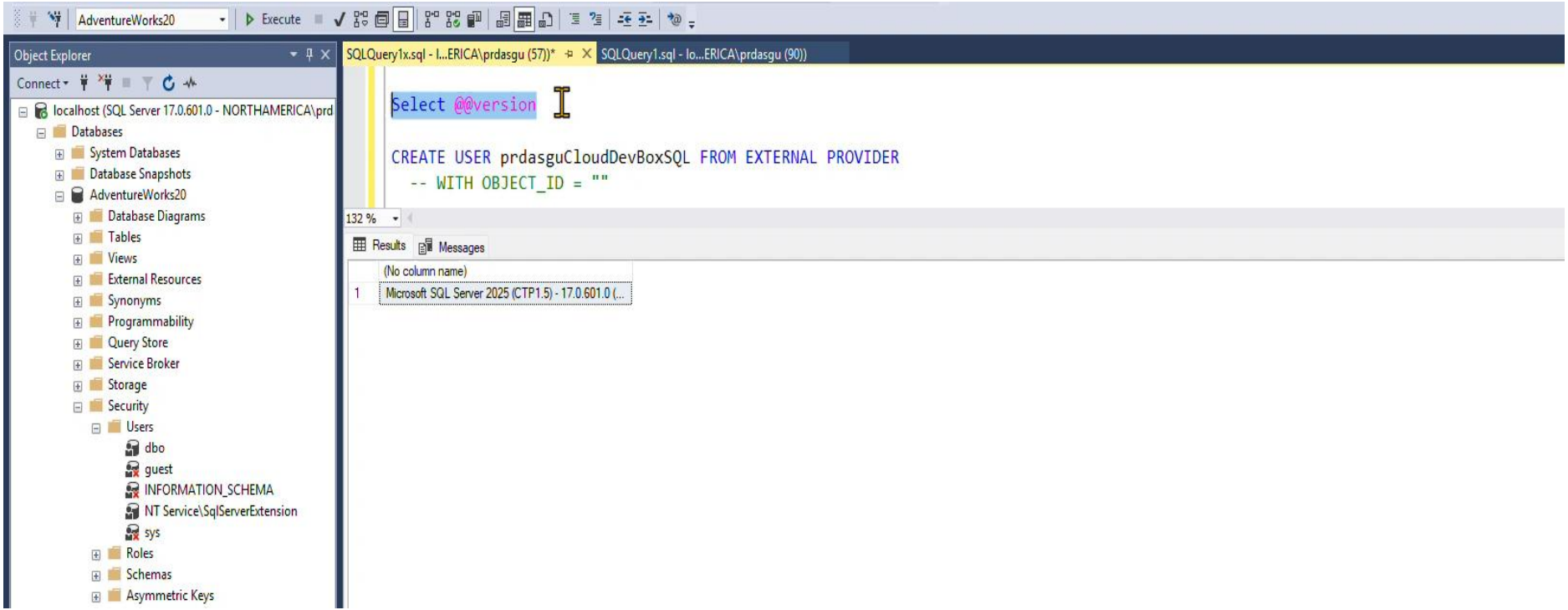
Backup to URL


Execute
mi.sql - PRDASGU-...ICA\prdasgu (175))*
SQL Serve
sabled)
DBCC TRACEON (4675, -1)
DBCC TRACEOff (4675, -1)
CREATE CREDENTIAL [https://prdasgustorage.blob.core.windows.net/sqlbackup]
WITH IDENTITY = 'Managed Identity';
DROP CREDENTIAL [https://prdasgustorage.blob.core.windows.net/sqlbackup]
177 %
Messages
DBCC execution completed. If DBCC printed error messages, contact your system administrator.
Completion time: 2025-03-20T18:49:04.8193511-05:00


Execute
SQLQuery1.sql - lo...ERICA\prdasgu (66))*
DBCC TRACEON (4675, -1)
CREATE CREDENTIAL [https://prdasgustorage.blob.core.windows.net/sqlbackup]
WITH IDENTITY = 'Managed Identity';
CREATE DATABASE [AdventureWorks2022];
BACKUP DATABASE [AdventureWorks2022]
TO URL = 'https://prdasgustorage.blob.core.windows.net/sqlbackup/AdventureWorks2022.bak'
195 %
Messages
Commands completed successfully.
Completion time: 2025-03-21T23:11:02.8215988-05:00



