SQL Server auf NetApp AFF

NetApp database solutions

NetApp
November 16, 2026

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

Inhalt

SQL Server auf NetApp AFF . . . 1
Informationen zu SQL Server 2025 auf NetApp AFF mit kontinuierlicher Verfügbarkeit von SMB 3 . . . 1
Vorteile von SQL Server auf SMB 3 mit NetApp ONTAP . . . 1
Lösungskomponenten . . . 2
Gestaltungsprinzipien . . . 3
Wie kontinuierliche Verfügbarkeit funktioniert . . . 4
Bereitstellung von SQL Server 2025 auf NetApp AFF mithilfe von SMB 3 kontinuierlich verfügbaren Freigaben . . . 5
Umfang . . . 5
Publikum . . . 5
Laborumgebung . . . 6
Voraussetzungen . . . 6
Schritt 1: ONTAP Cluster vorbereiten . . . 7
Schritt 2: Erstellen und Konfigurieren der Storage VM (SVM) . . . 8
Schritt 3: Erstellen der SQL Server Volumes und SMB-Freigaben . . . 13
Schritt 4: Anpassen der Volume-Einstellungen . . . 17
Schritt 5: Kontinuierliche Verfügbarkeit für die SMB-Freigaben aktivieren . . . 20
Schritt 6: Windows Server 2025 vorbereiten . . . 23
Schritt 7: Installation von SQL Server 2025 . . . 24
Schritt 8: Installation überprüfen und eine Datenbank erstellen . . . 41
Mit einem ONTAP CLI Skript lässt sich der Storage in einem Schritt konfigurieren . . . 43
Weitere Informationen . . . 45

SQL Server auf NetApp AFF

Informationen zu SQL Server 2025 auf NetApp AFF mit kontinuierlicher Verfügbarkeit von SMB 3

SQL Server 2025 kann Datenbanken auf SMB 3-Freigaben mit kontinuierlicher Verfügbarkeit (CA) auf einem NetApp AFF System mit ONTAP speichern. Beschrieben werden die Vorteile, Lösungskomponenten und Designprinzipien dieser Konfiguration sowie die Frage, wie die kontinuierliche Verfügbarkeit Datenbanken während eines Controller-Failover online hält.

Microsoft SQL Server unterstützt seit SQL Server 2012 das Speichern von Datenbankdateien auf SMB-Dateifreigaben. Mit SMB 3 Continuously Available (CA)-Freigaben ist eine Dateifreigabe eine unterstützte Storage-Option für SQL Server-Datenbanken und eine Alternative zu Block-Storage (iSCSI- oder FCP-LUNs).

ONTAP auf AFF All-Flash-Systemen implementiert SMB 3 nativ. In Kombination mit SQL Server 2025 und Windows Server 2025 bietet dies eine fehlertolerante Storage-Architektur, die in den Datenschutz von NetApp integriert ist.

Informationen zum Einsetzen dieser Konfiguration finden Sie unter "Bereitstellung von SQL Server 2025 auf NetApp AFF mithilfe von SMB 3 kontinuierlich verfügbaren Freigaben".

Vorteile von SQL Server auf SMB 3 mit NetApp ONTAP

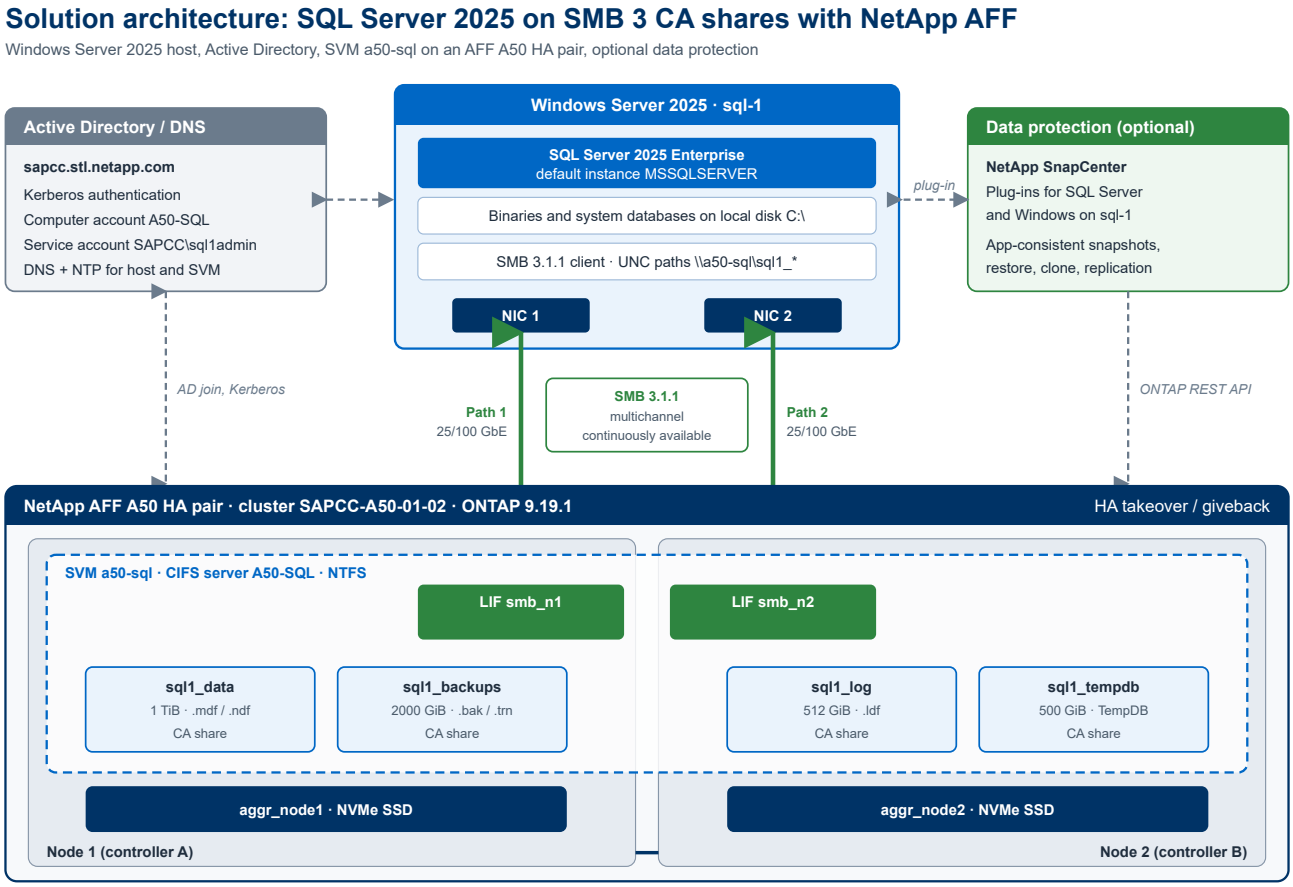
Nutzen	Beschreibung
Einfache Provisionierung	Es gibt keine LUNs, igroups, MPIO, Datenträgerinitialisierung oder Laufwerksbuchstaben zu managen. Der Speicherort einer Datenbankdatei ist lediglich ein UNC-Pfad wie `\\a50-sql\sql1_data`.
Online-Kapazitätsmanagement	Sie vergrößern (oder verkleinern) ein Volume online in ONTAP, und SQL Server erkennt die neue Kapazität sofort. Windows-Festplatten- oder Partitionsvorgänge sind nicht erforderlich, und autogrow kann dies automatisch übernehmen.
Unterbrechungsfreier Betrieb	CA-Freigaben gewährleisten den Betrieb von SQL Server während ONTAP Übernahmen und Rückgaben, unterbrechungsfreien Upgrades (NDU), LIF-Migrationen und Volume-Verschiebungen.
Performance und Ausfallsicherheit	SMB Multichannel verteilt die E/A auf mehrere Netzwerkpfade und Netzwerkkarten und übersteht den Ausfall eines einzelnen Pfades. SMB Freigaben unterstützen außerdem SQL Server Failoverclusterinstanzen (FCI).
Speichereffizienz	Inline-Deduplizierung, Komprimierung und Verdichtung reduzieren zusammen mit Thin Provisioning die von Datenbanken und Backups genutzte physische Kapazität.
Integrierter Datenschutz	ONTAP Snapshots, SnapRestore, FlexClone und SnapMirror, orchestriert von NetApp SnapCenter, ermöglichen Backups in Sekunden, Wiederherstellungen in Minuten und sofortige Datenbankklone.

