SQL Server on NetApp AFF

NetApp database solutions

NetApp
November 16, 2026

This PDF was generated from https://docs.netapp.com/us-en/netapp-solutions-databases/mssql/sql-smb3-aff-overview.html on November 16, 2026. Always check docs.netapp.com for the latest.

Table of Contents

SQL Server on NetApp AFF . . . 1
- Learn about SQL Server 2025 on NetApp AFF with SMB 3 continuous availability . . . 1
  - Benefits of SQL Server on SMB 3 with NetApp ONTAP . . . 1
  - Solution components . . . 1
  - Design principles . . . 2
  - How continuous availability works . . . 3
- Deploy SQL Server 2025 on NetApp AFF using SMB 3 continuously available shares . . . 4
  - Scope . . . 4
  - Audience . . . 4
  - Lab environment . . . 5
  - Prerequisites . . . 5
  - Step 1: Prepare the ONTAP cluster . . . 6
  - Step 2: Create and configure the storage VM (SVM) . . . 7
  - Step 3: Create the SQL Server volumes and SMB shares . . . 11
  - Step 4: Adjust the volume settings . . . 15
  - Step 5: Enable continuous availability on the SMB shares . . . 17
  - Step 6: Prepare Windows Server 2025 . . . 19
  - Step 7: Install SQL Server 2025 . . . 20
  - Step 8: Verify the installation and create a database . . . 36
  - Use an ONTAP CLI script to configure the storage in one pass . . . 38
  - Additional information . . . 40

SQL Server on NetApp AFF

Learn about SQL Server 2025 on NetApp AFF with SMB 3 continuous availability

SQL Server 2025 can store databases on SMB 3 continuously available (CA) shares on a NetApp AFF system running ONTAP. Learn about the benefits, solution components, and design principles of this configuration, and how continuous availability keeps databases online during a controller failover.

Microsoft SQL Server has supported placing database files on SMB file shares since SQL Server 2012. With SMB 3 continuously available (CA) shares, a file share is a supported storage option for SQL Server databases and an alternative to block storage (iSCSI or FCP LUNs).

ONTAP on AFF all-flash systems implements SMB 3 natively. Combined with SQL Server 2025 and Windows Server 2025, this provides a fault-tolerant storage architecture that integrates with NetApp data protection.

To deploy this configuration, see Deploy SQL Server 2025 on NetApp AFF using SMB 3 continuously available shares.

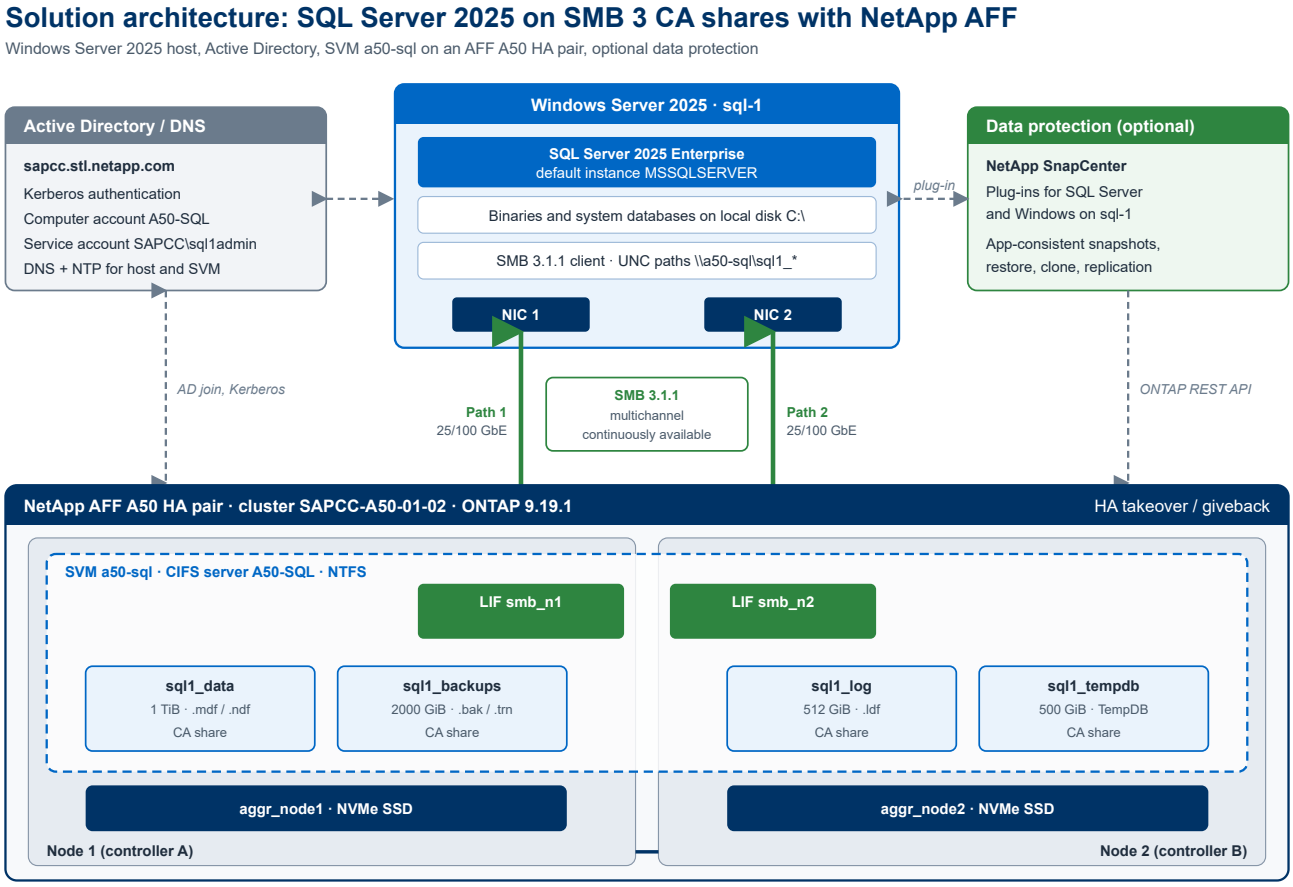
Benefits of SQL Server on SMB 3 with NetApp ONTAP

Benefit	Description
Simple provisioning	There are no LUNs, igroups, MPIO, disk initialization or drive letters to manage. A database file location is just a UNC path such as `\\a50-sql\sql1_data`.
Online capacity management	You grow (or shrink) a volume online in ONTAP, and SQL Server sees the new capacity immediately. No Windows disk or partition operations are required, and autogrow can do it automatically.
Nondisruptive operations	CA shares keep SQL Server running during ONTAP takeover/giveback, nondisruptive upgrades (NDU), LIF migrations and volume moves.
Performance and resiliency	SMB multichannel spreads the I/O across several network paths and NICs and survives the loss of a single path. SMB shares also support SQL Server failover cluster instances (FCI).
Storage efficiency	Inline deduplication, compression and compaction, together with thin provisioning, reduce the physical capacity used by databases and backups.
Integrated data protection	ONTAP snapshots, SnapRestore, FlexClone and SnapMirror, orchestrated by NetApp SnapCenter, provide backups in seconds, restores in minutes and instant database clones.
Flexibility	Databases can be moved between hosts by simply attaching them on another server, without remapping storage. The same SVM can also serve home directories, file services or other applications.

Solution components

The solution consists of the following components:

Component	Role
Windows Server 2025 host (`sql-1`)	Runs SQL Server 2025. The SQL Server binaries and system databases are on the local disk; all user databases, logs, TempDB and backups are accessed over SMB 3.
SQL Server 2025	Database Engine, running under a domain service account (`SAPCC\sql1admin`) that has access to the SMB shares.
Active Directory and DNS	Authenticates the SQL Server service account and the CIFS server (Kerberos) and provides name resolution and time synchronization.
NetApp AFF A50 HA pair	Two controllers with shared NVMe storage. If one controller fails or is upgraded, the partner takes over its storage and network interfaces.
SVM `a50-sql`	A dedicated, Active Directory-joined CIFS server with one SMB data LIF per node, hosting four volumes with CA shares.



Design principles

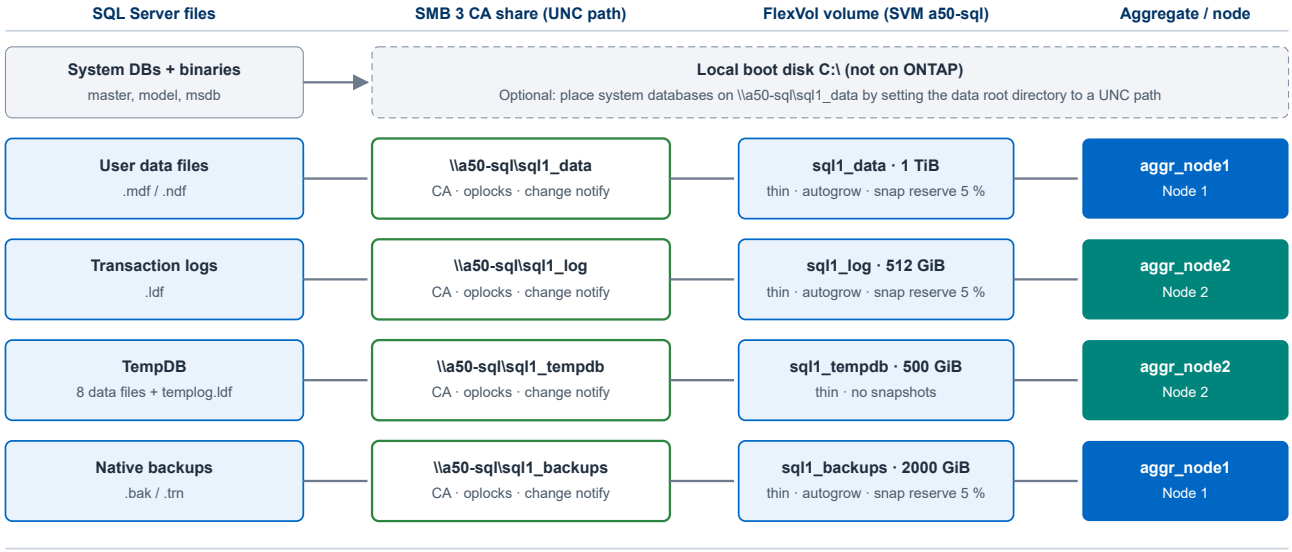
The design follows the NetApp best practices for SQL Server over SMB:

- **Separate volumes per file type.** Data, transaction log, TempDB and backups are placed on separate FlexVol volumes and shares. Each volume can have its own size, QoS, efficiency, snapshot and replication settings. TempDB is excluded from backups.
- **Volumes distributed across both nodes.** Data and backup volumes are on node 1, and log and TempDB volumes are on node 2, so that both controllers do useful work.

- **One SMB data LIF per node.** The host always has a direct path to the node that owns a volume, and SMB multichannel can use both paths.
- **NTFS security style and CA shares.** These are mandatory for SQL Server over SMB on ONTAP.
- **No scheduled ONTAP snapshots on the database volumes.** Backups must be application-consistent; they are created by SnapCenter.

Storage layout: SQL Server files to SMB shares, volumes and aggregates

One FlexVol volume and one continuously available (CA) SMB share per file type



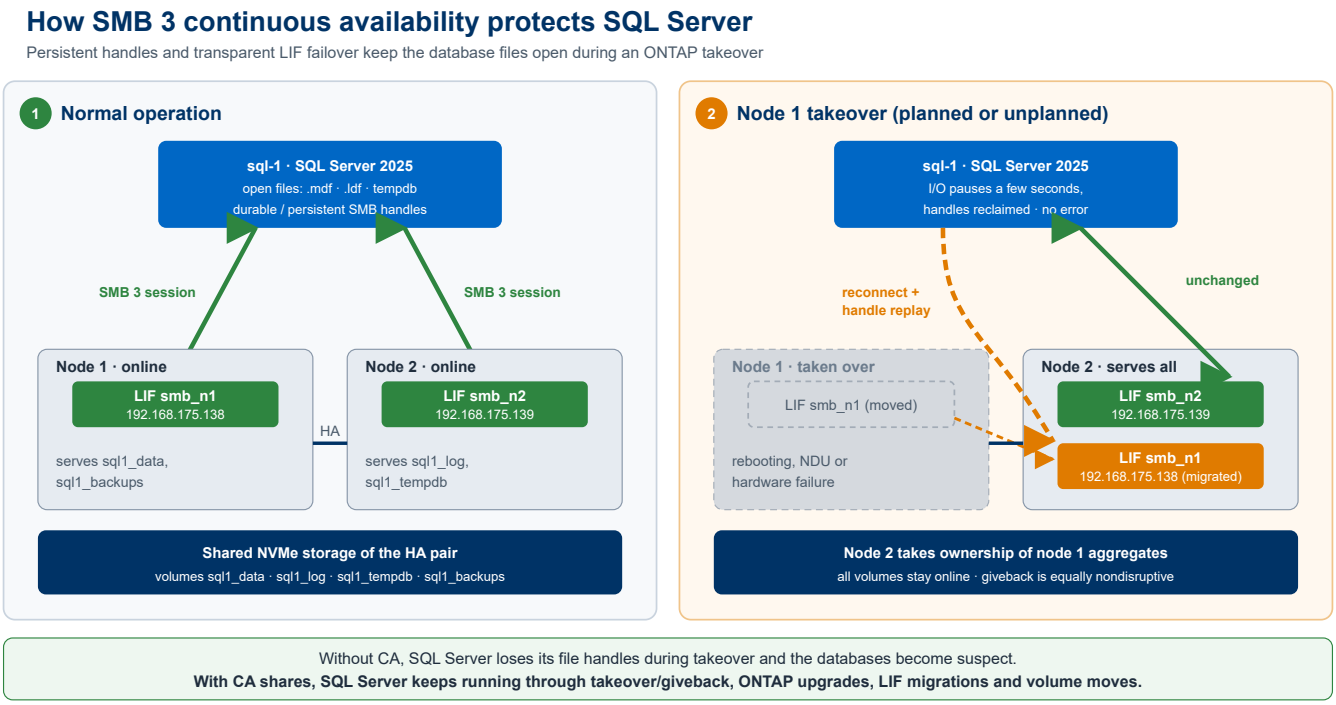
All volumes: NTFS security style · fractional reserve 0 · no scheduled ONTAP snapshots (application-consistent backups by NetApp SnapCenter)

Volumes are distributed across both nodes so that the resources of both controllers are used; each node has one SMB data LIF.

How continuous availability works

With a standard SMB share, a controller failover closes the open file handles. SQL Server then marks the affected databases as suspect, and they must be recovered manually.

With a CA share, ONTAP keeps the state of the open files (persistent handles) mirrored to the HA partner. During a takeover, the SMB LIF of the failed node migrates to the partner. The SMB 3 client on the SQL Server host reconnects automatically and reclaims its handles. SQL Server only sees a short I/O pause of a few seconds; the databases stay online and no transactions are lost. The same applies to planned events such as ONTAP upgrades, giveback, LIF migrations and volume moves.



Deploy SQL Server 2025 on NetApp AFF using SMB 3 continuously available shares

Deploy SQL Server 2025 on Windows Server 2025 with user databases, transaction logs, TempDB, and backups on SMB 3 continuously available shares on a NetApp AFF system. This procedure includes configuring the ONTAP SVM, volumes, and shares, installing SQL Server, and protecting the databases with SnapCenter.

Scope

This procedure deploys a standalone SQL Server 2025 instance on a single Windows Server 2025 host, with user databases, transaction logs, TempDB, and backups on SMB 3 continuously available (CA) shares. The same storage design applies to SQL Server failover cluster instances (FCI) and Always On availability groups, but their cluster-specific configuration is not covered. SQL Server performance tuning and sizing are also out of scope. For the benefits, solution components, design principles, and an explanation of how continuous availability works, see Learn about SQL Server 2025 on NetApp AFF with SMB 3 continuous availability.

Audience

This procedure is intended for:

- **Storage administrators**, who configure the ONTAP cluster, the SVM, the volumes and the SMB shares.
- **Windows and Active Directory administrators**, who prepare the Windows Server 2025 host, the service accounts and the network.
- **Database administrators**, who install and configure SQL Server 2025 and set up backup and recovery.

Basic knowledge of ONTAP System Manager, Windows Server and SQL Server administration is assumed.

Lab environment

The screenshots in this procedure were taken in the following lab environment. Replace the values with the values of your environment.

Component	Value used in the lab
Storage system	NetApp AFF A50 HA pair, cluster `SAPCC-A50-01-02`, ONTAP 9.19.1
SVM	`a50-sql` (CIFS server name `A50-SQL`)
SMB data LIFs	192.168.175.138 (node 1), 192.168.175.139 (node 2)
Active Directory domain	`SAPCC` (`sapcc.stl.netapp.com`)
SQL Server host	`sql-1.sapcc.stl.netapp.com`, Windows Server 2025 Datacenter (Desktop Experience)
SQL Server	SQL Server 2025 Enterprise Edition (17.0.1000.7), default instance `MSSQLSERVER`
SQL Server service account	`SAPCC\sql1admin` (domain account)

Table 1. Volume and share layout

Volume / share	Size	UNC path	Content
`sql1_data`	1024 GiB	`\\a50-sql\sql1_data`	User database data files (`.mdf`, `.ndf`)
`sql1_log`	512 GiB	`\\a50-sql\sql1_log`	User database transaction log files (`.ldf`)
`sql1_tempdb`	500 GiB	`\\a50-sql\sql1_tempdb`	TempDB data and log files
`sql1_backups`	2000 GiB	`\\a50-sql\sql1_backups`	Native SQL Server backup files (`.bak`, `.trn`)



Use separate volumes for data, log, TempDB and backups. This lets you apply different QoS, snapshot, efficiency and replication settings per volume. It also keeps TempDB, which changes constantly, out of the snapshots of your user databases.

Prerequisites

Make sure that the following requirements are met before you start:

NetApp ONTAP

- The AFF HA pair is installed, and the cluster is set up and healthy.
- The CIFS (SMB) license is installed. It is included in ONTAP One.
- At least one data aggregate (local tier) exists on each node.
- Time is synchronized between the cluster and Active Directory through NTP. The maximum allowed clock skew for Kerberos is 5 minutes.
- The data network ports, broadcast domain and (optionally) VLANs for the SMB LIFs are configured.

Active Directory and DNS

- An Active Directory domain is available, and the DNS servers can be reached from the SVM data LIFs.
- You have an account with permission to create computer objects in the target OU, for the CIFS server.
- A dedicated domain user account as service account is available for the SQL Server Database Engine and SQL Server Agent services.

> SQL Server must run under a **domain account** when its files are on an SMB share. Built-in virtual accounts (`NT SERVICE\MSSQLSERVER`) and local accounts cannot be granted access to a remote file share.

Windows Server

- Windows Server 2025 (Desktop Experience) is installed, patched and joined to the domain.
- The SQL Server 2025 installation media (ISO) and a valid product key (or a free edition) are available.

SMB requirements and restrictions for SQL Server on ONTAP

- SMB 3.0 or later must be enabled on the SVM.
- All volumes that host CA shares must use the **NTFS** security style and must have been NTFS from the start.
- SMB Direct (RDMA) is not supported.
- ReFS is not supported. ONTAP (WAFL) provides the file system for the shares.