Create User/Login


AdventureWorks20
Execute
Object Explorer
Connect
localhost (SQL Server 17.0.601.0 - NORTHAMERICA\prd
Databases
System Databases
Database Snapshots
AdventureWorks20
Database Diagrams
Tables
Views
External Resources
Synonyms
Programmability
Query Store
Service Broker
Storage
Security
Users
dbo
guest
INFORMATION_SCHEMA
NT Service\SqlServerExtension
sys
Roles
Schemas
Asymmetric Keys
SQLQuery1x.sql - I...ERICA\prdasgu (57))*
SQLQuery1.sql - lo...ERICA\prdasgu (90))
Select @@version
CREATE USER prdasguCloudDevBoxSQL FROM EXTERNAL PROVIDER
-- WITH OBJECT_ID = ""
132 %
Results
Messages
(No column name)
1
Microsoft SQL Server 2025 (CTP1.5) - 17.0.601.0 (...

Crypto Updates



PBKDF for password hashes on by default

How does it work?

- Currently supported versions of SQL Server and Azure SQL DB use a SHA-512 hash with a 32-bit random and unique salt.

```
H = SHA512(salt, password)
```

- SQL Server 2025 – we added an iterator to the password verifier algorithm
- The actual algorithm is RFC2898 often called a Password-based Key Derivation Function or PBKDF.

```
H0 = SHA512(salt, 0, password);
for n=1 to 100,000
        Hn = SHA512(salt, Hn-1, password)
```

JimBob	0x**03**00DBB5EF220AE31A08D4B4BF…
MaryJane	0x**02**00BC98F7977FFC8D93B7FF15F…

Good to know…

- The first byte is the algorithm version number.
- The data size on disk is the same for v2 and v3 password verifiers because the salt and resulting hash are the same size.

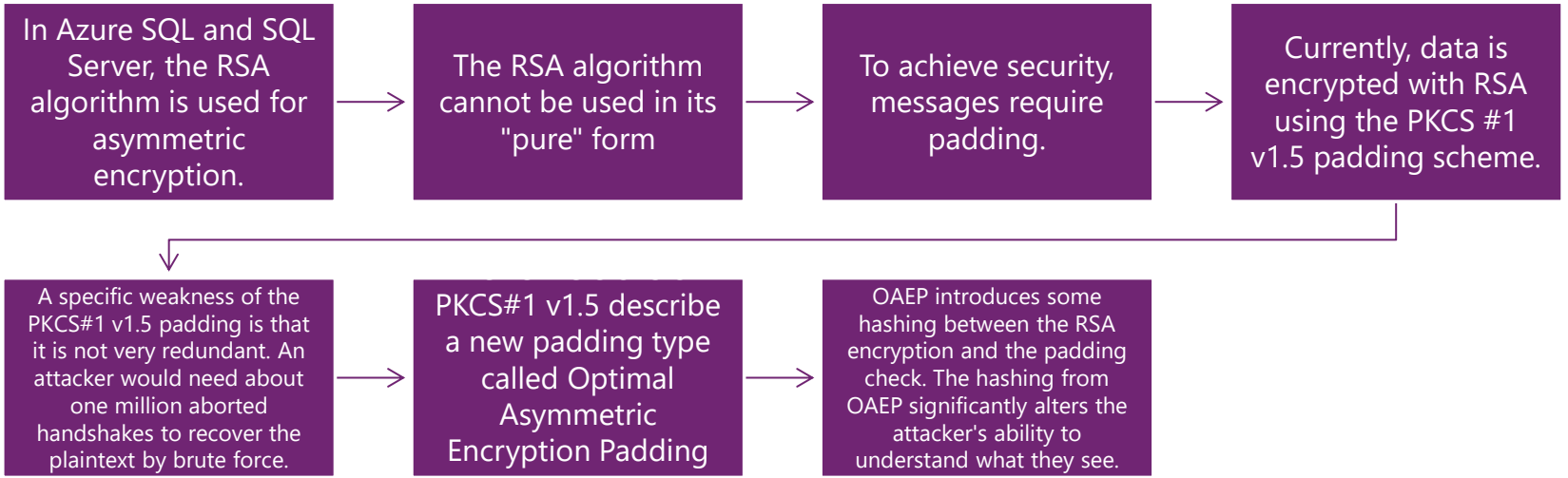


Demo



OAEP support for certificates and asymmetric keys

Why?