Nutzen	Beschreibung
Flexibilität	Datenbanken lassen sich zwischen Hosts verschieben, indem sie einfach an einen anderen Server angebunden werden, ohne das Storage neu zuzuordnen. Dieselbe SVM kann auch Home-Verzeichnisse, Dateidienste oder andere Anwendungen bereitstellen.

Lösungskomponenten

Die Lösung besteht aus folgenden Komponenten:

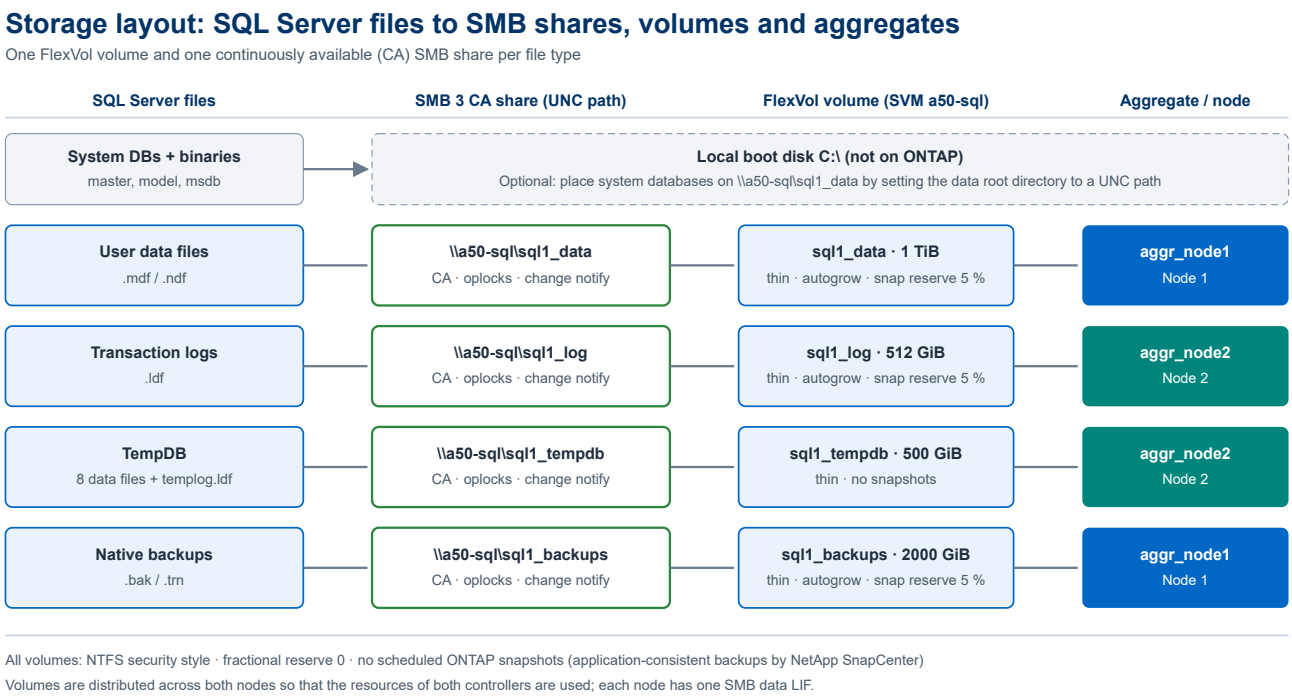
Komponente	Rolle
Windows Server 2025 Host (`sql-1`)	Verwendet SQL Server 2025. Die SQL Server Binärdateien und Systemdatenbanken befinden sich auf der lokalen Festplatte; auf alle Benutzerdatenbanken, Protokolle, TempDB und Backups wird über SMB 3 zugegriffen.
SQL Server 2025	Datenbank-Engine, die unter einem Domänendienstkonto ausgeführt wird (`SAPCC\sql1admin`), das Zugriff auf die SMB-Freigaben hat.
Active Directory und DNS	Authentifiziert das SQL Server-Dienstkonto und den CIFS-Server (Kerberos) und bietet Namensauflösung und Zeitsynchronisierung.
NetApp AFF A50 HA Paar	Zwei Controller mit gemeinsam genutztem NVMe Storage. Fällt ein Controller aus oder wird er aktualisiert, übernimmt der Partner dessen Storage und Netzwerkschnittstellen.
SVM `a50-sql`	Ein dedizierter, in Active Directory eingebundener CIFS-Server mit einem SMB-Daten-LIF pro Knoten, der vier Volumes mit CA-Freigaben hostet.