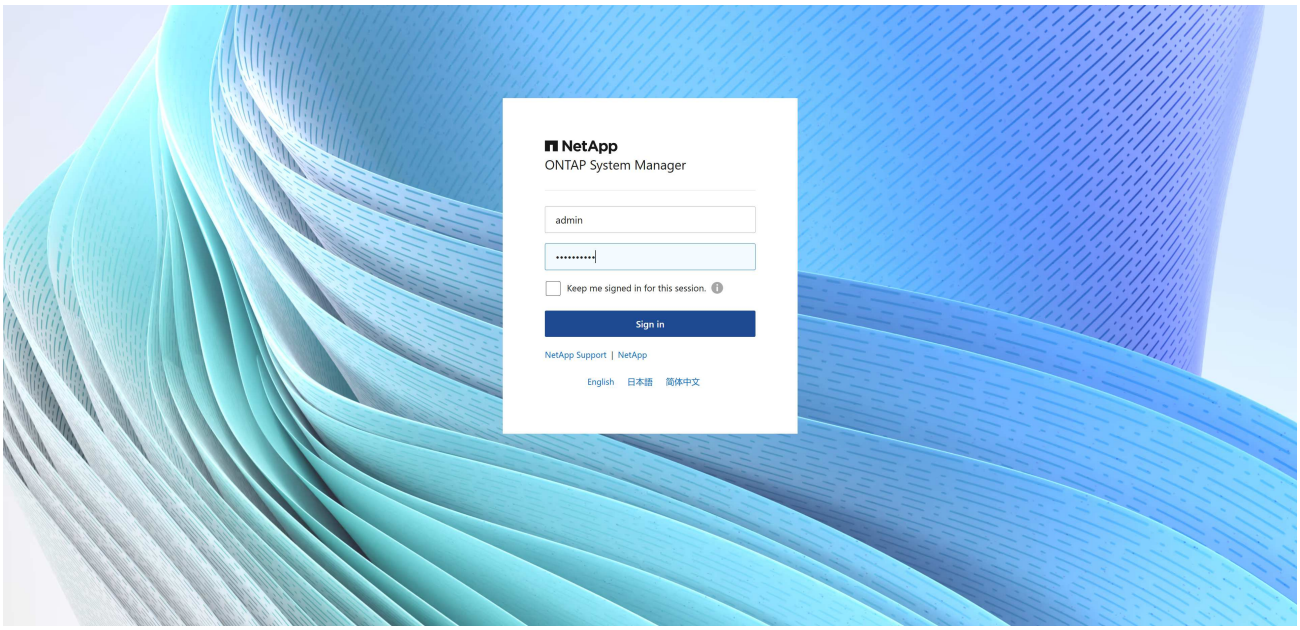
Step 1: Prepare the ONTAP cluster

Connect to ONTAP System Manager and make sure that the cluster time is synchronized with Active Directory. Kerberos authentication for the SMB shares fails if the clock skew exceeds 5 minutes.

Steps

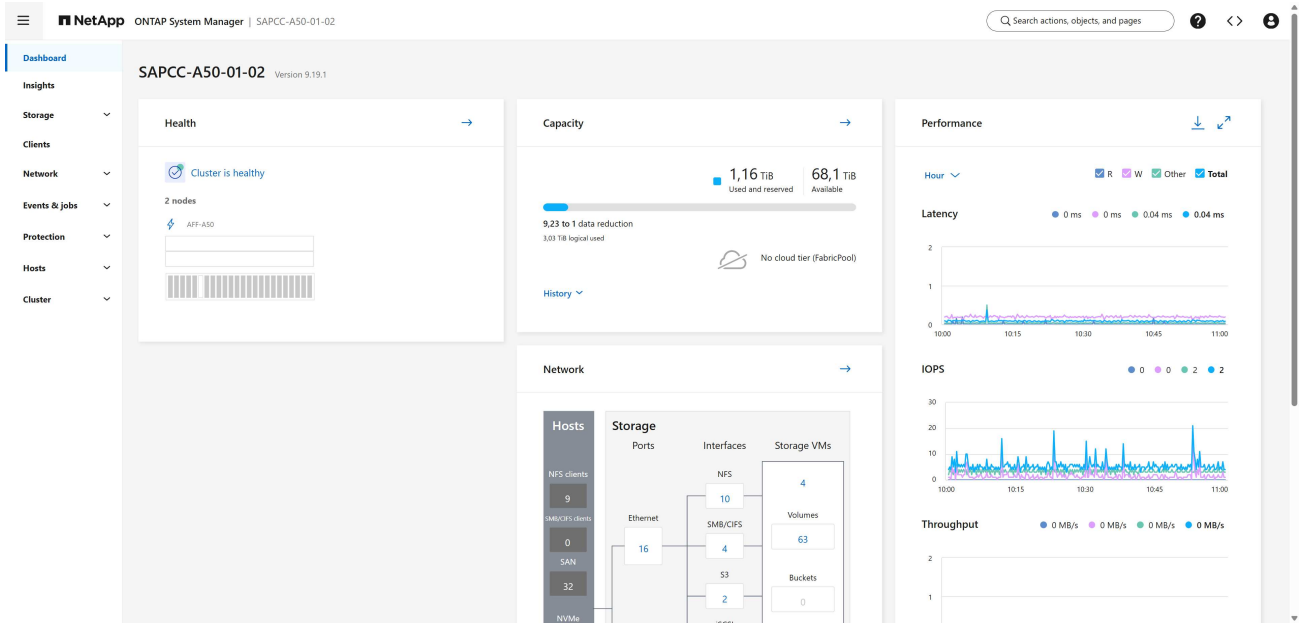
1. Open a web browser and connect to ONTAP System Manager at `https://<cluster-management-IP>`. Log in with the cluster administrator account.

   ▼ Show example



2. The **Dashboard** is the entry point for further configuration in System Manager.

▼ **Show example**



3. If NTP isn't configured yet, add your domain controllers or the corporate NTP servers using the CLI (SSH to the cluster management LIF):

```
cluster::> cluster time-service ntp server create -server <NTP-server-IP>
```

Step 2: Create and configure the storage VM (SVM)

Use a dedicated SVM for SQL Server. The SVM joins Active Directory as a CIFS server and provides one SMB data LIF on each node of the HA pair.

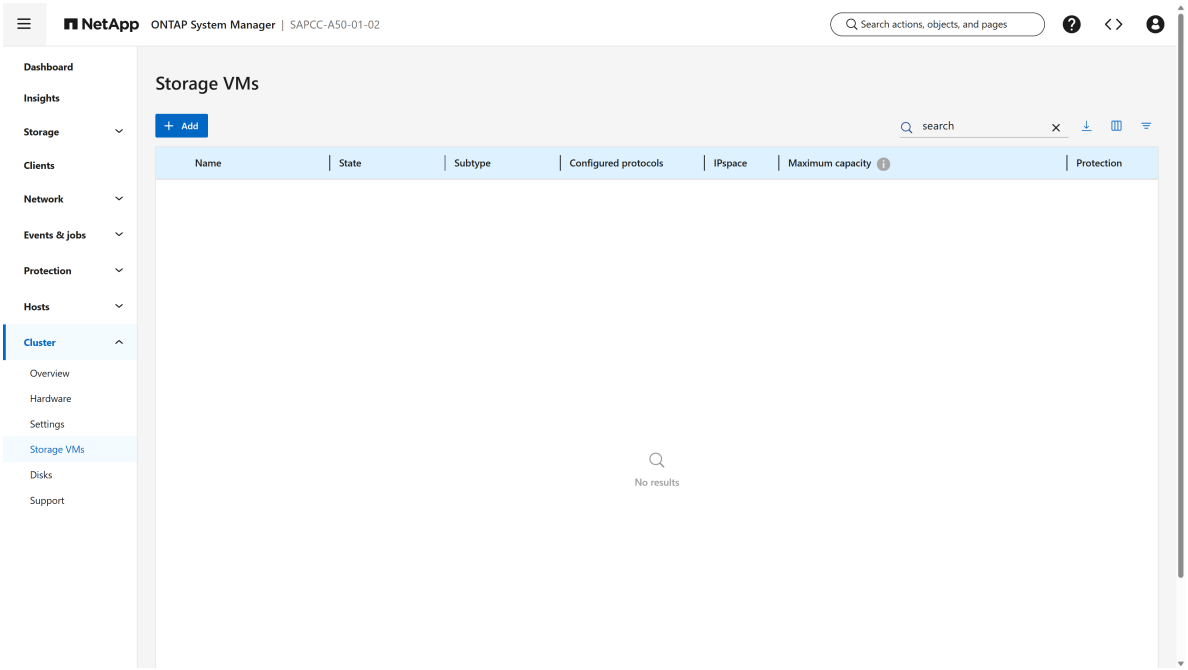
Steps

1. Create the SVM with System Manager or the CLI:

System Manager

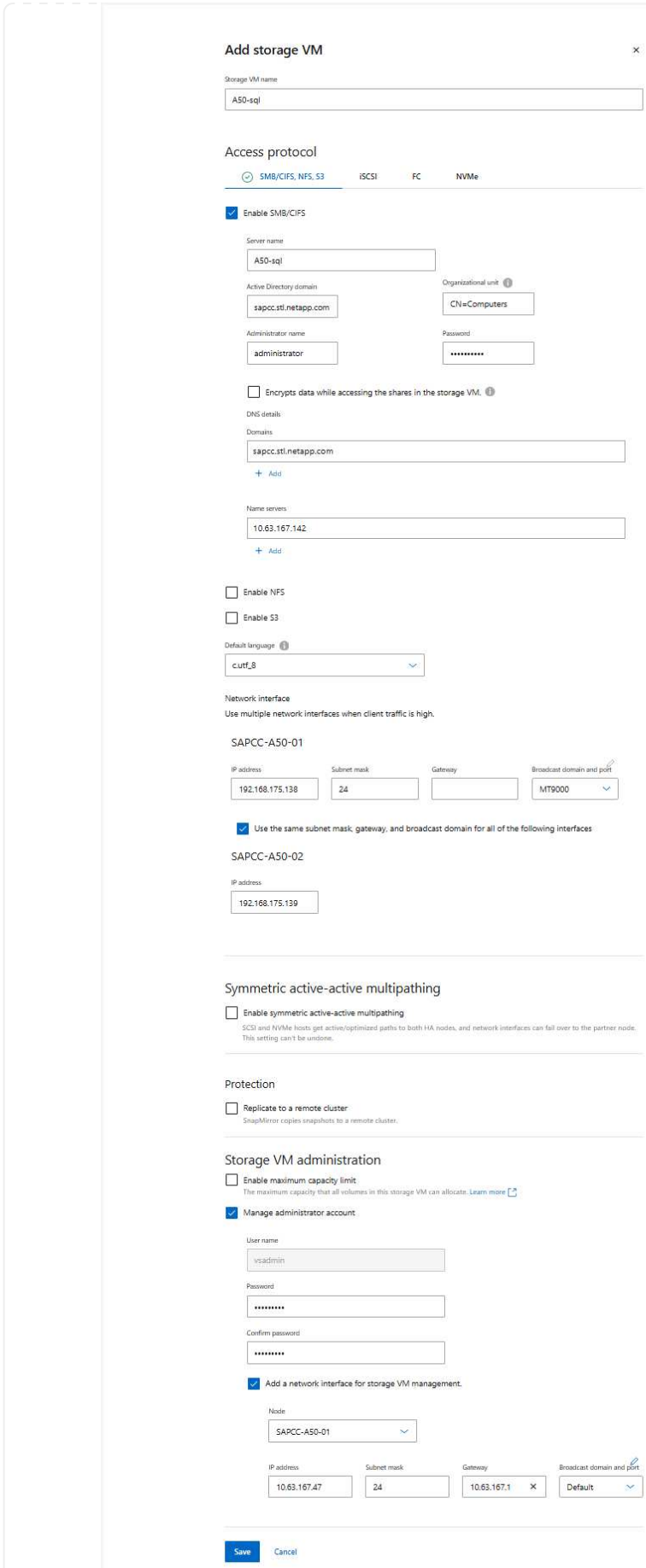
a. In System Manager, go to **Cluster › Storage VMs** and click **+ Add**.

▼ **Show example**



b. Enter the **Storage VM name** `a50-sql`. In **Access protocol**, select the **SMB/CIFS, NFS, S3** tab and select **Enable SMB/CIFS**.

▼ Show example


Add storage VM
Storage VM name
A50-sql
Access protocol
SMB/CIFS, NFS, S3
iSCSI
FC
NVMe
Enable SMB/CIFS
Server name
A50-sql
Active Directory domain
sapcc.stl.netapp.com
Organizational unit
CN=Computers
Administrator name
administrator
Password
Encrypts data while accessing the shares in the storage VM.
DNS details
Domains
sapcc.stl.netapp.com
Add
Name servers
10.63.167.142
Add
Enable NFS
Enable S3
Default language
c.utf_8
Network interface
Use multiple network interfaces when client traffic is high.
SAPCC-A50-01
IP address
192.168.175.138
Subnet mask
24
Gateway
Broadcast domain and port
MT9000
Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces
SAPCC-A50-02
IP address
192.168.175.139
Symmetric active-active multipathing
Enable symmetric active-active multipathing
SCSI and NVMe hosts get active/optimized paths to both HA nodes, and network interfaces can fail over to the partner node. This setting can't be undone.
Protection
Replicate to a remote cluster
SnapMirror copies snapshots to a remote cluster.
Storage VM administration
Enable maximum capacity limit
The maximum capacity that all volumes in this storage VM can allocate. Learn more
Manage administrator account
User name
vsadmin
Password
Confirm password
Add a network interface for storage VM management.
Node
SAPCC-A50-01
IP address
10.63.167.47
Subnet mask
24
Gateway
10.63.167.1
Broadcast domain and port
Default
Save
Cancel

The Storage VM name is the SMB name of the CIFS server.

c. Enter the Active Directory information (domain, administrator name and password, and OU) and the DNS information (DNS domain and name servers).

d. Under **Network interface**, configure one data LIF on **each** node.

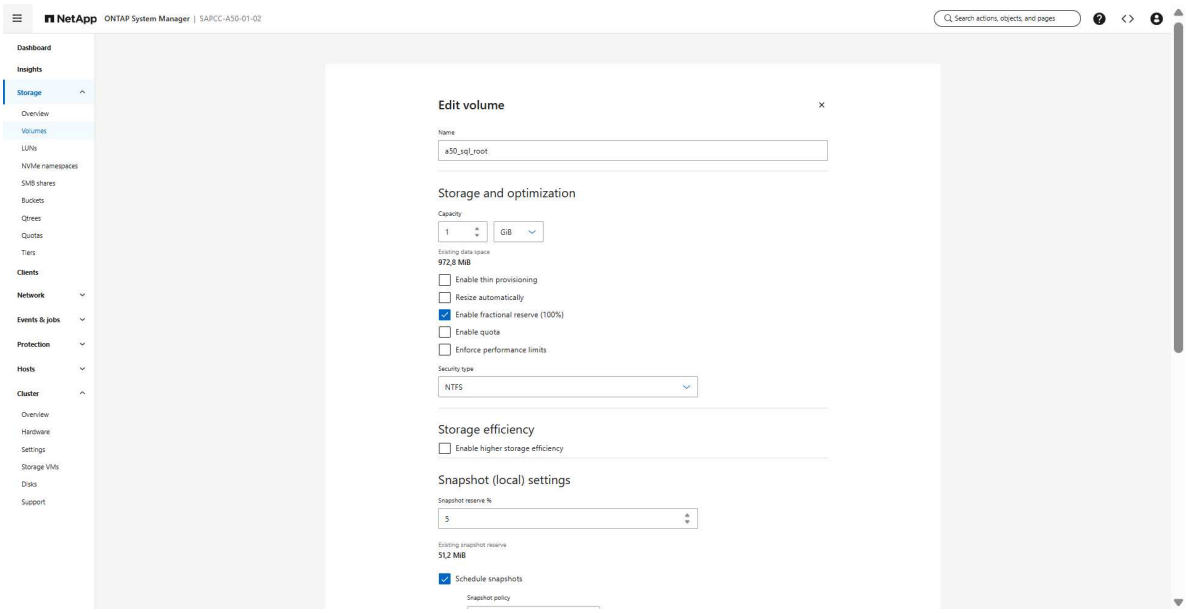
One LIF per node gives SQL Server a direct (local) path to each node, and it is a prerequisite for SMB multichannel and for nondisruptive failover. Use 25 GbE or faster ports, and use the same MTU end to end.

You must register these network interfaces in your DNS server. For details, see Map the SMB server to the DNS server.

e. Click **Save**. System Manager creates the SVM, the root volume, the LIFs and the DNS configuration, and it joins the CIFS server to the domain.

f. Verify the SVM root volume (`a50_sql_root` in the lab). It must use the **NTFS** security style as otherwise SMB shares will not work. Go to **Storage › Volumes**, select the root volume, and click **Edit** to review its settings.

▼ **Show example**



ONTAP CLI

The following commands create the same configuration from the CLI. Replace the placeholder values in angle brackets.

```
cluster::> vserver create -vserver a50-sql -rootvolume a50_sql_root
-aggregate <aggr_node1> -rootvolume-security-style ntfs

cluster::> vserver modify -vserver a50-sql -allowed-protocols cifs

cluster::> network interface create -vserver a50-sql -lif a50-
sql_smb_n1 -service-policy default-data-files -home-node <node1>
```

```
-home-port <port> -address 192.168.175.138 -netmask <netmask>
cluster::> network interface create -vserver a50-sql -lif a50-
sql_smb_n2 -service-policy default-data-files -home-node <node2>
-home-port <port> -address 192.168.175.139 -netmask <netmask>

cluster::> vserver services name-service dns create -vserver a50-sql
-domains sapcc.stl.netapp.com -name-servers <dns1>,<dns2>

cluster::> vserver cifs create -vserver a50-sql -cifs-server A50-SQL
-domain sapcc.stl.netapp.com -ou CN=Computers
```

2. Configure the SMB server options. Verify that the SMB options required for SQL Server are enabled on the SVM:

```
cluster::> set -privilege advanced
cluster::*> vserver cifs options show -vserver a50-sql -fields smb3-
enabled,is-multichannel-enabled,is-large-mtu-enabled,copy-offload-
enabled,shadowcopy-enabled
cluster::*> vserver cifs options modify -vserver a50-sql -smb3-enabled
true -is-multichannel-enabled true -is-large-mtu-enabled true -copy
-offload-enabled true -shadowcopy-enabled true
cluster::*> set -privilege admin
```

Option	Purpose
`smb3-enabled`	SMB 3.x is required for continuously available shares.
`is-multichannel-enabled`	SMB multichannel uses several TCP connections and network paths for higher throughput and resiliency.
`is-large-mtu-enabled`	Allows SMB reads and writes of up to 1 MB.
`copy-offload-enabled`	ODX copy offload; copies are performed inside the storage system.
`shadowcopy-enabled`	Remote VSS for SMB shares. Required by backup applications that use VSS for SMB shares.