In Azure SQL and SQL Server, the RSA algorithm is used for asymmetric encryption.
The RSA algorithm cannot be used in its "pure" form
To achieve security, messages require padding.
Currently, data is encrypted with RSA using the PKCS #1 v1.5 padding scheme.
A specific weakness of the PKCS#1 v1.5 padding is that it is not very redundant. An attacker would need about one million aborted handshakes to recover the plaintext by brute force.
PKCS#1 v1.5 describe a new padding type called Optimal Asymmetric Encryption Padding
OAEP introduces some hashing between the RSA encryption and the padding check. The hashing from OAEP significantly alters the attacker's ability to understand what they see.

How does it work?



From SQL Server 2025 onwards, OAEP-256 support for RSA-based encryption was introduced.



This feature is available for databases at the **170 level of database compatibility** or higher.

Changes in System Catalog View and DMV

- We have added encryption types in the sys.key_encryptions
  - C256 = Encrypted by certificate OAEP256
  - A256 = Encrypted by asymmetric key OAEP256

- In the dm_database_encryption_keys, the encryptor_type will be displayed as CERTIFICATE_OAEP_256 instead of CERTIFICATE.



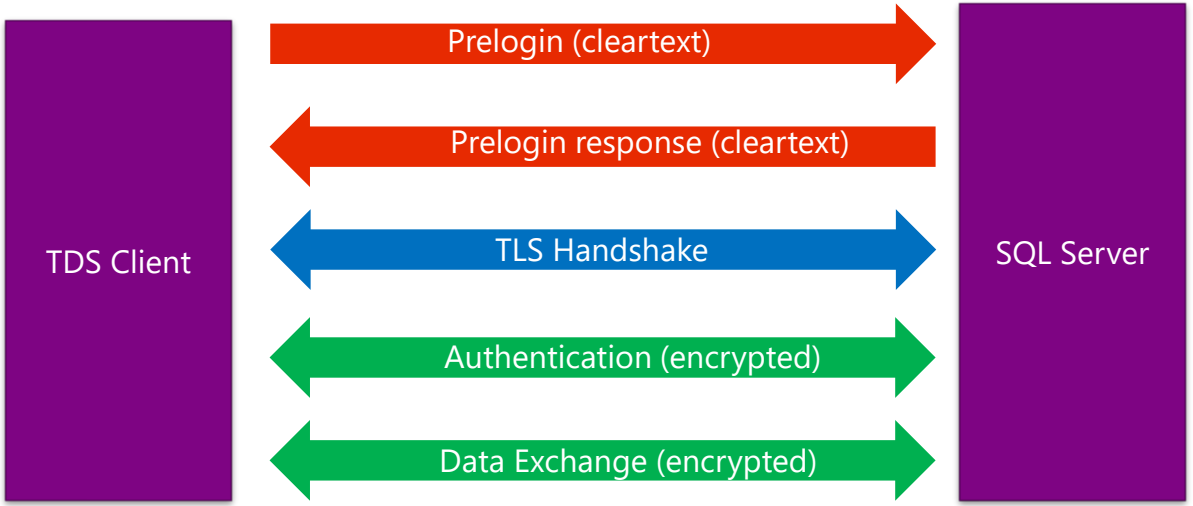
Support TDS 8.0 (TLS 1.3) in SQL Server 2025