Gestaltungsprinzipien

Das Design folgt den NetApp Best Practices für SQL Server über SMB:

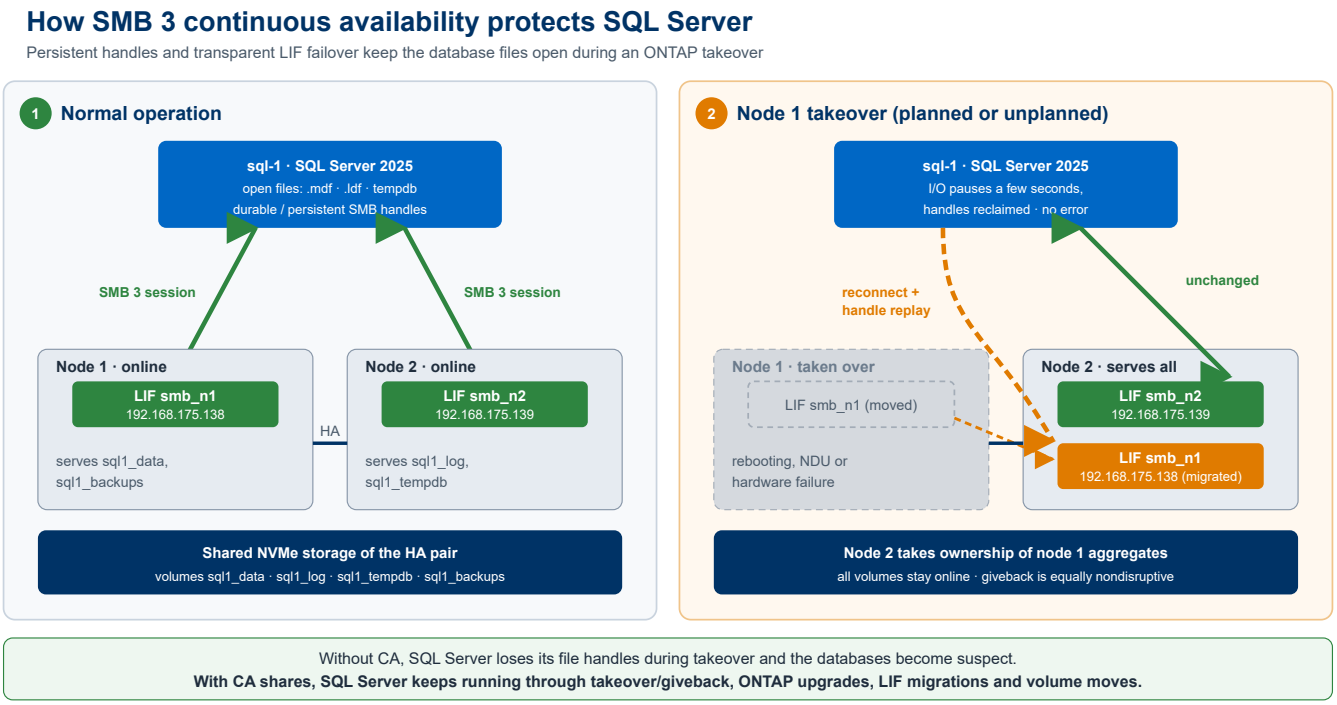
- **Separate Volumes pro Dateityp.** Daten, Transaktionsprotokolle, TempDB und Backups werden auf separaten FlexVol Volumes und Freigaben gespeichert. Jedes Volume kann eigene Einstellungen für Größe, QoS, Effizienz, Snapshots und Replikation haben. TempDB wird von Backups ausgeschlossen.
- **Die Volumes sind auf beide Knoten verteilt.** Daten- und Backup-Volumes befinden sich auf Knoten 1, Protokoll- und TempDB-Volumes auf Knoten 2, sodass beide Controller sinnvolle Arbeit leisten.
- **Ein SMB-Daten-LIF pro Knoten.** Der Host verfügt immer über einen direkten Pfad zu dem Knoten, dem ein Volume gehört, und SMB multichannel kann beide Pfade nutzen.
- **NTFS-Sicherheitsstil und CA-Freigaben.** Diese sind für SQL Server über SMB auf ONTAP obligatorisch.
- **Keine geplanten ONTAP Snapshots auf den Datenbankvolumes.** Backups müssen applikationskonsistent sein; sie werden von SnapCenter erstellt.



Wie kontinuierliche Verfügbarkeit funktioniert

Bei einer Standard-SMB-Freigabe schließt ein Controller-Failover die geöffneten Dateihandles. SQL Server kennzeichnet die betroffenen Datenbanken dann als verdächtig, und sie müssen manuell wiederhergestellt werden.

Bei einer CA-Freigabe hält ONTAP den Status der geöffneten Dateien (persistente Handles) auf den HA-Partner gespiegelt. Während eines Takeover migriert die SMB LIF des ausgefallenen Knotens zum Partner. Der SMB 3-Client auf dem SQL Server Host stellt die Verbindung automatisch wieder her und fordert seine Handles erneut an. SQL Server verzeichnet nur eine kurze I/O-Pause von wenigen Sekunden; die Datenbanken bleiben online, und es gehen keine Transaktionen verloren. Dasselbe gilt für geplante Ereignisse wie ONTAP Upgrades, Giveback, LIF-Migrationen und Volume-Verschiebungen.