3. Verify that the CIFS server is registered in DNS and can be resolved from the SQL Server host:

```
PS C:\> Resolve-DnsName a50-sql.sapcc.stl.netapp.com
```

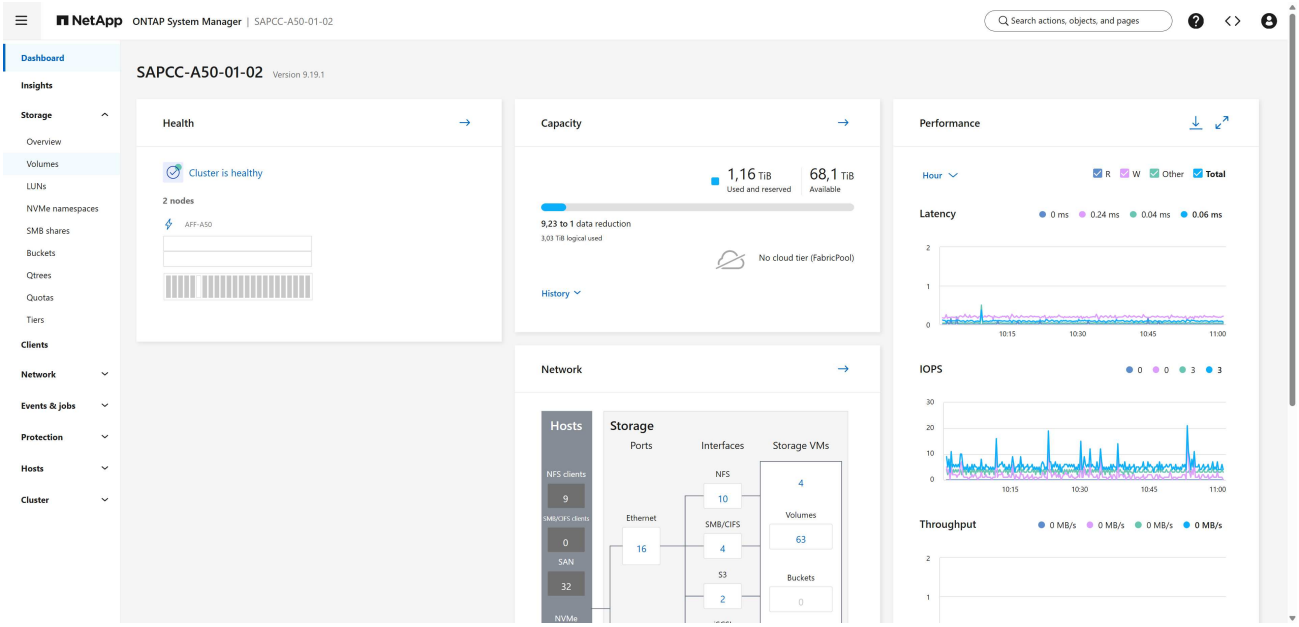
Step 3: Create the SQL Server volumes and SMB shares

Create one volume and one SMB share for each file type. System Manager creates the share together with the volume.

Steps

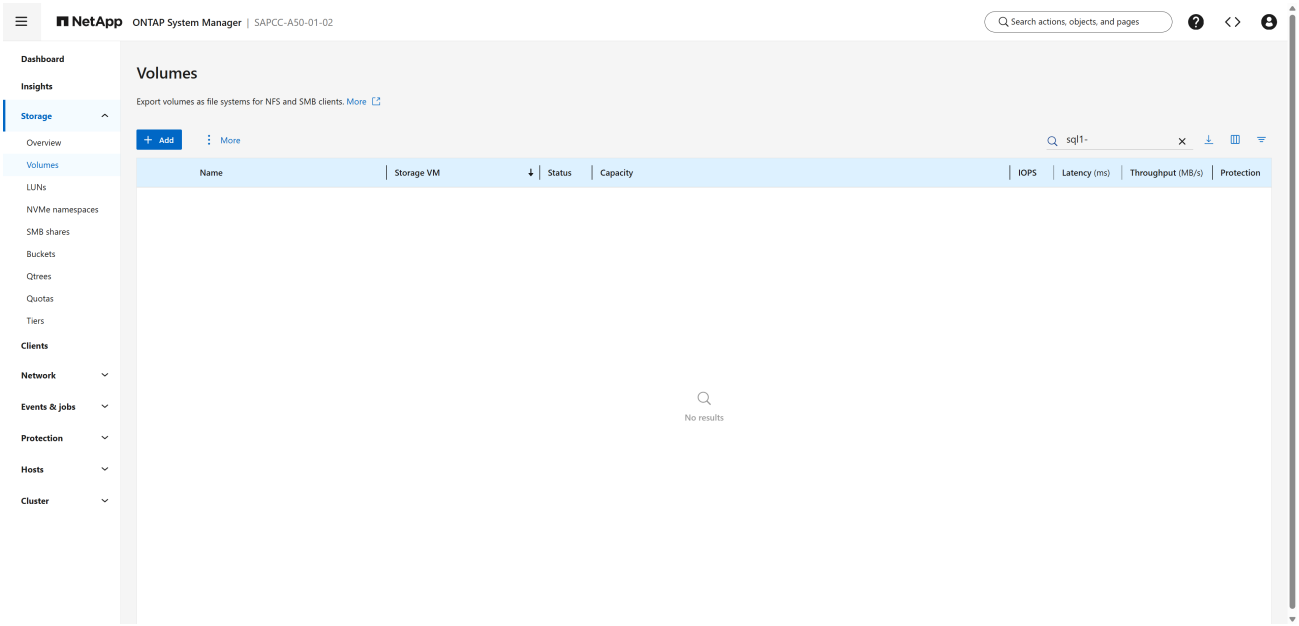
1. In System Manager, expand **Storage** and click **Volumes**.

▼ **Show example**



2. The volume list opens. Click **+ Add**.

▼ **Show example**

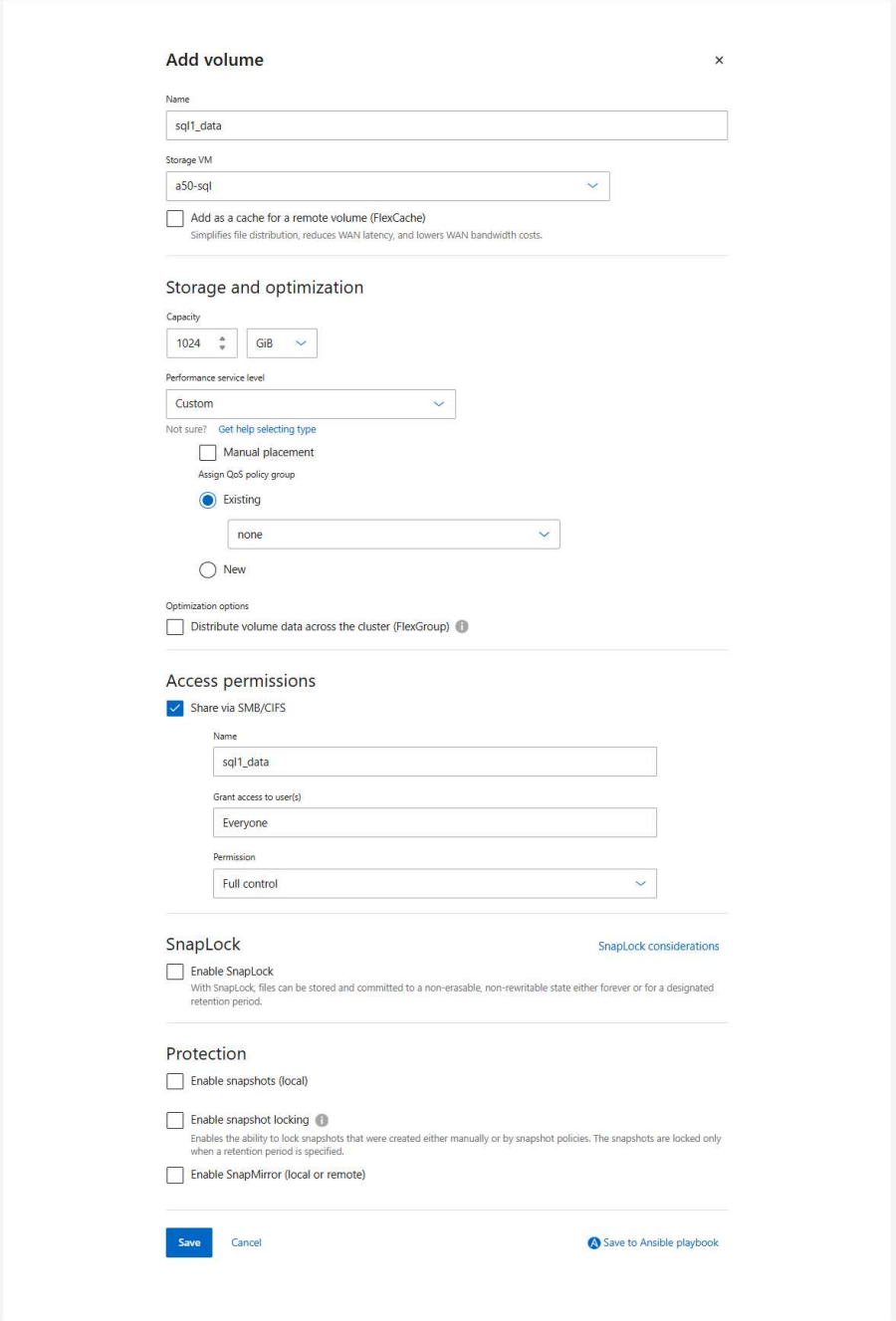


3. Create the `sql1_data` volume and its SMB share for the user database data files.
   a. In the **Add volume** dialog, enter the following values:
      - **Name**: `sql1_data`
      - **Storage VM**: `a50-sql`
      - **Capacity**: `1024 GiB`

- **Performance service level**: **Custom**, **Assign QoS policy group**: **Existing** > `none`
- **Access permissions**: select **Share via SMB/CIFS**. Share name `sql1_data`, grant access to user(s) `Everyone`, permission **Full control**.
- **Protection**: leave **Enable snapshots (local)** cleared. Application-consistent backups are created by NetApp SnapCenter.

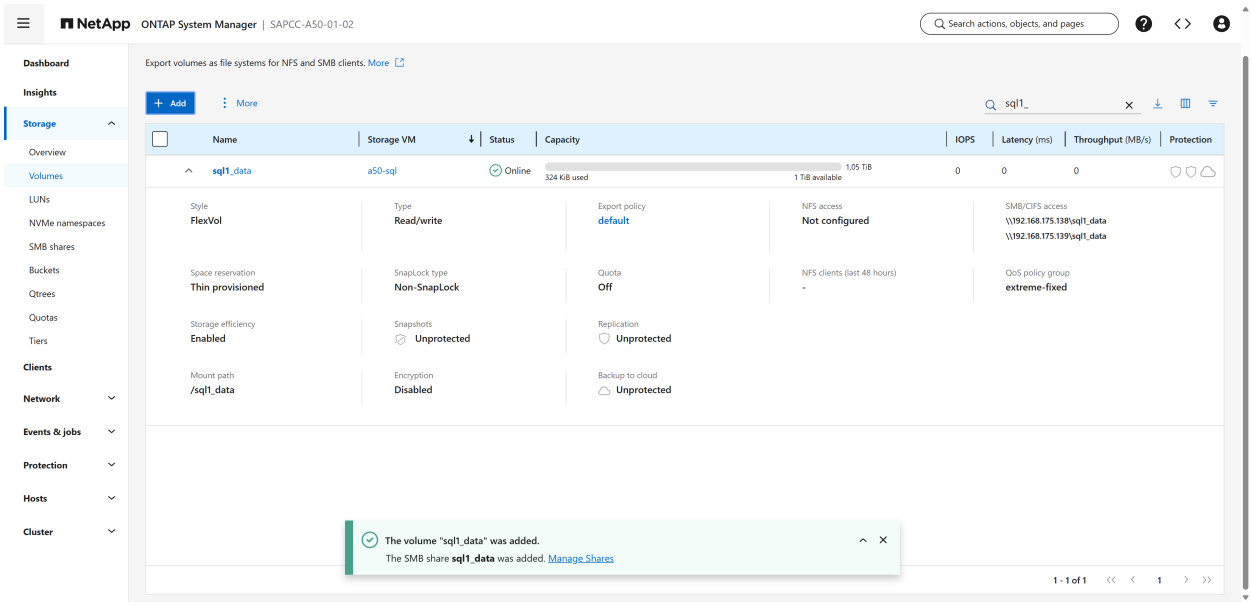
  Click **Save**.

  ▼ **Show example**



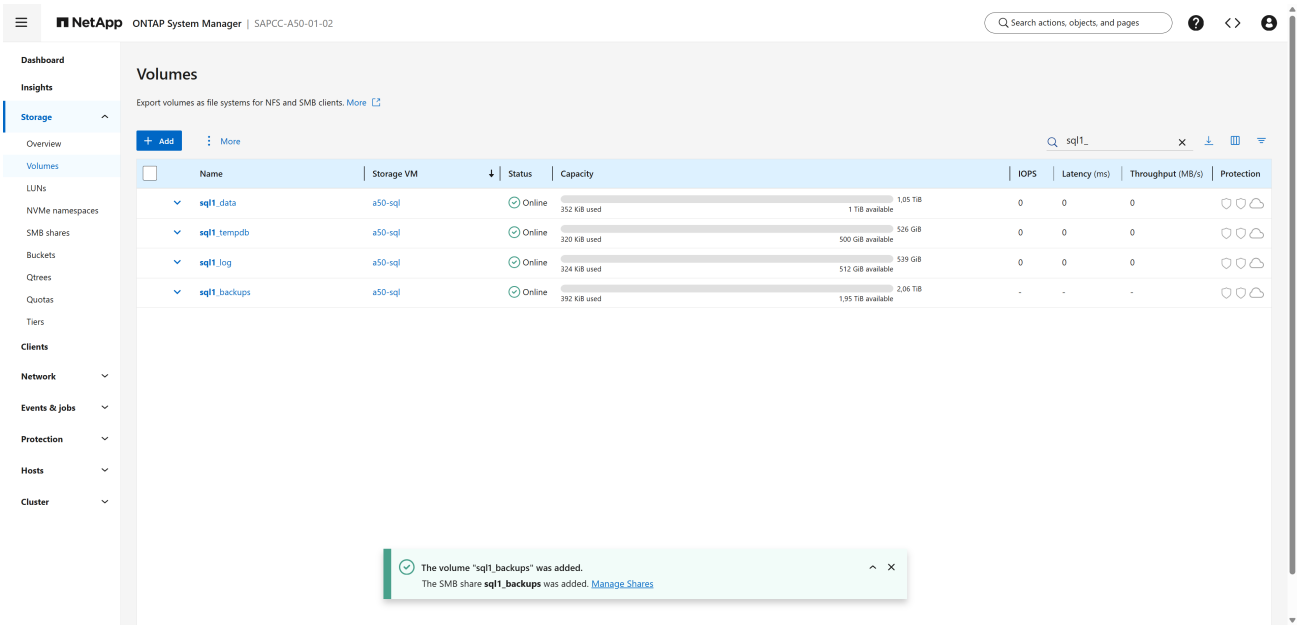
b. The volume is created and shows as **Online**. Expand the volume row to review the details: NTFS security style, SMB access paths through both LIFs (`\\192.168.175.138\sql1_data` and `\\192.168.175.139\sql1_data`), and the QoS policy group.

▼ Show example



4. Repeat the steps for the log, TempDB, and backup volumes with the sizes and names listed in Lab environment.

▼ Show example



The lab grants **Everyone / Full control** on the share level for simplicity. In production, restrict the share ACL to the SQL Server service account, the SQL Server Agent account and the DBA administration group, for example:

```
cluster::> vserver cifs share access-control create -vserver a50-sql
-share sql1_data -user-or-group SAPCC\sql1admin -permission Full_Control
cluster::> vserver cifs share access-control create -vserver a50-sql
-share sql1_data -user-or-group "SAPCC\SQL Admins" -permission
Full_Control
```

```
cluster::> vserver cifs share access-control delete -vserver a50-sql
-share sql1_data -user-or-group Everyone
```

5. Repeat the commands for `sql1_log`, `sql1_tempdb` and `sql1_backups`. The service account also needs **Full Control** on the NTFS permissions of the share root. SQL Server Setup checks this, as shown in Step 7.

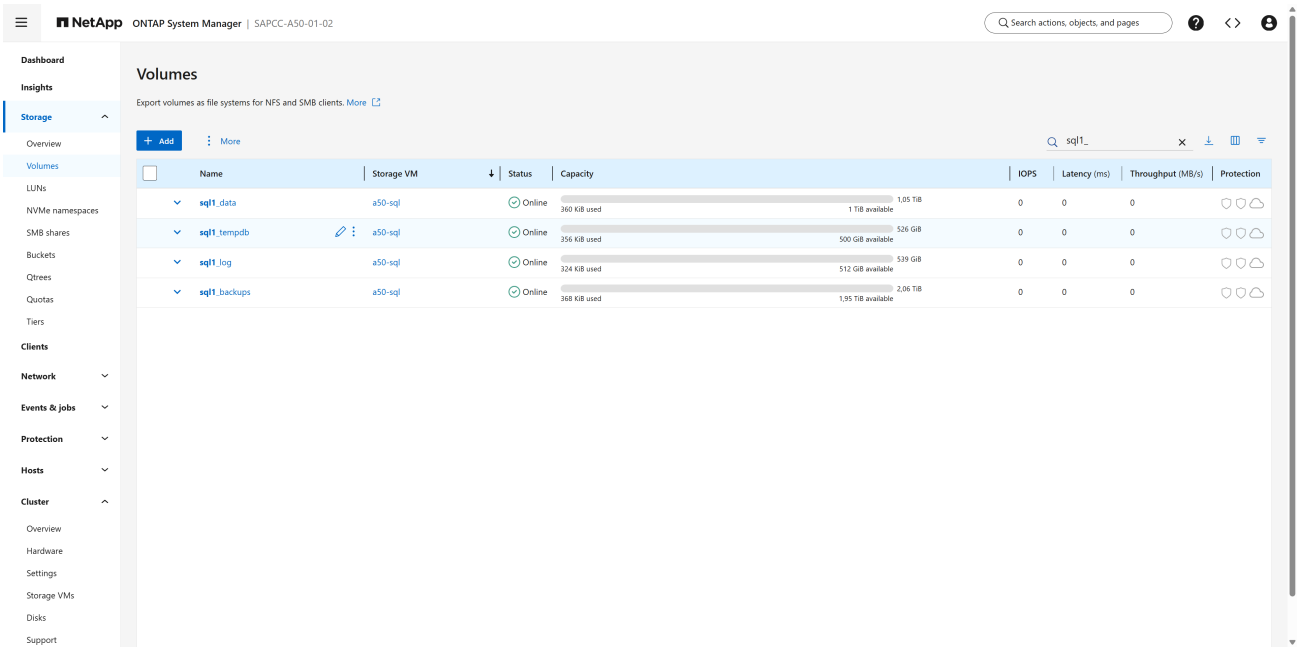
Step 4: Adjust the volume settings

Review and adjust the space and snapshot settings of each SQL Server volume.