Terminology

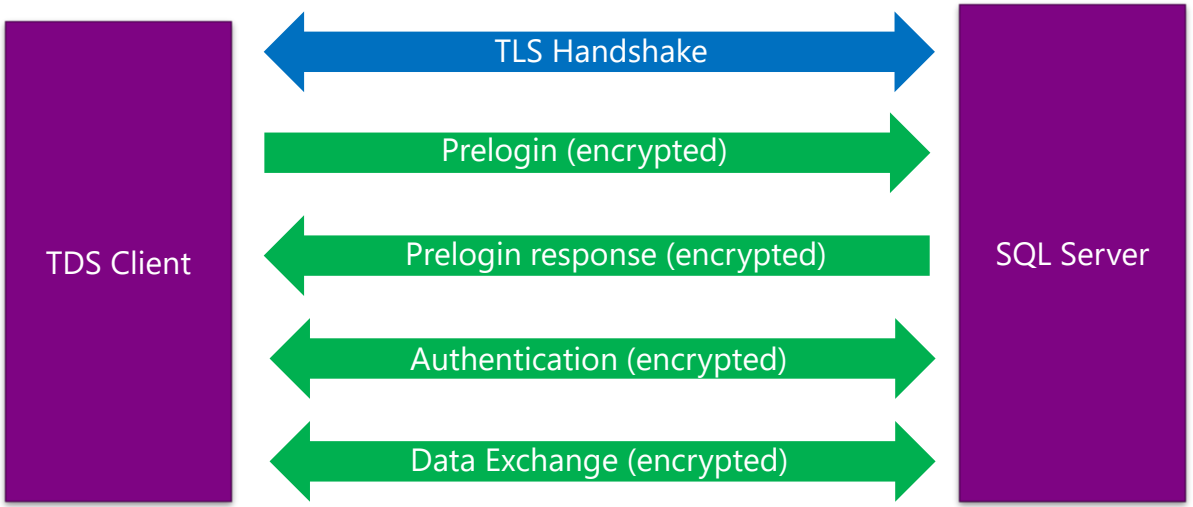
TDS - The Tabular Data Stream (TDS) protocol is an application layer protocol used by clients to connect to SQL Server.

TLS - SQL Server uses Transport Layer Security (TLS) to encrypt data that is transmitted across a network between an instance of SQL Server and a client application.

How TDS works



TDS wrapped in TLS (TDS 8.0)



Strict Connection Encryption

Enhanced Security
SQL Server 2022 includes an enhanced security feature with 'strict' connection encryption type, ensuring safer connections.

Driver Updates
To utilize 'strict' encryption, download the latest versions of SQL Server drivers such as .NET, ODBC, OLE DB, JDBC, PHP, and Python.



Support Forcing Strict Encryption

SQL Server 2022	SQL Server 2025
❖Always On availability groups	✓Always On availability groups
❖Always On failover cluster instance (FCI)	✓Always On failover cluster instance (FCI)
❖SQL Server Replication	✓SQL Server Replication
❖Log Shipping	✓Log Shipping
❖sqlcmd utility	✓sqlcmd utility
❖bcp utility	✓bcp utility
❖SQL Server CEIP service	✓SQL Server CEIP service
❖SQL Server Agent	✓SQL Server Agent
❖Database Mail	✓Database Mail
❖Linked Servers	✓Linked Servers
❖Polybase connector to SQL Server	✓Polybase connector to SQL Server
❖SQL VSS Writer	✓SQL VSS Writer