Bereitstellung von SQL Server 2025 auf NetApp AFF mithilfe von SMB 3 kontinuierlich verfügbaren Freigaben

Bereitstellung von SQL Server 2025 auf Windows Server 2025 mit Benutzerdatenbanken, Transaktionsprotokollen, TempDB und Backups auf kontinuierlich verfügbaren SMB 3-Freigaben auf einem NetApp AFF System. Dieses Verfahren umfasst die Konfiguration der ONTAP SVM, Volumes und Freigaben, die Installation von SQL Server und den Schutz der Datenbanken mit SnapCenter.

Umfang

Dieses Verfahren setzt eine eigenständige SQL Server 2025 Instanz auf einem einzelnen Windows Server 2025 Host ein, wobei sich Benutzerdatenbanken, Transaktionsprotokolle, TempDB und Backups auf SMB 3 Freigaben mit kontinuierlicher Verfügbarkeit (CA) befinden. Dasselbe Storage Design gilt für SQL Server Failoverclusterinstanzen (FCI) und Always On Verfügbarkeitsgruppen, ihre clusterspezifische Konfiguration wird jedoch nicht behandelt. SQL Server Performance Tuning und Dimensionierung fallen ebenfalls nicht in den Geltungsbereich. Eine Beschreibung der Vorteile, Lösungskomponenten, Designprinzipien und der Funktionsweise der kontinuierlichen Verfügbarkeit ist unter "Informationen zu SQL Server 2025 auf NetApp AFF mit kontinuierlicher Verfügbarkeit von SMB 3" zu finden.

Publikum

Dieses Verfahren ist bestimmt für:

- **Storage-Administratoren**, die den ONTAP Cluster, die SVM, die Volumes und die SMB-Freigaben konfigurieren.
- **Windows und Active Directory Administratoren**, die den Windows Server 2025 Host, die Dienstkonten und das Netzwerk vorbereiten.

- **Datenbankadministratoren**, die SQL Server 2025 installieren und konfigurieren sowie Backup und Recovery einrichten.

Grundkenntnisse in der Administration von ONTAP System Manager, Windows Server und SQL Server werden vorausgesetzt.

Laborumgebung

Die Screenshots in diesem Verfahren stammen aus der folgenden Laborumgebung. Anstelle dieser Werte sind die Werte Ihrer Umgebung zu verwenden.

Komponente	Im Labor verwendeter Wert
Speichersystem	NetApp AFF A50 HA-Paar, Cluster `SAPCC-A50-01-02`, ONTAP 9.19.1
SVM	`a50-sql` (CIFS-Servername `A50-SQL`)
SMB Daten-LIFs	192.168.175.138 (Knoten 1), 192.168.175.139 (Knoten 2)
Active Directory Domäne	`SAPCC` (`sapcc.stl.netapp.com`)
SQL Server Host	`sql-1.sapcc.stl.netapp.com`, Windows Server 2025 Datacenter (Desktopdarstellung)
SQL-Server	SQL Server 2025 Enterprise Edition (17.0.1000.7), Standardinstanz `MSSQLSERVER`
SQL Server Dienstkonto	`SAPCC\sql1admin` (Domänenkonto)

Volume / Freigabe	Größe	UNC Pfad	Inhalt
`sql1_data`	1024 GiB	`\\a50-sql\sql1_data`	Datendateien der Benutzerdatenbank (`.mdf`, `.ndf`)
`sql1_log`	512 GiB	`\\a50-sql\sql1_log`	Protokolldateien für Datenbanktransaktionen des Benutzers (`.ldf`)
`sql1_tempdb`	500 GiB	`\\a50-sql\sql1_tempdb`	TempDB Daten- und Protokolldateien
`sql1_backups`	2000 GiB	`\\a50-sql\sql1_backups`	Native SQL Server Sicherungsdateien (`.bak`, `.trn`)



Für Daten, Protokolle, TempDB und Backups empfiehlt sich die Verwendung separater Volumes. Dadurch können pro Volume unterschiedliche QoS-, Snapshot-, Effizienz- und Replikationseinstellungen festgelegt werden. Außerdem wird so verhindert, dass die sich ständig ändernde TempDB in die Snapshots Ihrer Benutzerdatenbanken aufgenommen wird.

Voraussetzungen

Vor dem Start müssen die folgenden Voraussetzungen erfüllt sein:

NetApp ONTAP

- Das AFF HA Paar ist installiert und der Cluster ist eingerichtet und betriebsbereit.

- Die CIFS (SMB)-Lizenz ist installiert. Sie ist in ONTAP One enthalten.
- Auf jedem Knoten existiert mindestens ein Datenaggregat (lokale Ebene).
- Die Uhrzeit des Clusters und von Active Directory wird über NTP synchronisiert. Die maximal zulässige Zeitabweichung für Kerberos beträgt 5 Minuten.
- Die Datennetzwerk-Ports, die Broadcast-Domäne und (optional) die VLANs für die SMB LIFs sind konfiguriert.

Active Directory und DNS

- Eine Active Directory Domäne ist verfügbar, und die DNS-Server sind von den SVM-Daten-LIFs aus erreichbar.
- Sie verfügen über ein Konto mit der Berechtigung, Computerobjekte in der Ziel-OU für den CIFS-Server zu erstellen.
- Für SQL Server Database Engine und SQL Server Agent services ist ein dediziertes Domänenbenutzerkonto als Dienstkonto verfügbar.

> SQL Server muss unter einem Domänenkonto ausgeführt werden, wenn sich seine Dateien auf einer SMB-Freigabe befinden. Integrierte virtuelle Konten (`NT SERVICE\MSSQLSERVER`) und lokale Konten können keinen Zugriff auf eine Remote-Dateifreigabe erhalten.

Windows Server

- Windows Server 2025 (Desktop Experience) ist installiert, gepatcht und in die Domäne aufgenommen.
- Die Installationsmedien (ISO) für SQL Server 2025 und ein gültiger Produktschlüssel (oder eine kostenlose Edition) sind verfügbar.