Steps

1. In the volume list, hover over the volume and click the pencil icon (**Edit**).

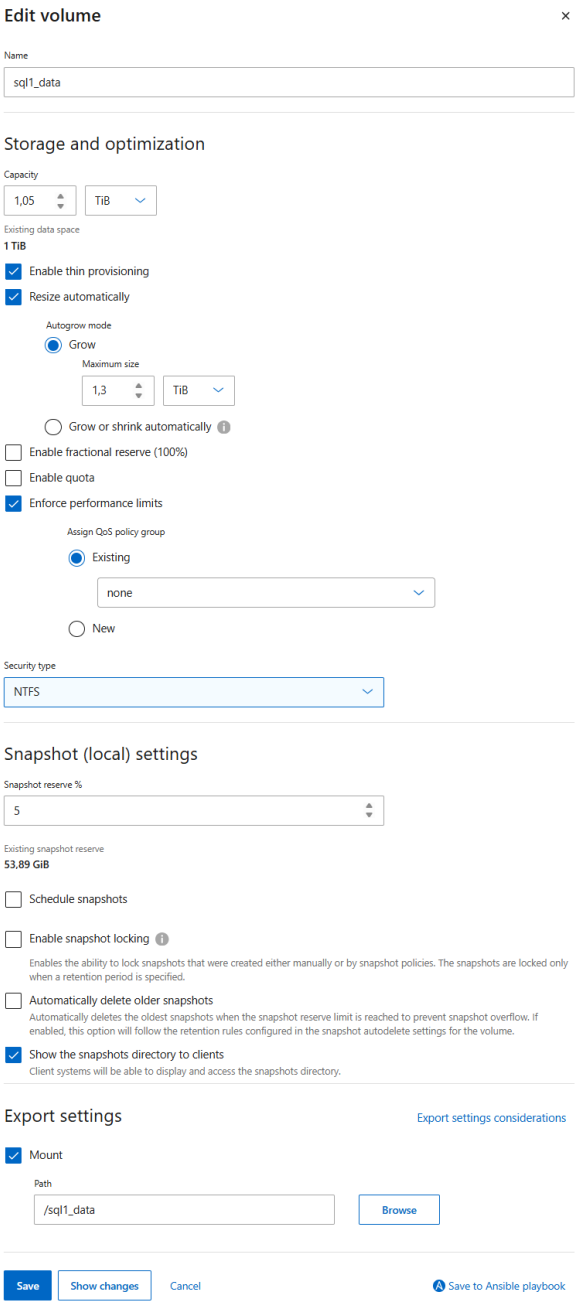
▼ **Show example**



2. Configure the volume as follows (shown for `sql1_data`):
   - **Enable thin provisioning**: selected
   - **Resize automatically**: selected, **Autogrow mode**: **Grow**, **Maximum size**: for example `1.3 TiB` (about 125–130 % of the volume size)
   - **Enable fractional reserve (100%)**: cleared
   - **Security type**: `NTFS`
   - **Snapshot reserve %**: `5` (`0` for `sql1_tempdb`)
   - **Schedule snapshots**: cleared. Snapshots that are not application-consistent are of no use for SQL Server; use NetApp SnapCenter instead.
   - **Show the snapshots directory to clients**: optional (the lab left it selected; clearing it hides `~snapshot` from the share)

     Click **Save**, and repeat for `sql1_log`, `sql1_tempdb` and `sql1_backups`.

▼ **Show example**




```
cluster::> volume modify -vserver a50-sql -volume sql1_data -space
-guarantee none -fractional-reserve 0 -percent-snapshot-space 5 -snapshot
-policy none -autosize-mode grow -max-autosize 1.3TB
```

Keep storage efficiency (deduplication, compression, compaction) enabled on AFF. It is inline and has no measurable impact on SQL Server performance.

Step 5: Enable continuous availability on the SMB shares

Continuous availability is the most important setting for SQL Server on SMB. Without it, SQL Server loses its open file handles during an ONTAP takeover or LIF migration, and the databases go suspect.

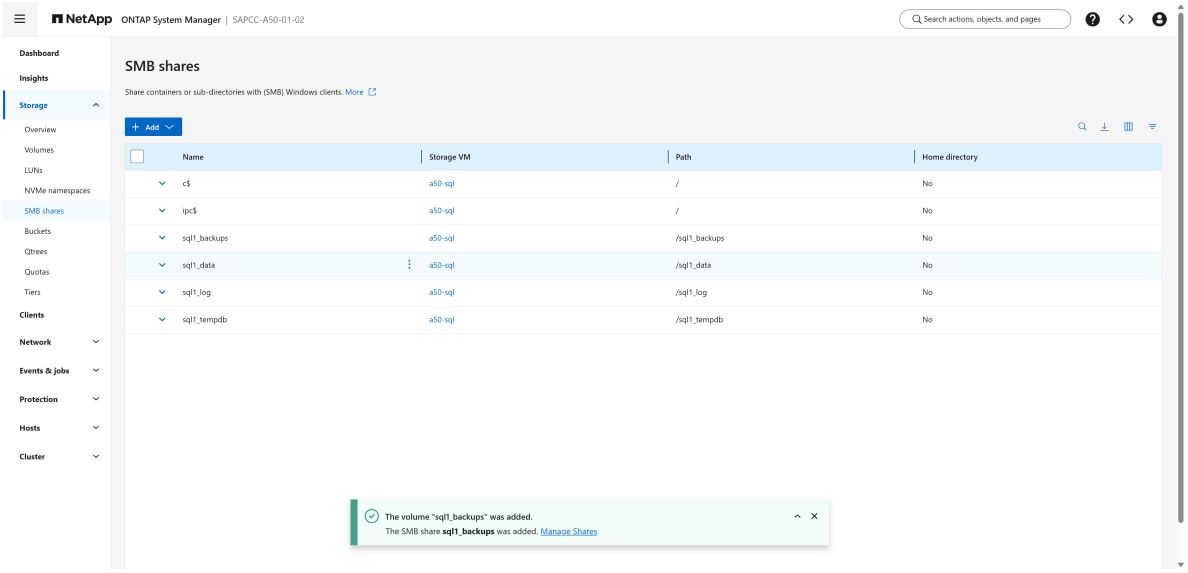
Steps

1. Enable continuous availability on the SMB shares with System Manager or the CLI:

System Manager

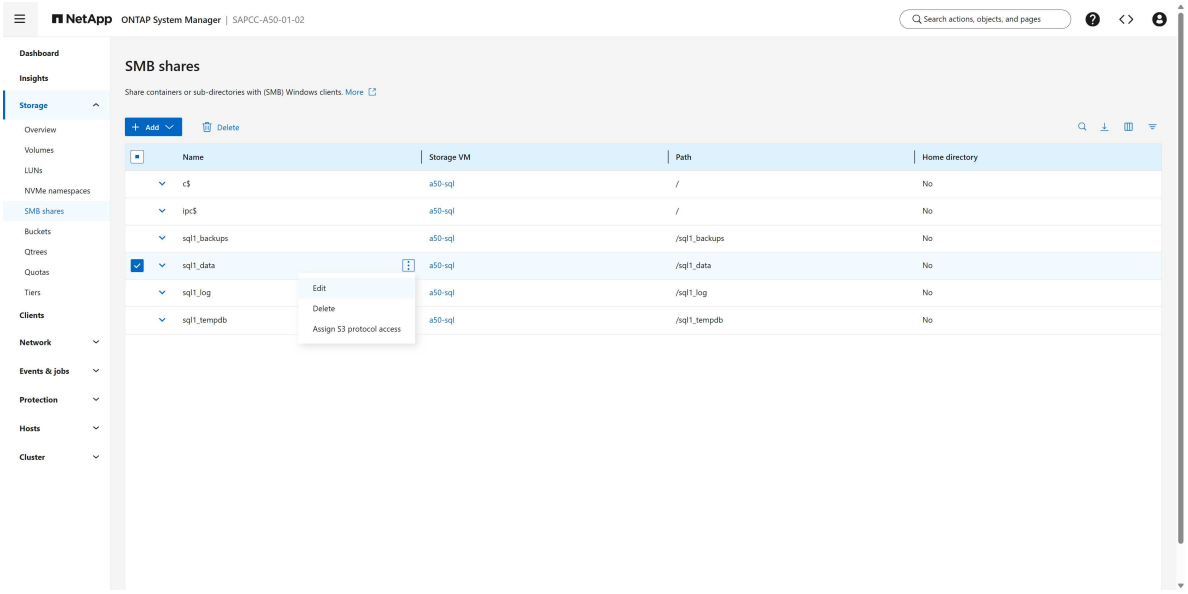
a. Go to **Storage › SMB shares**. The list shows the four new shares and the default administrative shares `c$` and `ipc$`.

▼ Show example



b. Click the more icon (⋮) next to the share `sql1_data` and select **Edit**.

▼ Show example

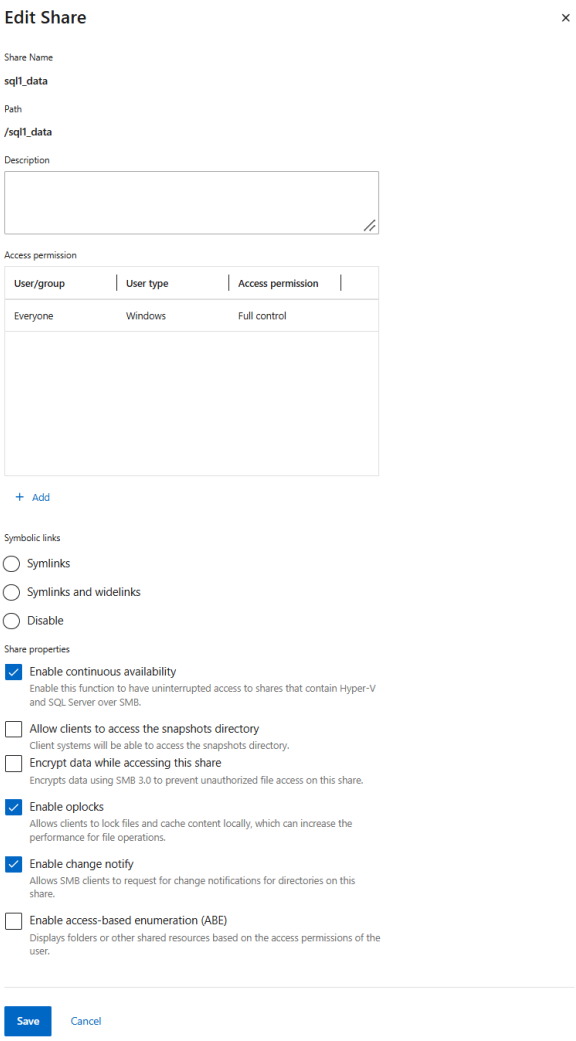


c. Under **Share properties**, set the following:

- **Enable continuous availability**: **selected**
- **Allow clients to access the snapshots directory**: cleared
- **Encrypt data while accessing this share**: cleared (optional, depending on your security requirements)
- **Enable oplocks**: selected
- **Enable change notify**: selected
- **Enable access-based enumeration (ABE)**: cleared

Click **Save**.

▼ **Show example**



d. Repeat these steps for `sql1_log`, `sql1_tempdb` and `sql1_backups`.

ONTAP CLI

```
cluster::> vserver cifs share properties add -vserver a50-sql -share
-name sql1_data -share-properties continuously-available
```

```
cluster::> vserver cifs share properties add -vserver a50-sql -share
-name sql1_log -share-properties continuously-available
cluster::> vserver cifs share properties add -vserver a50-sql -share
-name sql1_tempdb -share-properties continuously-available
cluster::> vserver cifs share properties add -vserver a50-sql -share
-name sql1_backups -share-properties continuously-available

cluster::> vserver cifs share show -vserver a50-sql -fields share-
name,path,share-properties
```

Step 6: Prepare Windows Server 2025

Perform the following steps on the SQL Server host `sql-1` as a domain administrator.

Steps

1. Verify that the server is joined to the domain and that the CIFS server can be resolved (see Configure the SMB server options).
2. Make sure that the SQL Server service account exists in Active Directory, for example `SAPCC\sql1admin`. Use the same account for the Database Engine and for SQL Server Agent, or use a separate account for each. Whichever you choose, grant each account access to all four shares.
3. Test access to the shares in the security context of the service account:

```
PS C:\> runas /user:SAPCC\sql1admin "cmd /c dir \\a50-sql\sql1_data &&
echo test > \\a50-sql\sql1_data\write-test.txt && del \\a50-
sql\sql1_data\write-test.txt"
```

4. Open the SQL Server port in the Windows firewall:

```
PS C:\> New-NetFirewallRule -DisplayName "SQL Server (TCP 1433)"
-Direction Inbound -Protocol TCP -LocalPort 1433 -Action Allow
```

5. Verify the SMB connection to the SVM. The dialect must be 3.x and `ContinuouslyAvailable` must be `True`:

```
PS C:\> dir \\a50-sql\sql1_data | Out-Null
PS C:\> Get-SmbConnection -ServerName a50-sql | Format-Table ServerName
,ShareName,Dialect,ContinuouslyAvailable,Encrypted,Signed
PS C:\> Get-SmbMultichannelConnection -ServerName a50-sql
```

By default, Windows Server 2025 requires SMB signing for all outbound SMB connections. ONTAP supports SMB signing and negotiates it automatically. Signing adds CPU overhead on both sides, so include it in your performance tests. Don’t disable signing without a security

review.

Step 7: Install SQL Server 2025

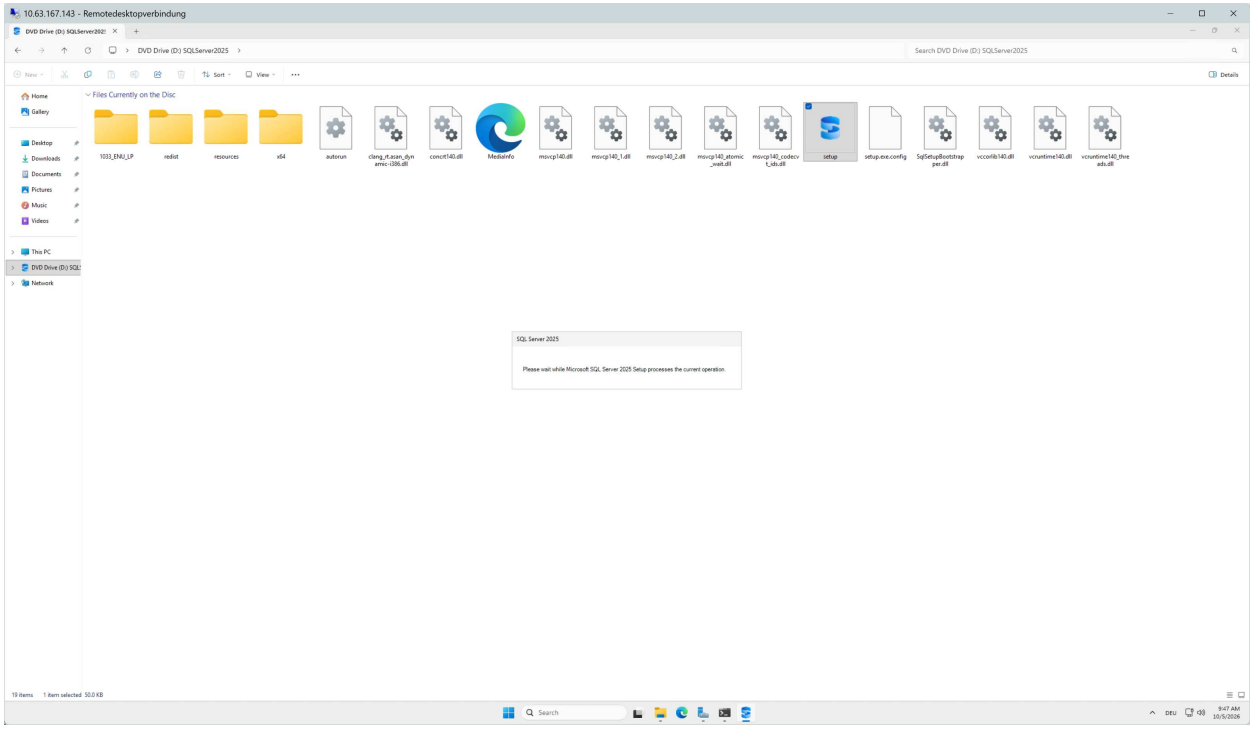
Install SQL Server 2025 on the Windows Server host with the Setup wizard. Install the binaries and system databases on the local disk, and point the user database, transaction log, TempDB, and backup locations to the SMB shares you created.

Steps

1. Start the standalone installation from the SQL Server Installation Center.

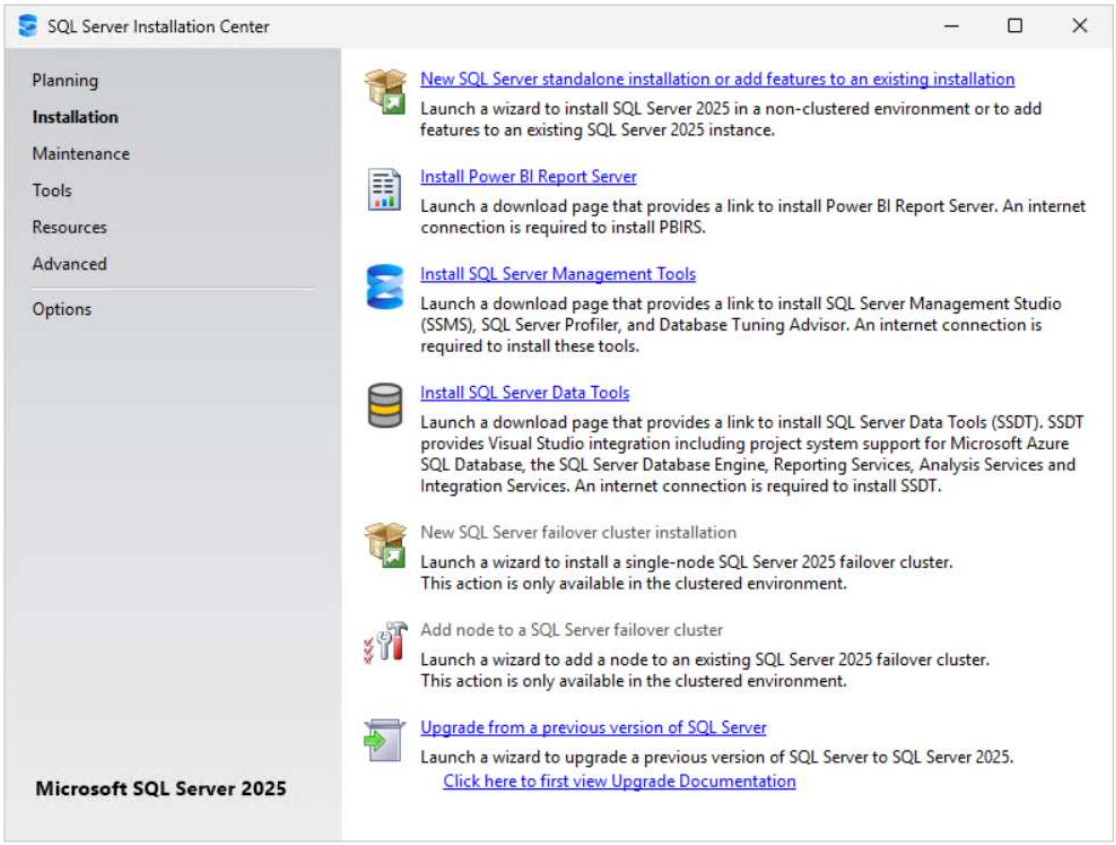
   a. Mount the SQL Server 2025 ISO image. In File Explorer, open the DVD drive (`D:` in the lab) and double-click **setup**.