Other Security Enhancements

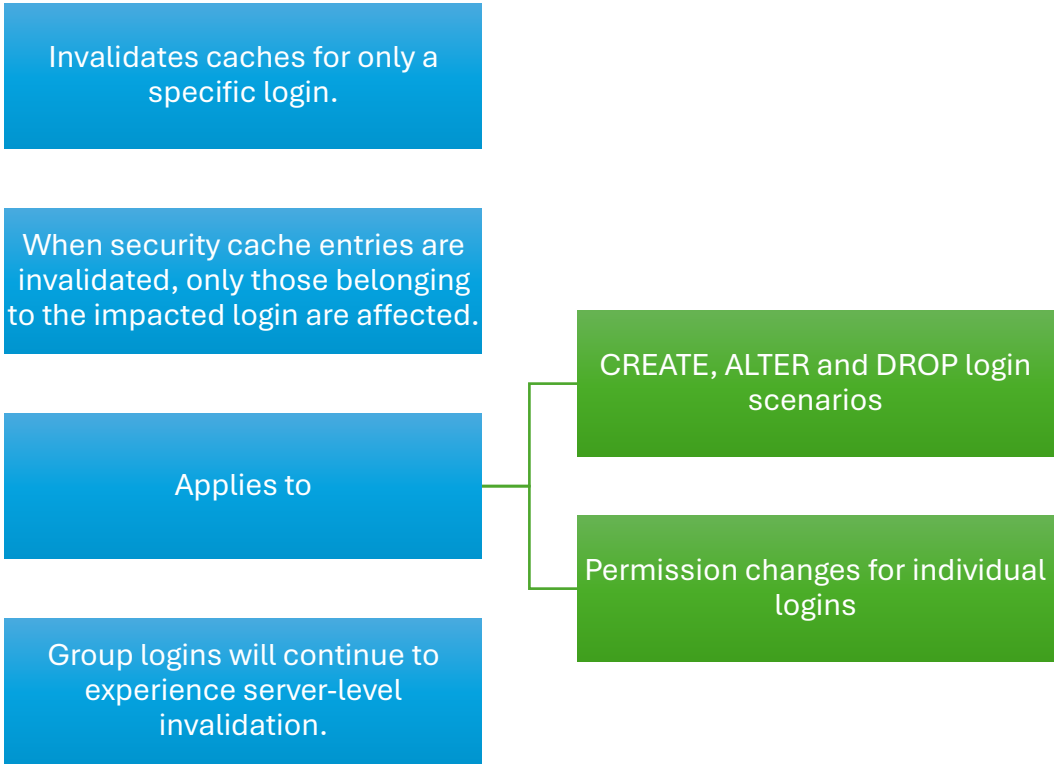


Security Cache Improvements

Security Cache Invalidations

Action	Subject	Scope
CREATE/ALTER/DROP	APPLICATION ROLE (A)SYMMETRIC KEY AUTHORIZATION CERTIFICATE ROLE SCHEMA USER	Specified database
DROP	***Any*** object that appears in sys.all_objects or any securable listed in the database or schema-scoped securable list.	Specified database
GRANT/DENY/REVOKE	***ANY*** permission to securable contained by database or schema	Specified database
CREATE/ALTER/DROP	LOGIN (SERVICE) MASTER KEY	SQL Server Instance
ALTER	DATABASE	Specified database