SMB Anforderungen und Einschränkungen für SQL Server auf ONTAP

- SMB 3.0 oder höher muss auf der SVM aktiviert sein.
- Alle Volumes, die CA-Freigaben hosten, müssen den **NTFS**-Sicherheitsstil verwenden und von Anfang an den NTFS-Stil gehabt haben.
- SMB Direct (RDMA) wird nicht unterstützt.
- ReFS wird nicht unterstützt. ONTAP (WAFL) stellt das Dateisystem für die Freigaben bereit.

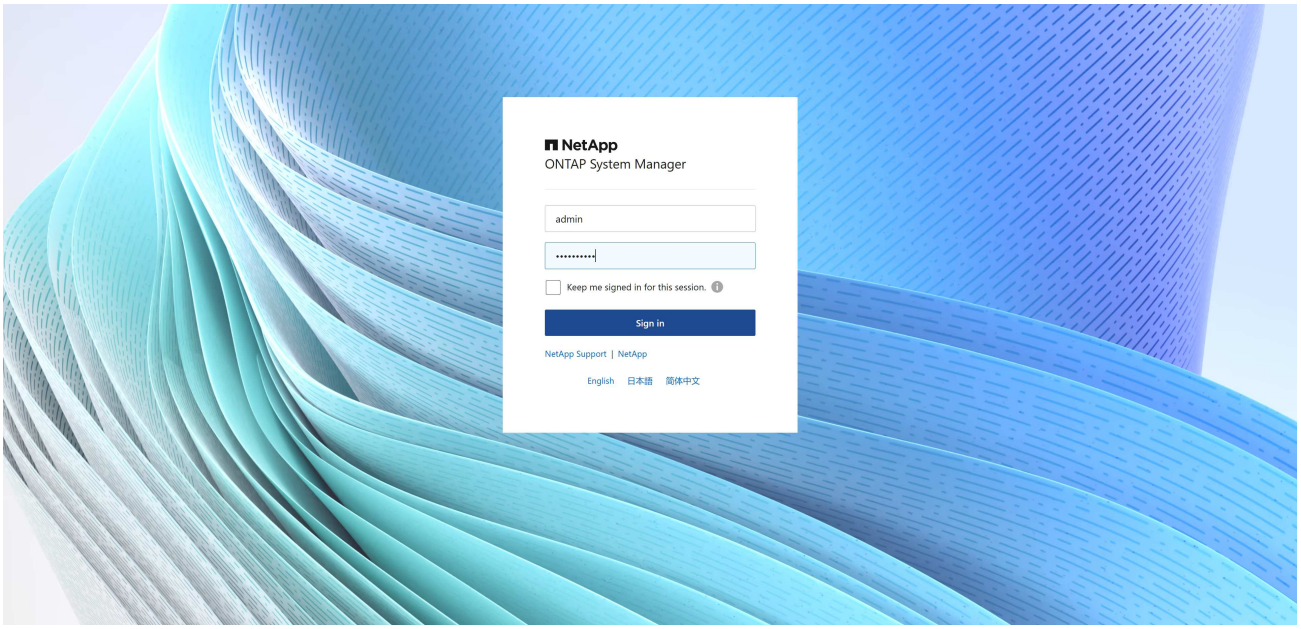
Schritt 1: ONTAP Cluster vorbereiten

Die Verbindung zu ONTAP System Manager muss bestehen, und die Clusterzeit muss mit Active Directory synchronisiert sein. Die Kerberos-Authentifizierung für die SMB-Freigaben schlägt fehl, wenn die Zeitabweichung 5 Minuten überschreitet.

Schritte

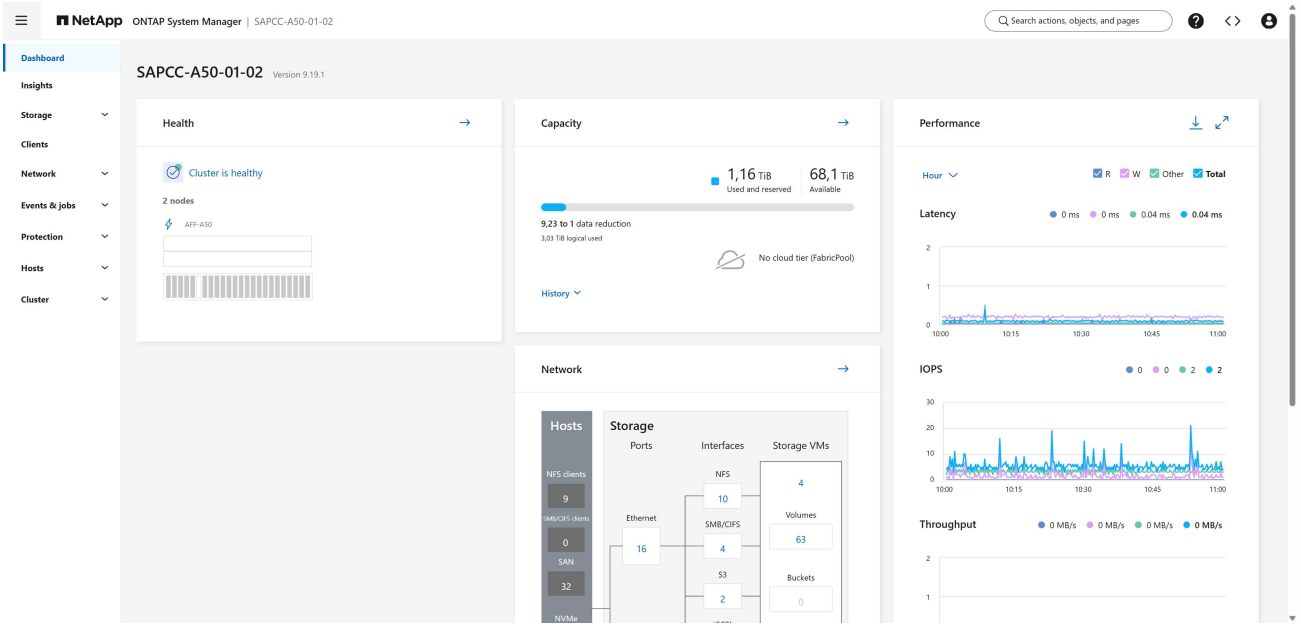
1. Sie stellen in einem Webbrowser eine Verbindung zum ONTAP System Manager unter `https://<cluster-management-IP>` her. Sie melden sich mit dem Cluster-Administratorkonto an.