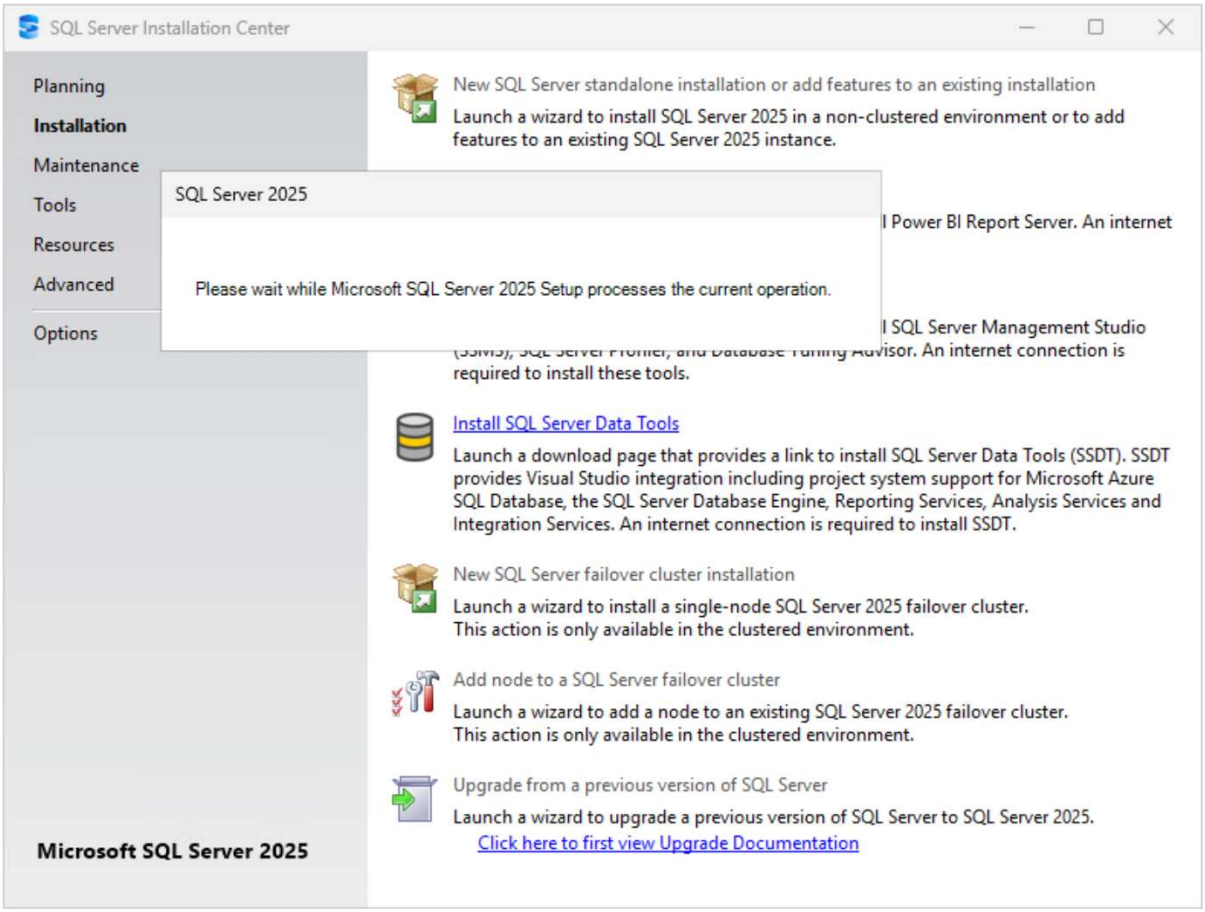
   ▼ **Show example**

   b. The **SQL Server Installation Center** opens. Select **Installation** in the left pane and click **New SQL Server standalone installation or add features to an existing installation**.

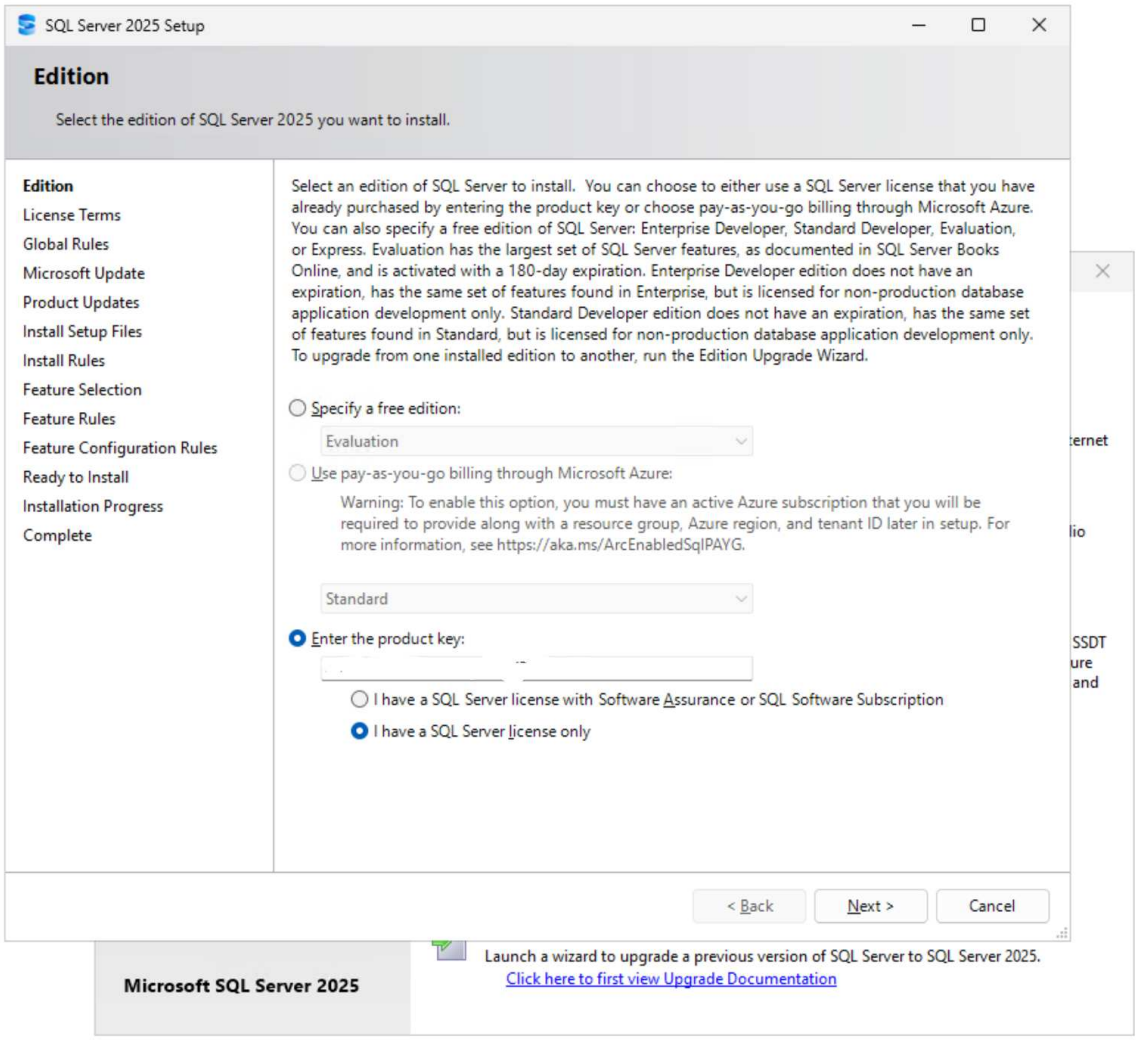
   ▼ **Show example**


SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
New SQL Server standalone installation or add features to an existing installation
Launch a wizard to install SQL Server 2025 in a non-clustered environment or to add features to an existing SQL Server 2025 instance.
Install Power BI Report Server
Launch a download page that provides a link to install Power BI Report Server. An internet connection is required to install PBIRS.
Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio (SSMS), SQL Server Profiler, and Database Tuning Advisor. An internet connection is required to install these tools.
Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2025 failover cluster.
This action is only available in the clustered environment.
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2025 failover cluster.
This action is only available in the clustered environment.
Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2025.
Click here to first view Upgrade Documentation
Microsoft SQL Server 2025


SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
SQL Server 2025
Please wait while Microsoft SQL Server 2025 Setup processes the current operation.
New SQL Server standalone installation or add features to an existing installation
Launch a wizard to install SQL Server 2025 in a non-clustered environment or to add features to an existing SQL Server 2025 instance.
Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Microsoft Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2025 failover cluster.
This action is only available in the clustered environment.
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2025 failover cluster.
This action is only available in the clustered environment.
Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2025.
Click here to first view Upgrade Documentation
Microsoft SQL Server 2025

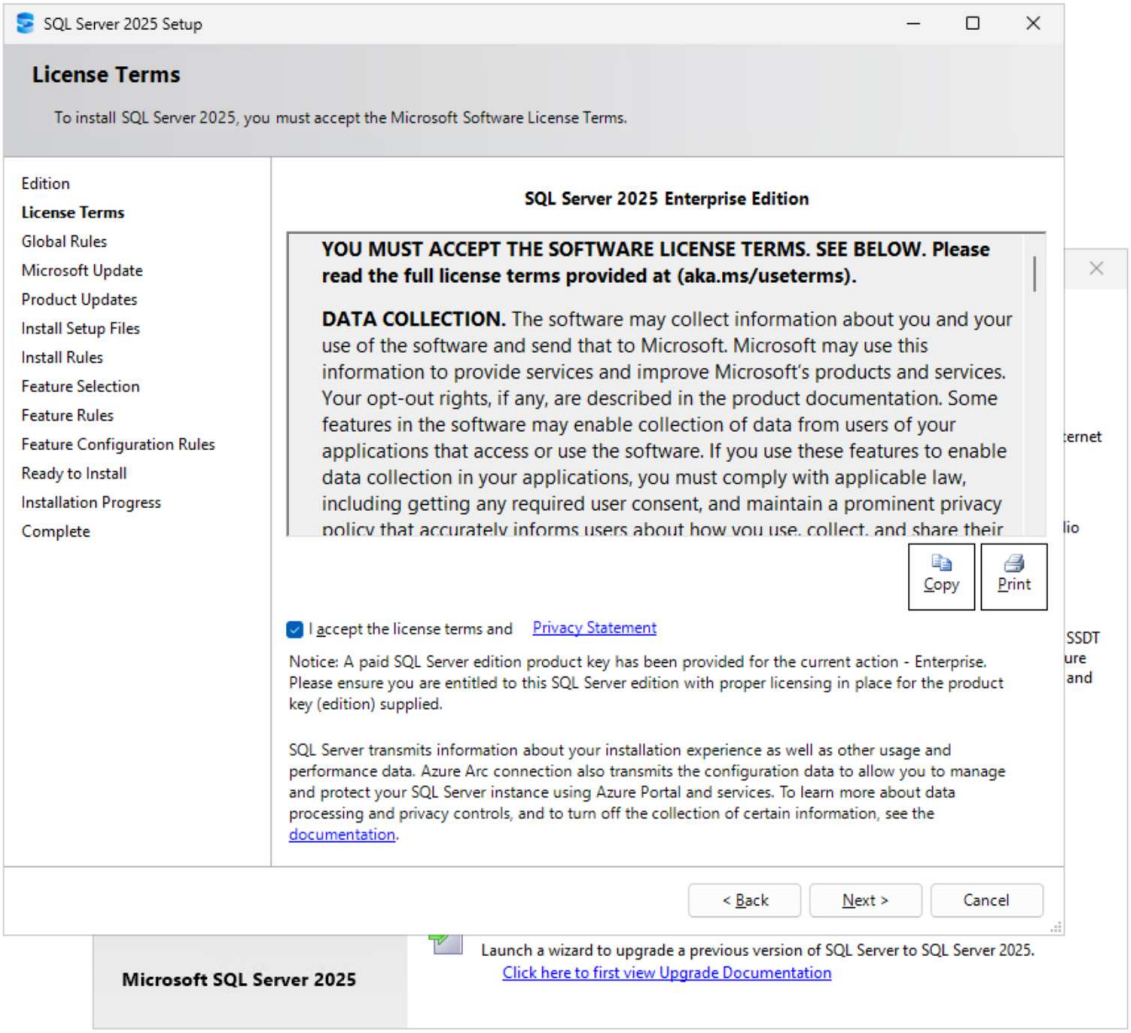
2. Select the SQL Server edition, accept the license terms, and let Setup check for product updates.
   a. On the **Edition** page, select **Enter the product key** and enter your product key, or select a free edition (Evaluation, Enterprise Developer, Standard Developer or Express). Select the license type that applies to you (**I have a SQL Server license only** in the lab) and click **Next**.

      ▼ Show example



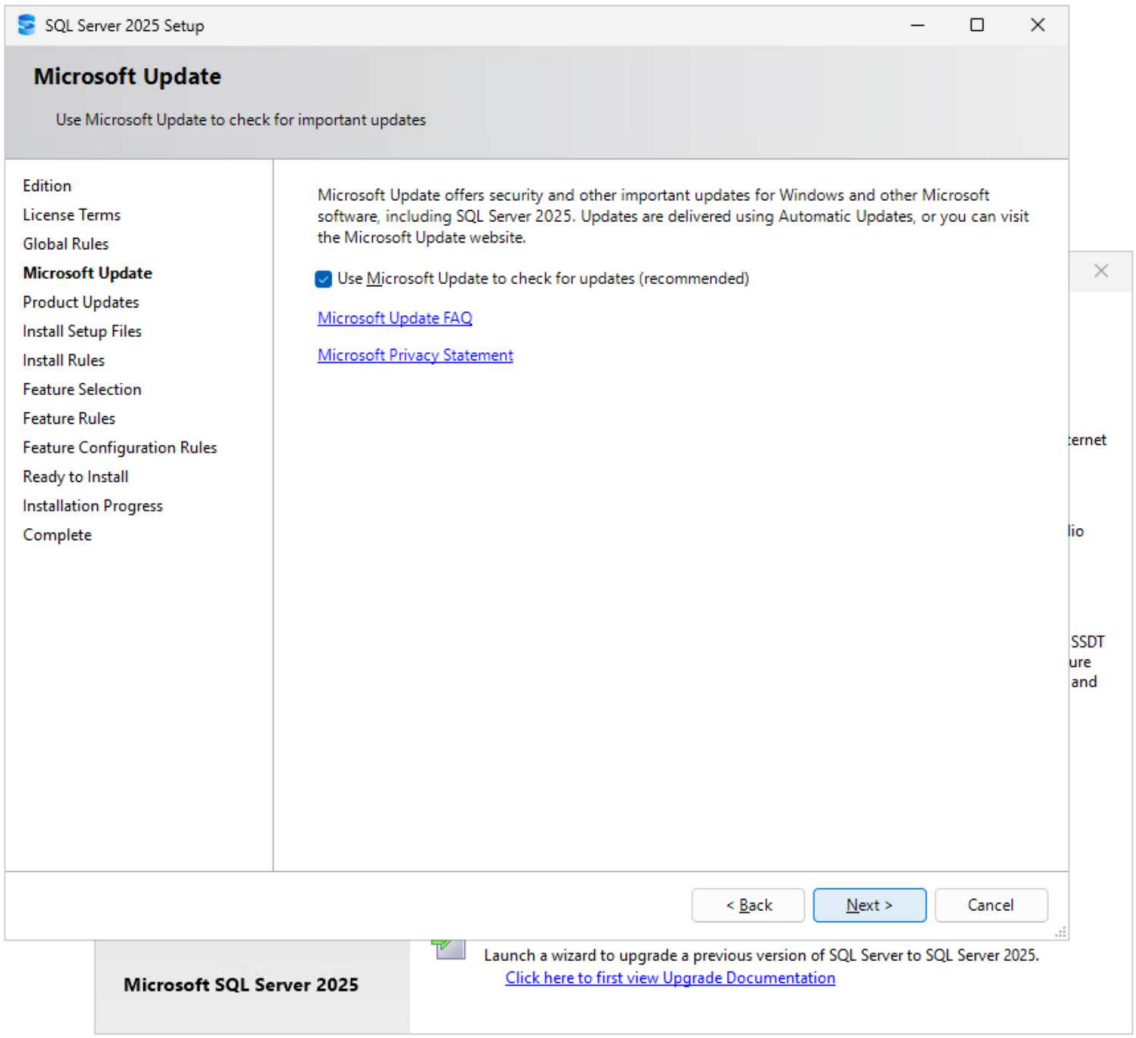
   b. On the **License Terms** page, read the terms, select **I accept the license terms and Privacy Statement**, and click **Next**.

      ▼ Show example



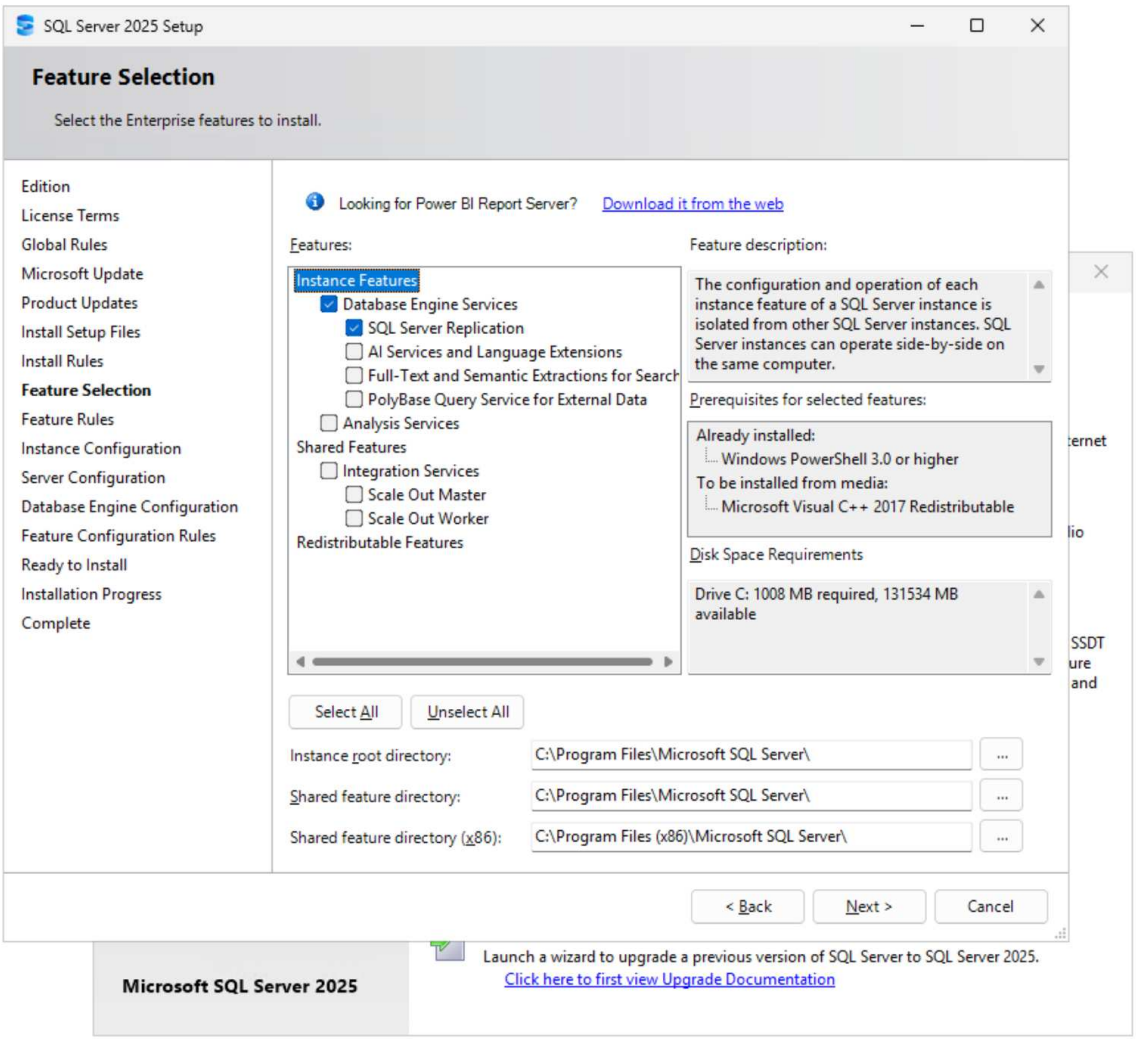
c. On the **Microsoft Update** page, select **Use Microsoft Update to check for updates (recommended)** and click **Next**. Setup then runs the **Global Rules**, **Product Updates**, **Install Setup Files** and **Install Rules** checks.