What is new in SQL Server 2025





Demo



Custom Password Policy SQL Server on Linux

Custom Password Policy support for SQL Logins on SQL Server on Linux

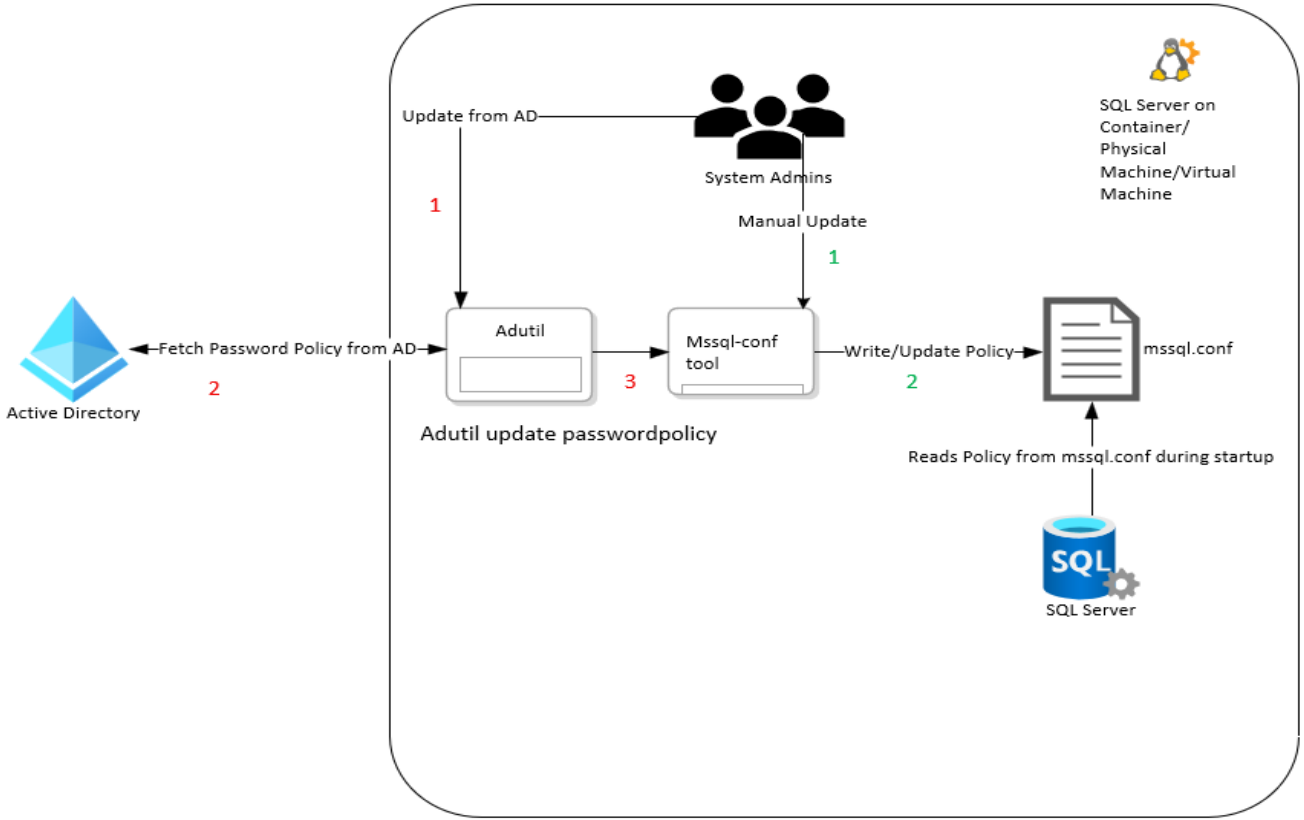
- Password policies are a crucial aspect of securing any database environment. They enforce:
  - Complexity
  - Expiration
  - Changes
- New mssql.conf parameters introduced as shown below
- Can be configured using adutil if AD exists else manually through the mssql.conf changes.

Configuration option	Description
`passwordpolicy.passwordminimumlength`	Defines the minimum number of characters required for a password. The passwords can be up to 128 characters long.
`passwordpolicy.passwordhistorylength`	Determines the number of previous passwords that must be remembered.
`passwordpolicy.passwordminimumage`	Specifies the minimum duration a user must wait before changing their password again.
`passwordpolicy.passwordmaximumage`	Sets the maximum duration a password can be used before it must be changed.

the minimumpasswordlength can't be set to more than 14 characters*

Get started with custom password policy- SQL Server on Linux

- Domain-Joined: Use adutil when SQL Server on Linux is integrated with AD for centralized policy management.
- Non-Domain: If not domain-joined and no domain controller is available, manually configure password policies in mssql.conf.



File Edit Selection View Go Run ··· Search

Welcome

Start Walkthroughs

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS sudo

```
amvin@sqldomain:~$ sudo su
root@sqldomain:/home/amvin# cat /var/opt/mssql/mssql.conf
[sqlagent]
enabled = false

[licensing]
azurebilling = false

[EULA]
accepteula = Y

root@sqldomain:/home/amvin# realm list
contoso.com
  type: kerberos
  realm-name: CONTOSO.COM
  domain-name: contoso.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
```

SSH: 10.0.0.131 ⊗ 0 ⚠ 0 0 Continue

SQL KONFERENZ 2026

Agenda

- Entra Authentication
- Crypto Updates
- Other Security Enhancements



Resources

SFI & Entra Authentication

- Managed identity with Microsoft Entra authentication
- Back up to/restore from URL with managed identity
- Managed Identity support for Extensible Key Management with Azure Key Vault
- Create Microsoft Entra logins and users with *nonunique display names*

Crypto Updates

- OAEP padding mode support for RSA encryption
- PBKDF for password hashes on by default
- TDS 8.0 support

Other Security Enhancements

- Security cache improvements
- Support custom password policy on Linux

SQL
KONFERENZ
2026



Thank you!

Pieter Vanhove
Senior Product Manager - Microsoft