   ▼ Beispiel anzeigen



2. Das **Dashboard** ist der Einstiegspunkt für weitere Konfigurationen im System Manager.

▼ **Beispiel anzeigen**



3. Falls NTP noch nicht konfiguriert ist, lassen sich Ihre Domänencontroller oder die unternehmensinternen NTP-Server über die CLI hinzufügen (SSH zum Cluster-Management-LIF):

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

Schritt 2: Erstellen und Konfigurieren der Storage VM (SVM)

Für SQL Server sollte eine dedizierte SVM verwendet werden. Die SVM tritt Active Directory als CIFS-Server bei und stellt auf jedem Knoten des HA-Paars eine SMB-Daten-LIF bereit.

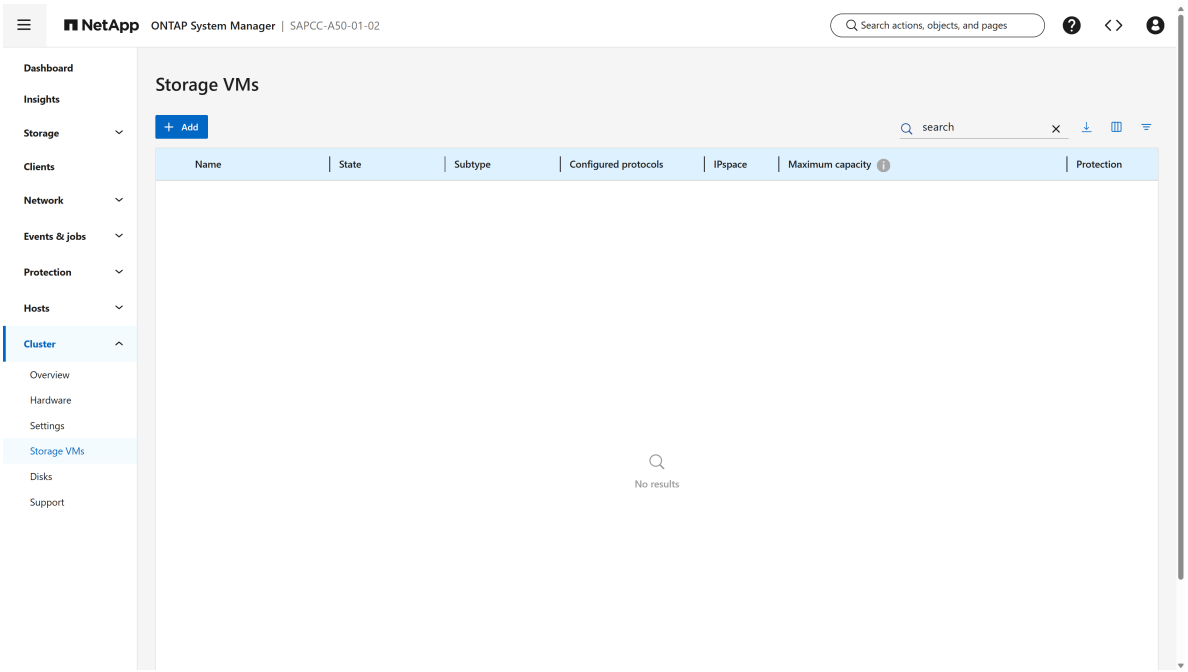
Schritte

1. Die SVM kann mit System Manager oder der CLI erstellt werden:

System Manager

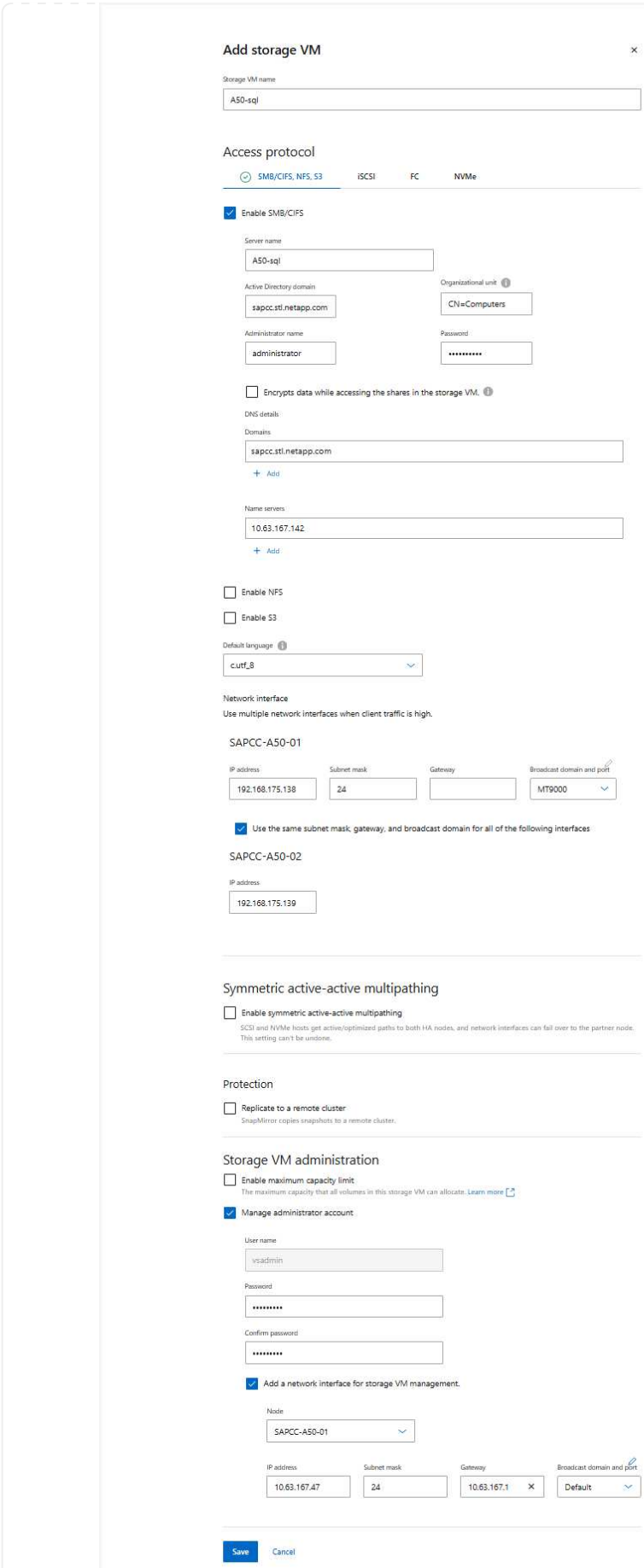
a. In System Manager erfolgt der Wechsel zu **Cluster › Storage VMs** und anschließend ein Klick auf **+ Add**.