▼ Show example



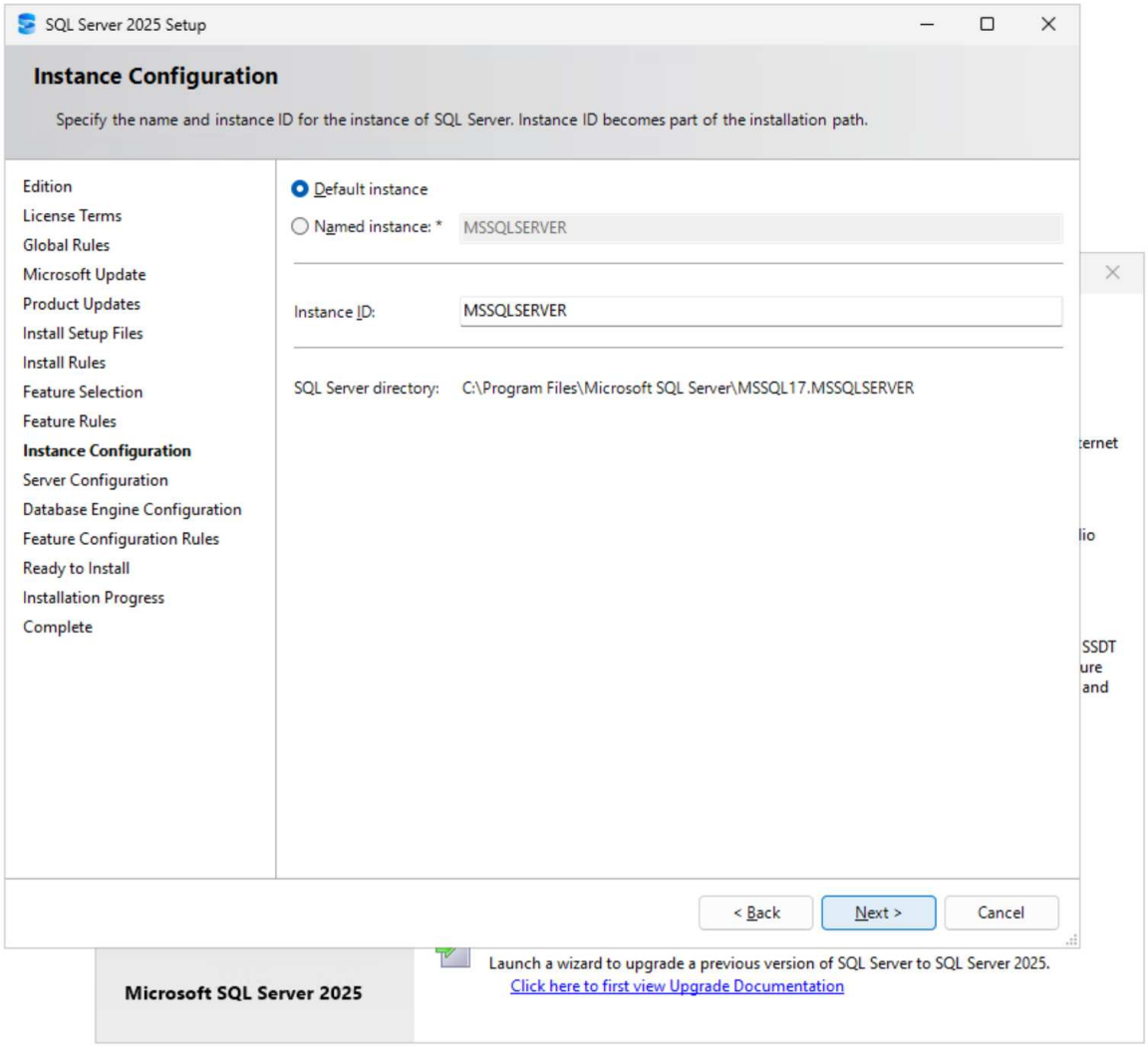
3. Select the SQL Server features and the instance to install. The binaries stay on the local disk; only the database files are placed on the SMB shares.
   a. On the **Feature Selection** page, select **Database Engine Services** and any additional features you need (the lab also selected **SQL Server Replication**). Leave the **Instance root directory** and **Shared feature directory** on the local disk `C:`. The binaries are installed locally; only the database files go to the SMB shares.

      ▼ Show example



b. On the **Instance Configuration** page, select **Default instance** (`MSSQLSERVER`), or enter a named instance, and click **Next**.

▼ Show example

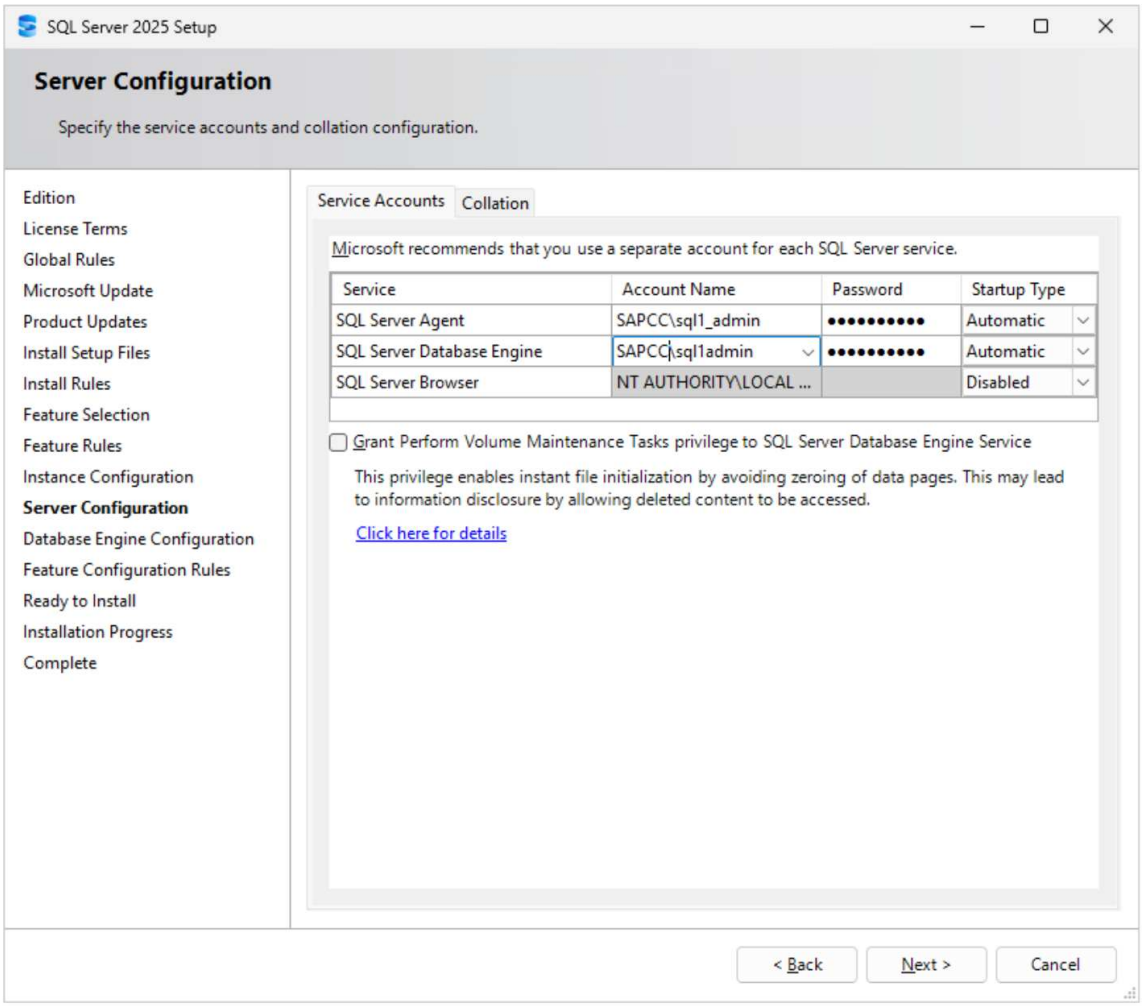


4. Configure the SQL Server Database Engine and SQL Server Agent services to run under a domain account that has access to the SMB shares.
   a. On the **Server Configuration** page, **Service Accounts** tab, enter the domain account and password for **SQL Server Agent** and **SQL Server Database Engine**, and set the **Startup Type** to **Automatic**.

> Use the domain account that has Full Control on the SMB shares. The screenshot shows two different spellings (`SAPCC\sql1_admin` and `SAPCC\sql1admin`). Make sure that every account you enter exists in Active Directory and has access to all four shares.

> Select **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service**. This enables instant file initialization, which speeds up database creation, file growth and restores considerably.

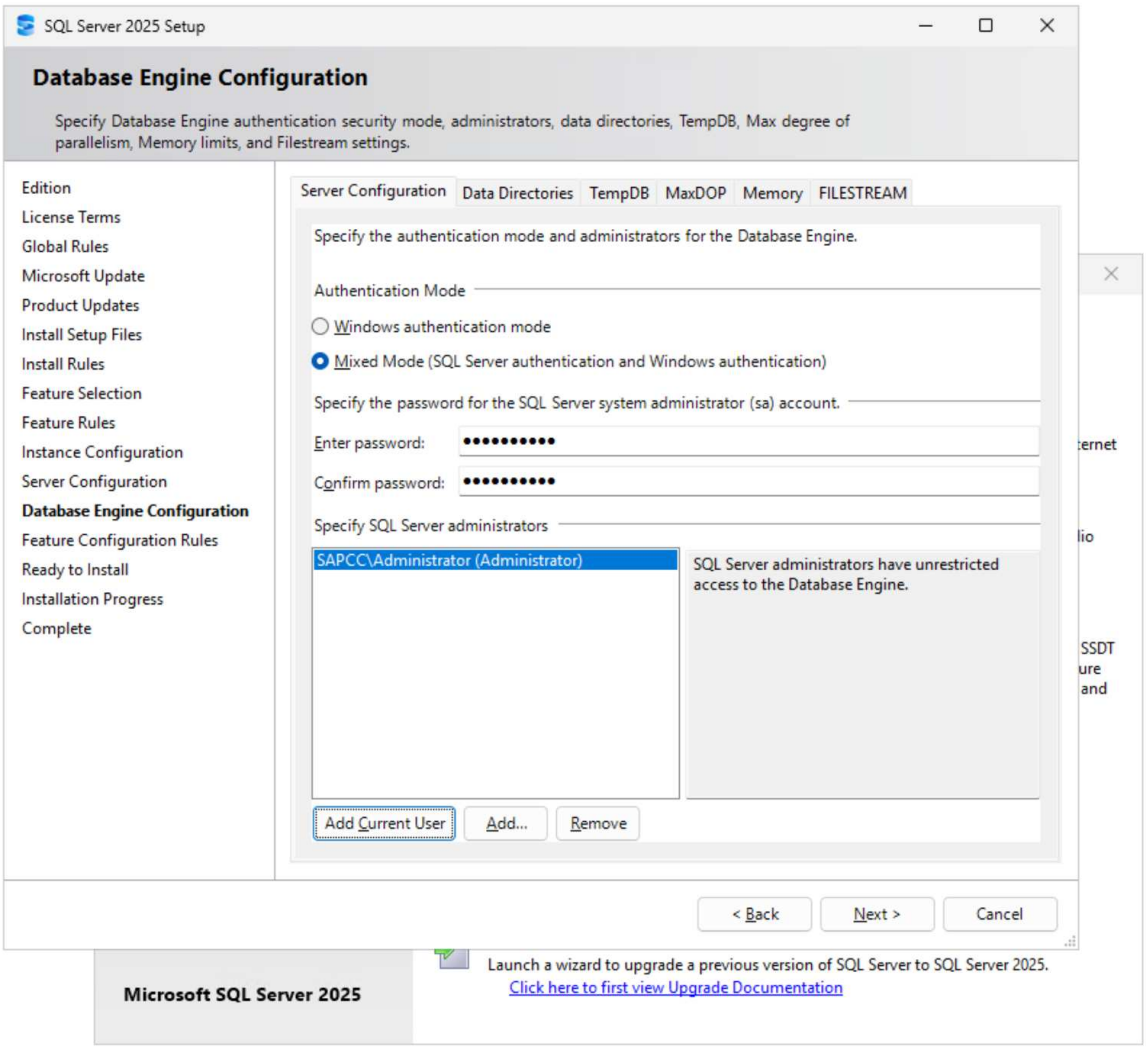
▼ Show example



5. Set the authentication mode and the SQL Server administrators, and enter the UNC paths of the SMB shares for the user database, transaction log, backup, and TempDB files.
   a. On the **Database Engine Configuration** page, **Server Configuration** tab, select the authentication mode. The lab uses **Mixed Mode** with a strong password for the `sa` account. Click **Add Current User** and **Add…** to add the SQL Server administrators (users or, preferably, an AD group).

      Use **Windows authentication mode** unless applications require SQL Server logins.

      ▼ Show example



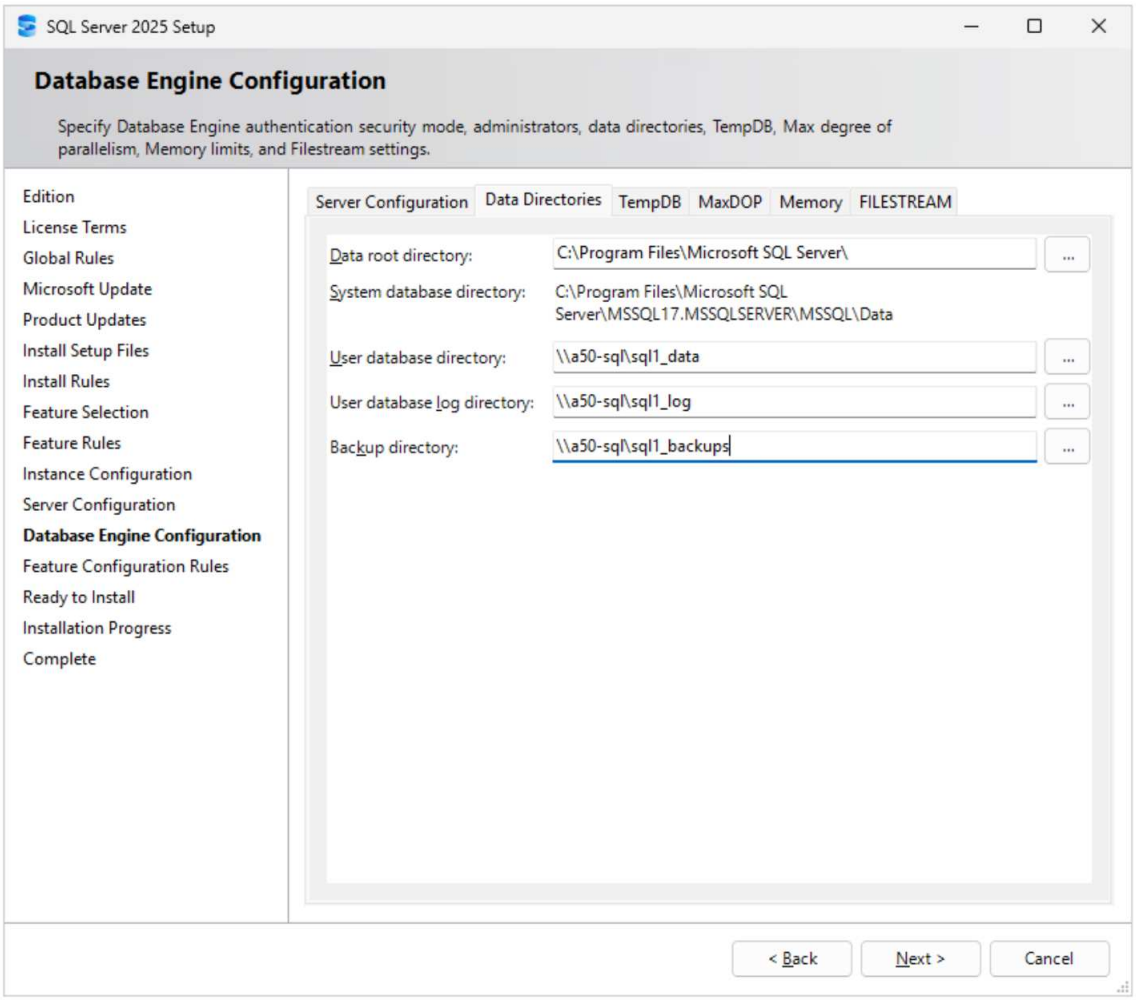
b. On the **Data Directories** tab, enter the UNC paths of the SMB shares:

Setting	Value
Data root directory	`C:\Program Files\Microsoft SQL Server\` (local; system databases stay on `C:`)
User database directory	`\\a50-sql\sql1_data`
User database log directory	`\\a50-sql\sql1_log`
Backup directory	`\\a50-sql\sql1_backups`

To place the system databases (`master`, `model`, `msdb`) on the SMB share as well, set **Data root directory** to a UNC path. Create a new volume and share for the system databases if this is desired.