▼ **Beispiel anzeigen**



b. **Storage VM-Name** `a50-sql` eingeben. Unter **Zugriffsprotokoll** die Registerkarte **SMB/CIFS, NFS, S3** auswählen und **SMB/CIFS aktivieren** auswählen.

▼ **Beispiel anzeigen**


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

Der Name der Storage VM ist der SMB-Name des CIFS-Servers.

c. Einzugeben sind die Active Directory-Informationen (Domäne, Administratorname und Kennwort sowie OU) und die DNS-Informationen (DNS-Domäne und Nameserver).

d. Unter **Netzwerkschnittstelle** erfolgt die Konfiguration einer Daten-LIF auf **jedem** Knoten.

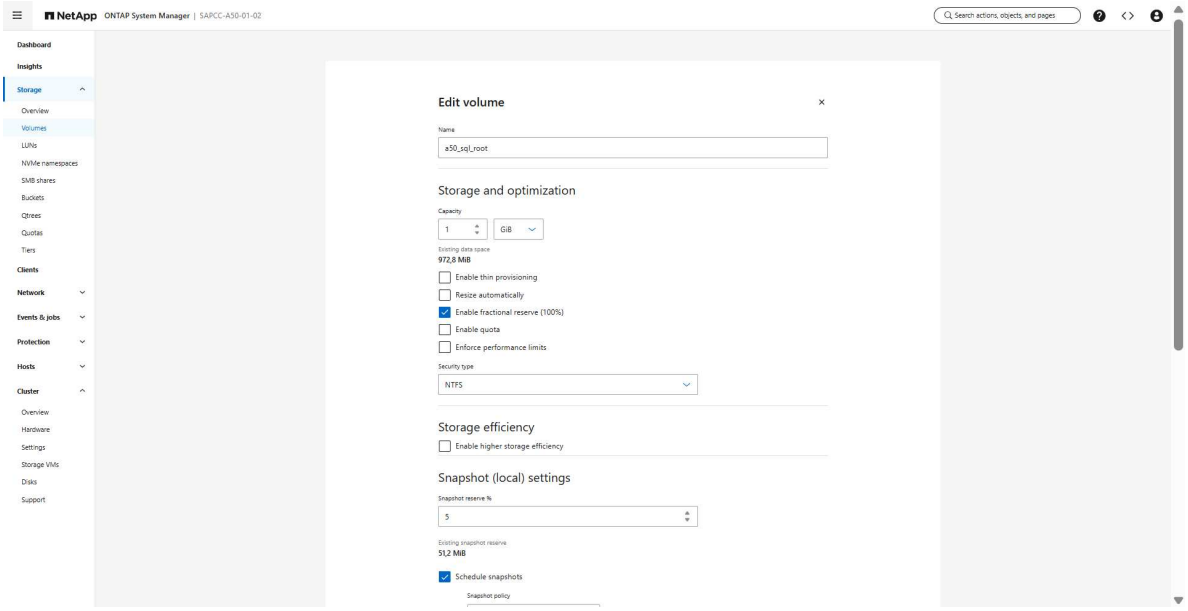
Ein LIF pro Knoten bietet SQL Server einen direkten (lokalen) Pfad zu jedem Knoten und ist eine Voraussetzung für SMB-Mehrkanalbetrieb und für unterbrechungsfreies Failover. 25-GbE- oder schnellere Ports sowie dieselbe MTU über die gesamte End-to-End-Verbindung werden empfohlen.

Sie müssen diese Netzwerkschnittstellen in Ihrem DNS-Server registrieren. Einzelheiten finden Sie unter "Zuordnung des SMB-Servers zum DNS-Server".

e. Der nächste Schritt ist die Auswahl von **Save**. System Manager erstellt die SVM, das Root-Volume, die LIFs und die DNS-Konfiguration und fügt den CIFS-Server der Domäne hinzu.

f. Überprüfung des SVM-Root-Volume (`a50_sql_root` im Labor). Es muss den **NTFS** -Sicherheitsstil verwenden, da SMB-Freigaben sonst nicht funktionieren. Zur Überprüfung der Einstellungen **Storage › Volumes** öffnen, das Root-Volume auswählen und auf **Edit** klicken.

▼ **Beispiel anzeigen**



ONTAP CLI

Die folgenden Befehle erstellen dieselbe Konfiguration über die CLI. Die Platzhalterwerte in spitzen Klammern sind zu ersetzen.

```
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. Konfiguration der SMB-Serveroptionen. Voraussetzung ist, dass die für SQL Server erforderlichen SMB-Optionen auf der SVM aktiviert sind:

```
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	Zweck
`smb3-enabled`	Für dauerhaft verfügbare Freigaben ist SMB 3.x erforderlich.
`is-multichannel-enabled`	SMB multichannel verwendet mehrere TCP-Verbindungen und Netzwerkpfade für höheren Durchsatz und höhere Ausfallsicherheit.
`is-large-mtu-enabled`	Ermöglicht SMB-Lese- und Schreibvorgänge von bis zu 1 MB.
`copy-offload-enabled`	ODX-Kopierauslagerung; Kopien erfolgen innerhalb des Storage-Systems.
`shadowcopy-enabled`	Remote VSS für SMB-Freigaben. Erforderlich für Sicherungsanwendungen, die VSS für SMB-Freigaben verwenden.