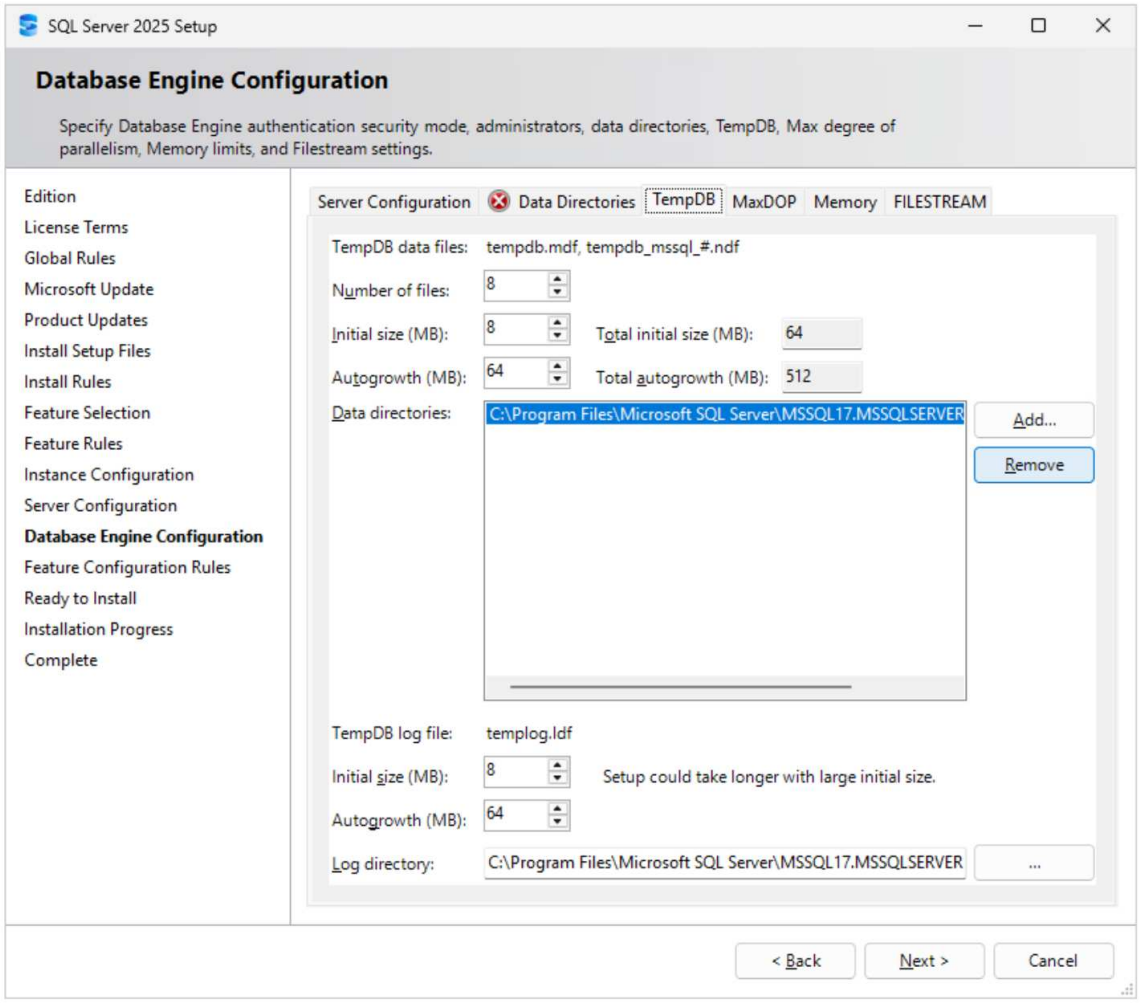
You need to use the UNC paths for the directories as mapped drives are not supported.

▼ **Show example**



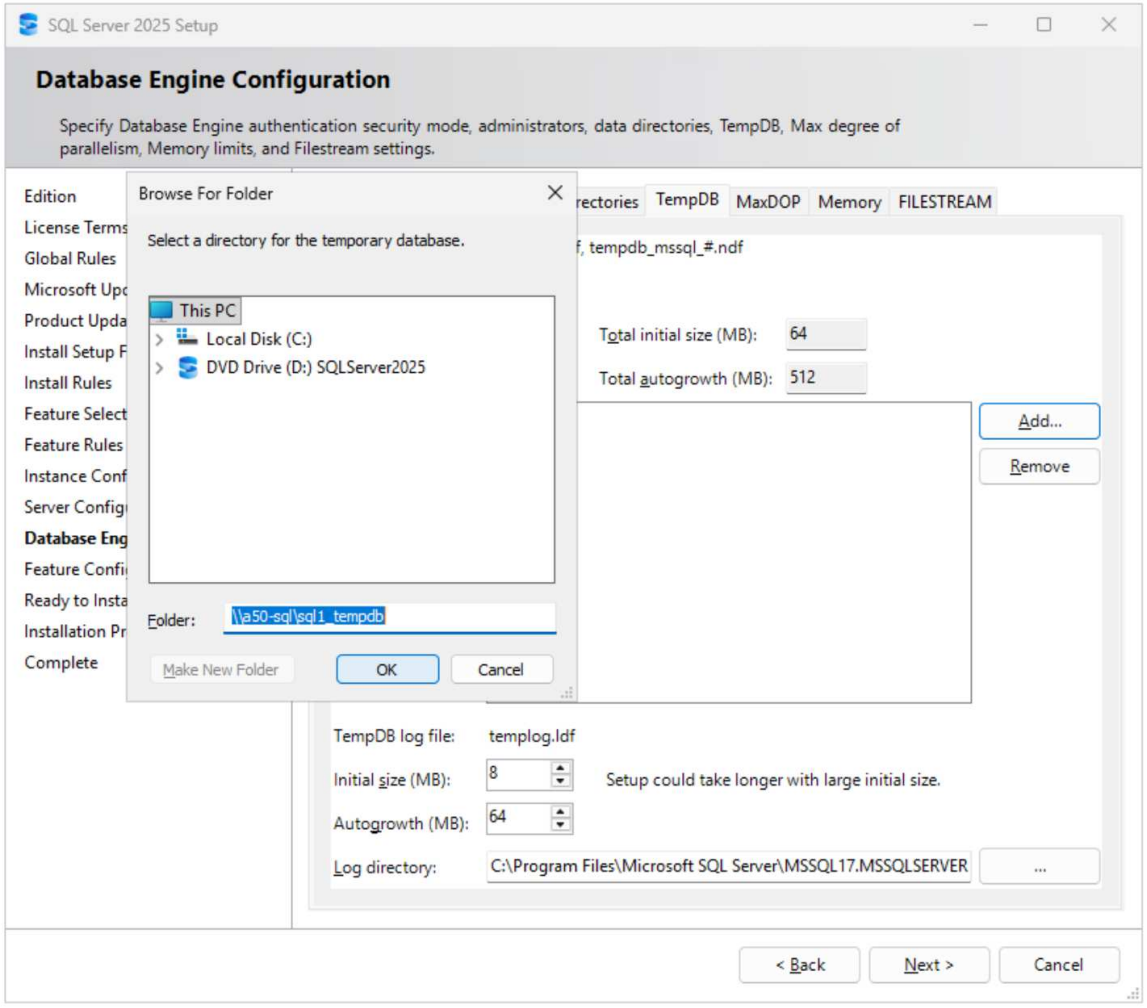
c. On the **TempDB** tab, select the default local data directory and click **Remove**.

▼ **Show example**



d. Click **Add…**. In the **Browse For Folder** dialog, type the UNC path `\\a50-sql\sql1_tempdb\data` into the **Folder** field and click **OK**.

▼ Show example

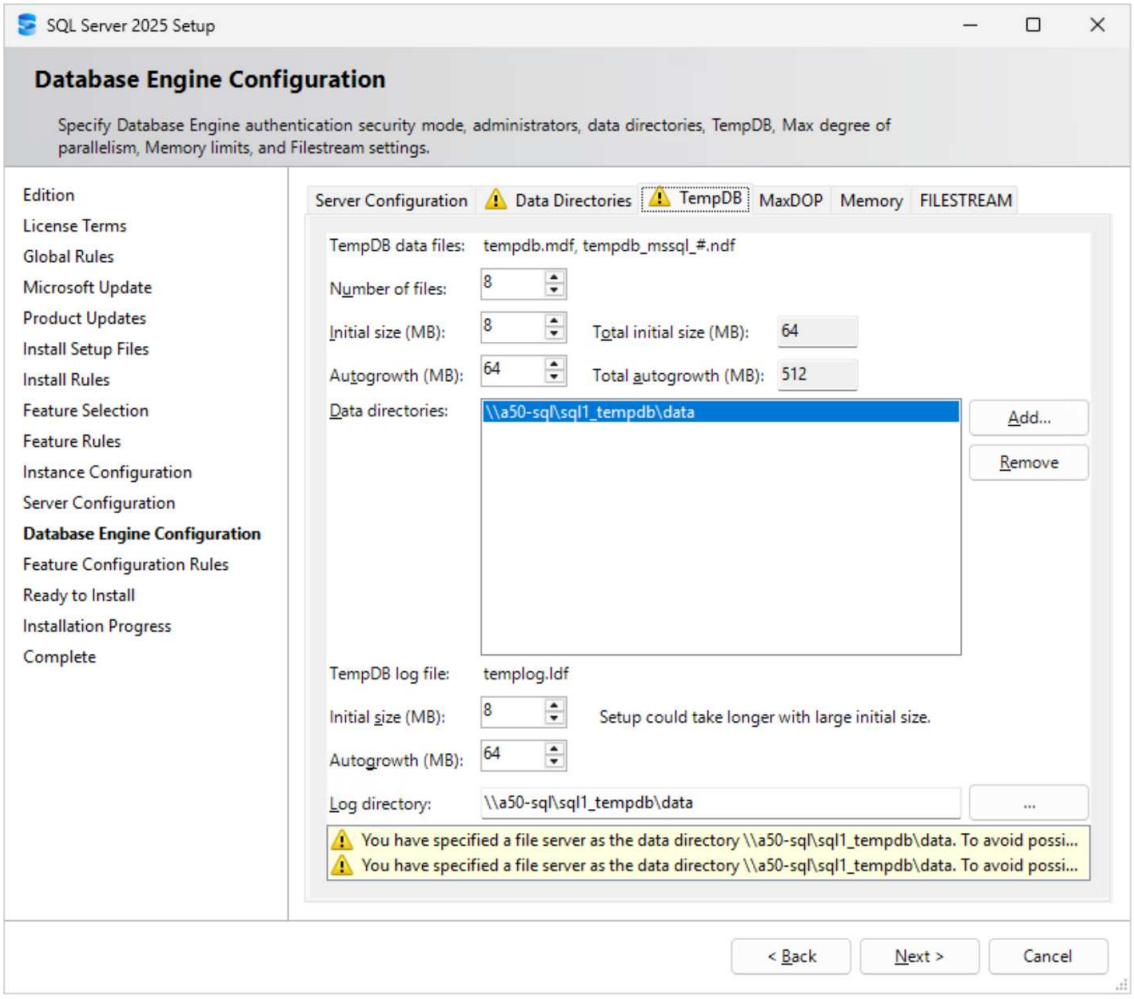


e. Set the **Log directory** to the same share (click **…**). The lab uses `\\a50-sql\sql1_tempdb\data` for both TempDB data files and the TempDB log file. The yellow warnings, which say that a file server was specified as the data directory, are expected.

Use one TempDB data file per logical CPU core, up to 8 files. Set the initial sizes to the expected TempDB working set so that TempDB doesn't need to grow during operation. All data files must have the same size and autogrowth.

You need to use a folder for the TempDB data and log files as otherwise the installation will fail.

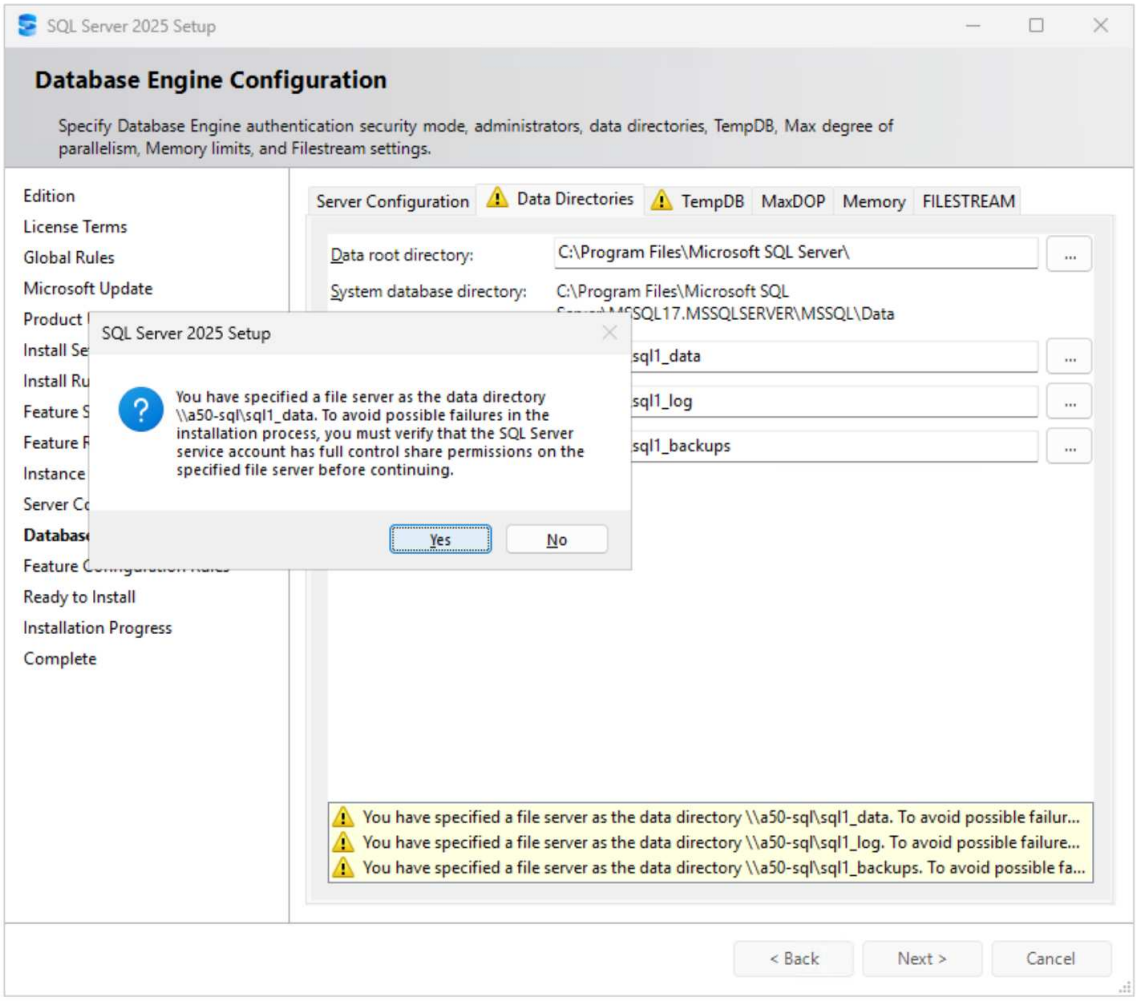
▼ **Show example**



f. Configure the **MaxDOP** and **Memory** tabs according to your sizing (the recommended defaults are a good starting point) and click **Next**.

g. For each UNC path, Setup displays a dialog asking you to verify that the SQL Server service account has Full Control share permissions on the file server. After you have verified the permissions (see Step 3: Create the SQL Server volumes and SMB shares and Step 6: Prepare Windows Server 2025), click **Yes**.

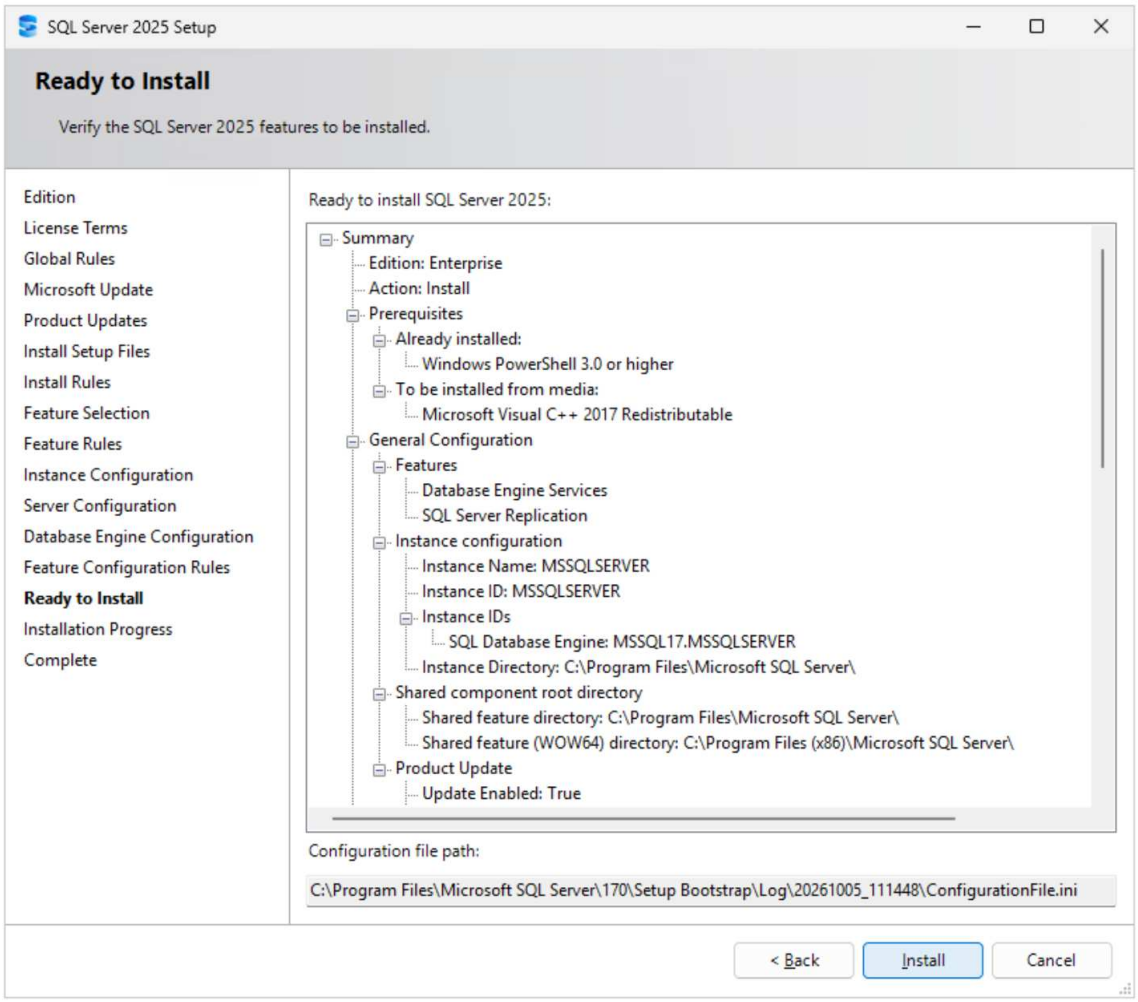
▼ Show example



6. Review the installation summary, run the installation, and confirm that all features installed successfully.
   a. On the **Ready to Install** page, review the summary and click **Install**.

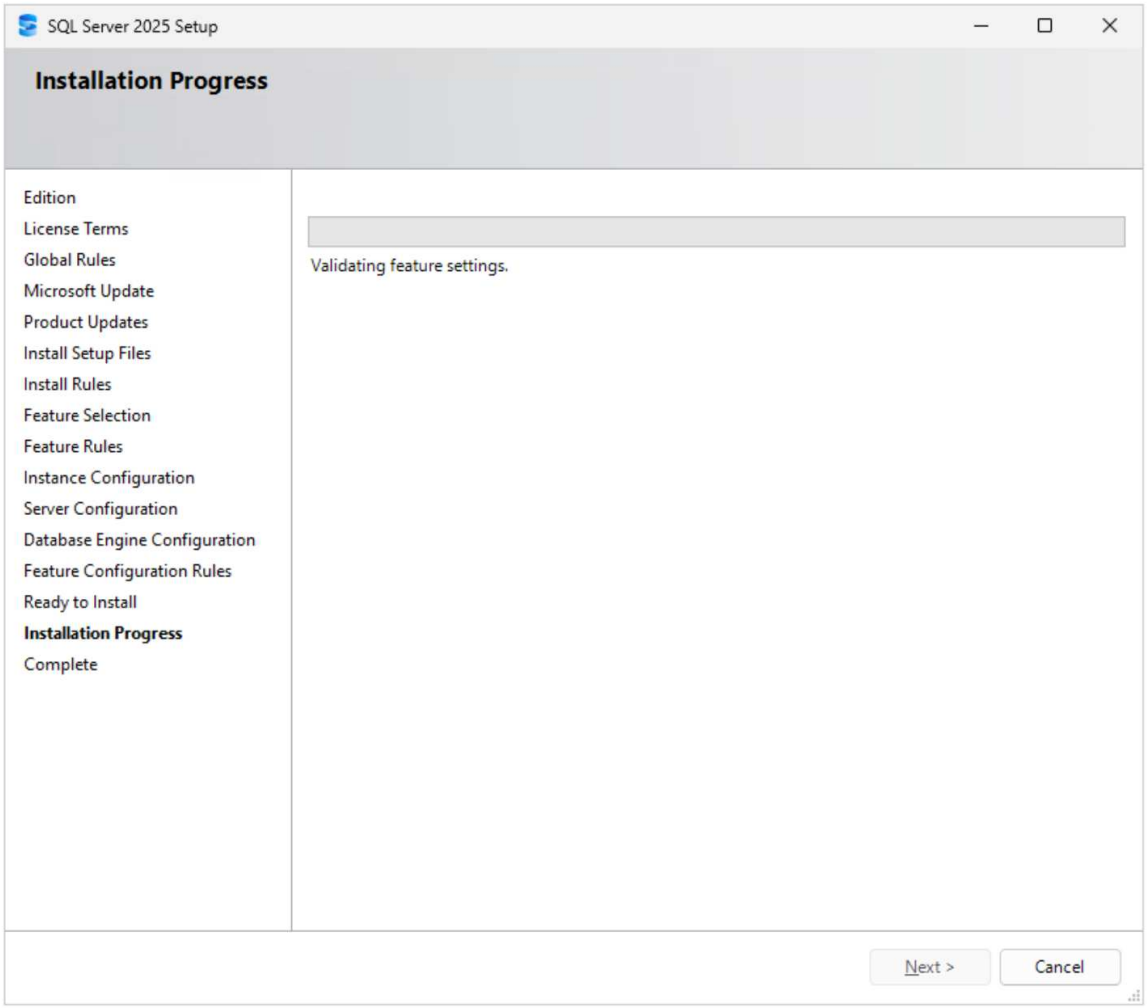
> Copy the `ConfigurationFile.ini` shown under **Configuration file path**. You can use it for unattended installations of additional SQL Server hosts (`setup.exe /ConfigurationFile=<path>`).

▼ Show example



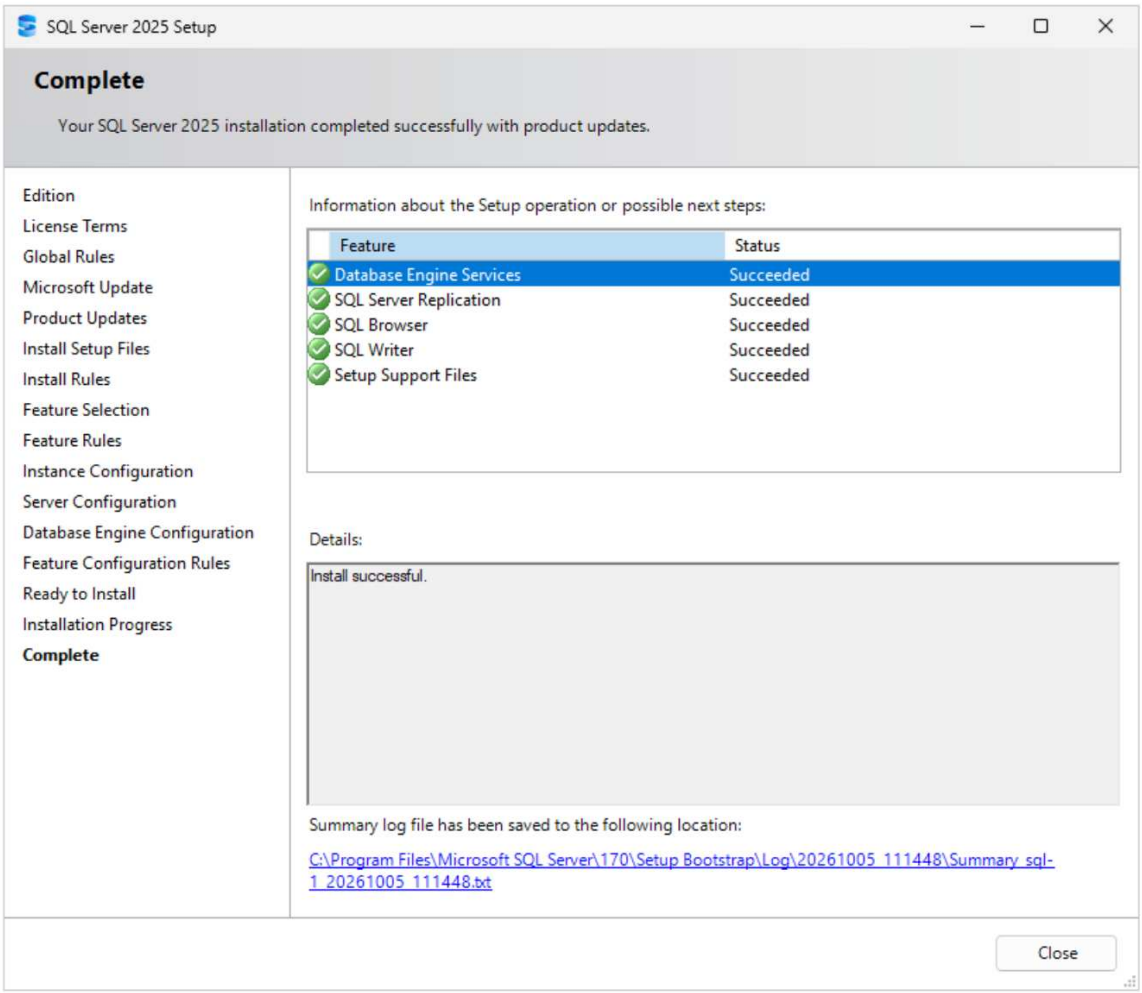
b. Wait while the installation runs.

▼ **Show example**



c. When the installation is finished, verify that all features show **Succeeded** and click **Close**.

▼ Show example



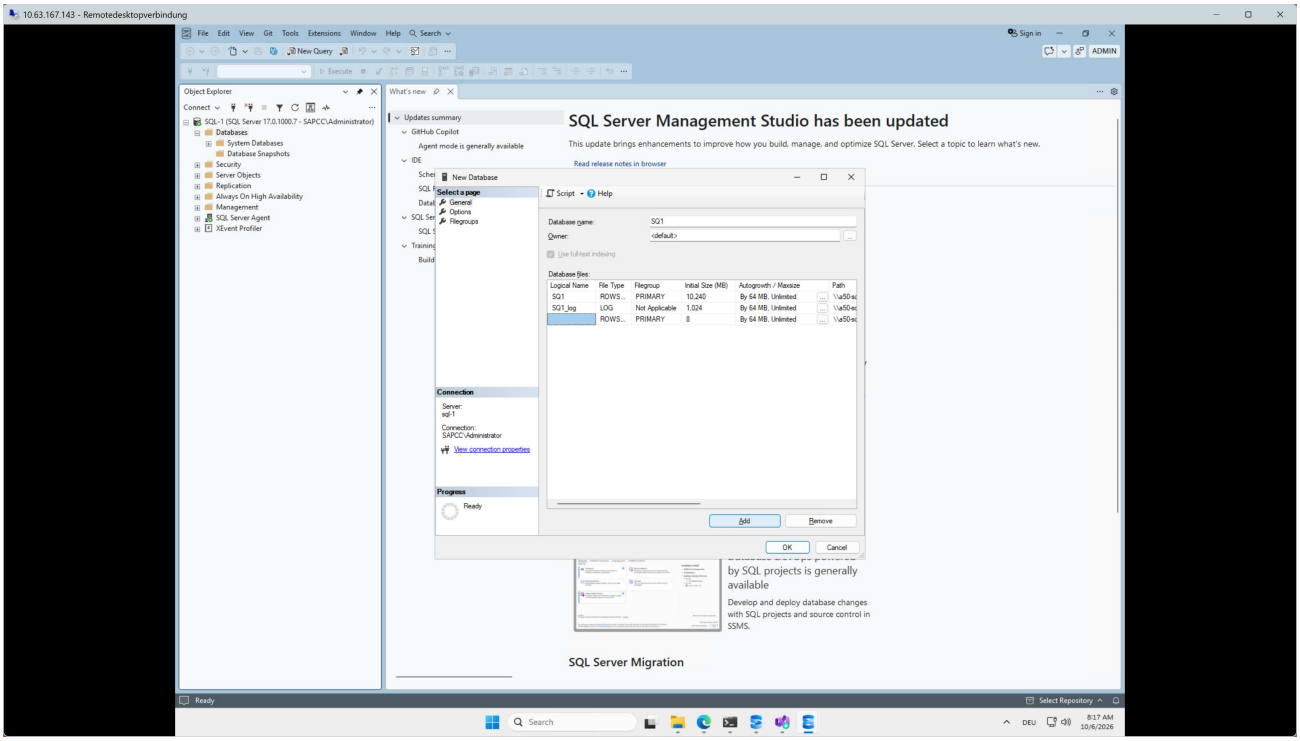
Step 8: Verify the installation and create a database

Create a test database with SQL Server Management Studio (SSMS) and verify that its data and log files are on the SMB shares. Optionally, confirm on ONTAP that the open files use continuous availability.

Steps

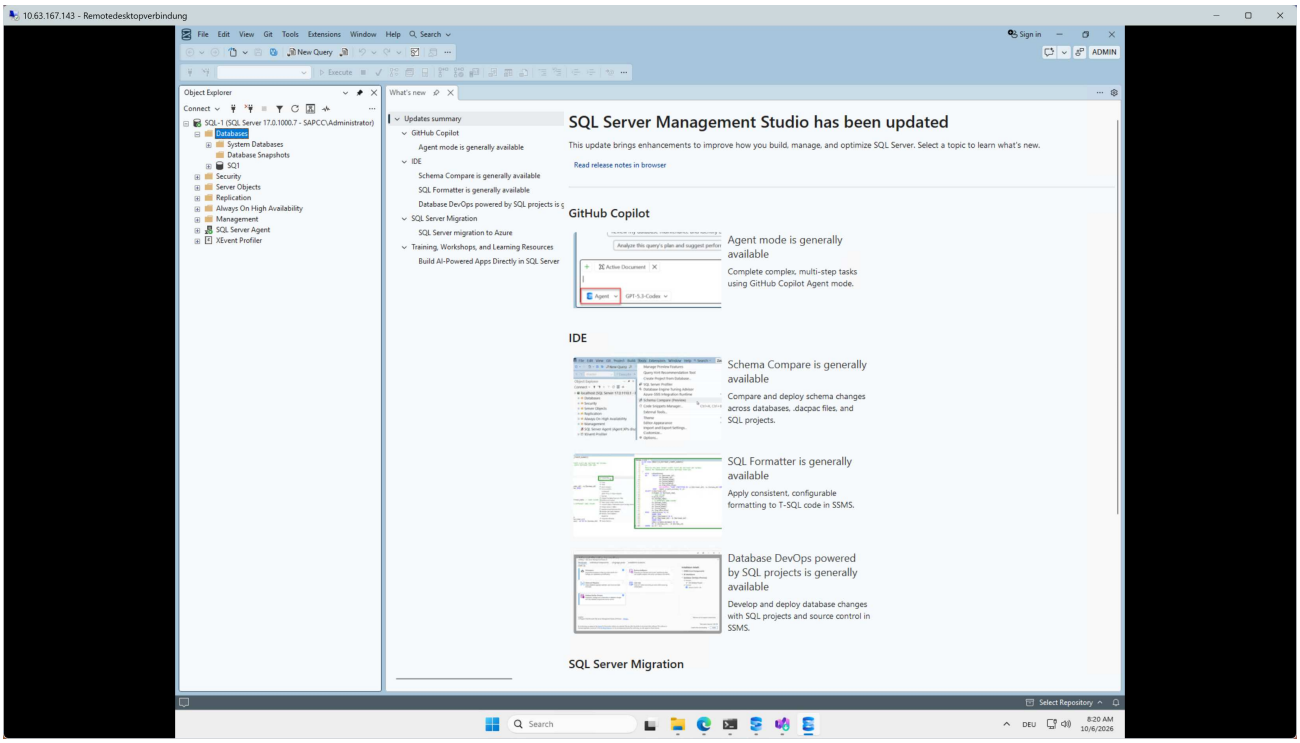
1. Install SQL Server Management Studio (SSMS) from the **Install SQL Server Management Tools** link in the Installation Center, or from the Microsoft website.
2. Start SSMS and connect to the instance (`sql-1`) with Windows authentication.
3. Right-click **Databases** and select **New Database…**. Enter a database name (`SQ1` in the lab), set the initial file sizes, and click **OK**. The data and log file paths default to `\\a50-sql\sql1_data` and `\\a50-sql\sql1_log`.

▼ **Show example**



4. The new database appears in **Object Explorer**.

▼ **Show example**



5. Verify the file locations with T-SQL:

```
SELECT DB_NAME(database_id) AS database_name,
       type_desc,
       name AS logical_name,
```

```
        physical_name,
        size * 8 / 1024 AS size_mb
FROM    sys.master_files
ORDER   BY database_id, type_desc;
```

6. Optional: verify the continuous availability of the open files on ONTAP:

```
cluster::> vserver cifs session show -vserver a50-sql
cluster::> vserver cifs session file show -vserver a50-sql -fields
share,path,continuously-available
```

All SQL Server files must show `continuously-available: Yes`.

Use an ONTAP CLI script to configure the storage in one pass

The following script contains the complete storage configuration from this procedure. Replace the values in angle brackets before you run it.

```
# --- SVM
-----------------------------------------------------------------
vserver create -vserver a50-sql -rootvolume a50_sql_root -aggregate
<aggr_node1> -rootvolume-security-style ntfs
vserver modify -vserver a50-sql -allowed-protocols cifs

network interface create -vserver a50-sql -lif a50-sql_smb_n1 -service
-policy default-data-files -home-node <node1> -home-port <port> -address
192.168.175.138 -netmask <netmask>
network interface create -vserver a50-sql -lif a50-sql_smb_n2 -service
-policy default-data-files -home-node <node2> -home-port <port> -address
192.168.175.139 -netmask <netmask>

vserver services name-service dns create -vserver a50-sql -domains
sapcc.stl.netapp.com -name-servers <dns1>,<dns2>
vserver cifs create -vserver a50-sql -cifs-server A50-SQL -domain
sapcc.stl.netapp.com -ou CN=Computers

set -privilege advanced
vserver cifs options modify -vserver a50-sql -smb3-enabled true -is
-multichannel-enabled true -is-large-mtu-enabled true -copy-offload
-enabled true -shadowcopy-enabled true
set -privilege admin

# --- Volumes
-------------------------------------------------------------
volume create -vserver a50-sql -volume sql1_data    -aggregate
```

```
<aggr_node1> -size 1TB   -security-style ntfs -junction-path /sql1_data
-space-guarantee none -fractional-reserve 0 -percent-snapshot-space 5
-snapshot-policy none -autosize-mode grow -max-autosize 1.3TB
volume create -vserver a50-sql -volume sql1_log     -aggregate
<aggr_node2> -size 512GB -security-style ntfs -junction-path /sql1_log
-space-guarantee none -fractional-reserve 0 -percent-snapshot-space 5
-snapshot-policy none -autosize-mode grow -max-autosize 650GB
volume create -vserver a50-sql -volume sql1_tempdb  -aggregate
<aggr_node2> -size 500GB -security-style ntfs -junction-path /sql1_tempdb
-space-guarantee none -fractional-reserve 0 -percent-snapshot-space 0
-snapshot-policy none -autosize-mode grow -max-autosize 650GB
volume create -vserver a50-sql -volume sql1_backups -aggregate
<aggr_node1> -size 2000GB -security-style ntfs -junction-path
/sql1_backups -space-guarantee none -fractional-reserve 0 -percent
-snapshot-space 5 -snapshot-policy none -autosize-mode grow -max-autosize
2600GB

# --- CA shares
-------------------------------------------------------------
vserver cifs share create -vserver a50-sql -share-name sql1_data    -path
/sql1_data    -share-properties
oplocks,browsable,changenotify,continuously-available
vserver cifs share create -vserver a50-sql -share-name sql1_log     -path
/sql1_log     -share-properties
oplocks,browsable,changenotify,continuously-available
vserver cifs share create -vserver a50-sql -share-name sql1_tempdb  -path
/sql1_tempdb  -share-properties
oplocks,browsable,changenotify,continuously-available
vserver cifs share create -vserver a50-sql -share-name sql1_backups -path
/sql1_backups -share-properties
oplocks,browsable,changenotify,continuously-available

# --- Share permissions (repeat for each share)
-----------------------------
vserver cifs share access-control create -vserver a50-sql -share sql1_data
-user-or-group SAPCC\sql1admin -permission Full_Control
vserver cifs share access-control delete -vserver a50-sql -share sql1_data
-user-or-group Everyone

# --- Verification
-------------------------------------------------------------
vserver cifs show -vserver a50-sql
vserver cifs share show -vserver a50-sql -fields share-name,path,share-
properties
vserver cifs session file show -vserver a50-sql -fields
share,path,continuously-available
```

Distribute the volumes across the aggregates of both nodes, for example data and backups on node 1, and log and TempDB on node 2. This uses the resources of both controllers.

Additional information

For more information about the topics in this procedure, see the following resources:

- NetApp: Microsoft SQL Server and SMB with ONTAP
- NetApp: Configure ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions
- NetApp: SMB server and volume requirements for SQL Server over SMB
- Microsoft: Install SQL Server with SMB fileshare storage
- NetApp: SnapCenter Plug-in for Microsoft SQL Server overview
- NetApp: Interoperability Matrix Tool (IMT)

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.