3. Zu überprüfen ist, ob der CIFS-Server im DNS registriert ist und vom SQL Server Host aus aufgelöst werden kann:

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

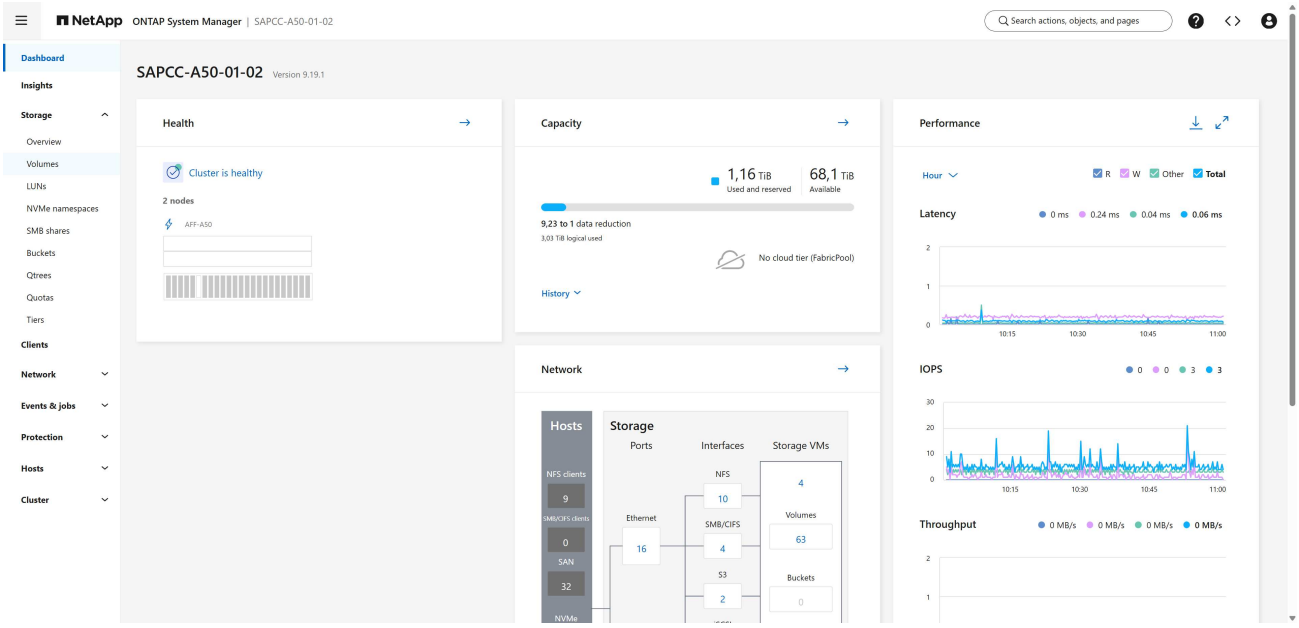
Schritt 3: Erstellen der SQL Server Volumes und SMB-Freigaben

Für jeden Dateityp werden jeweils ein Volume und eine SMB-Freigabe benötigt. System Manager erstellt die Freigabe zusammen mit dem Volume.

Schritte

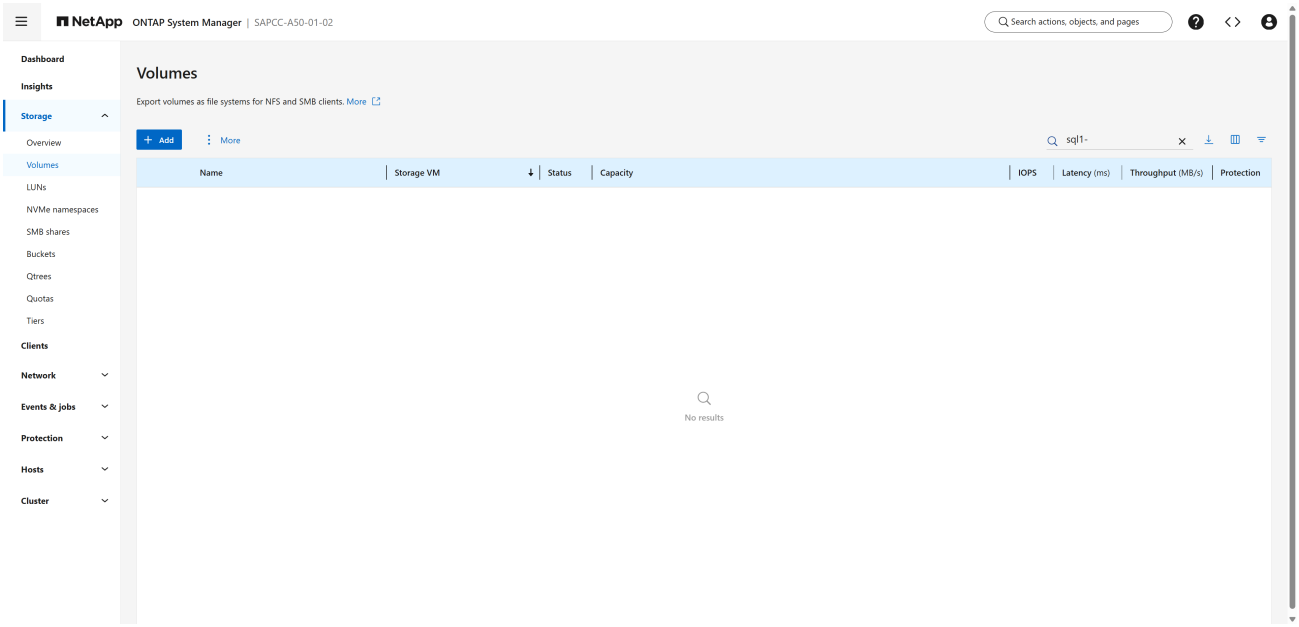
1. In System Manager **Storage** erweitern und anschließend auf **Volumes** klicken.

▼ **Beispiel anzeigen**



2. Die Volumenliste öffnet sich. Dann erfolgt ein Klick auf **+ Hinzufügen**.

▼ **Beispiel anzeigen**



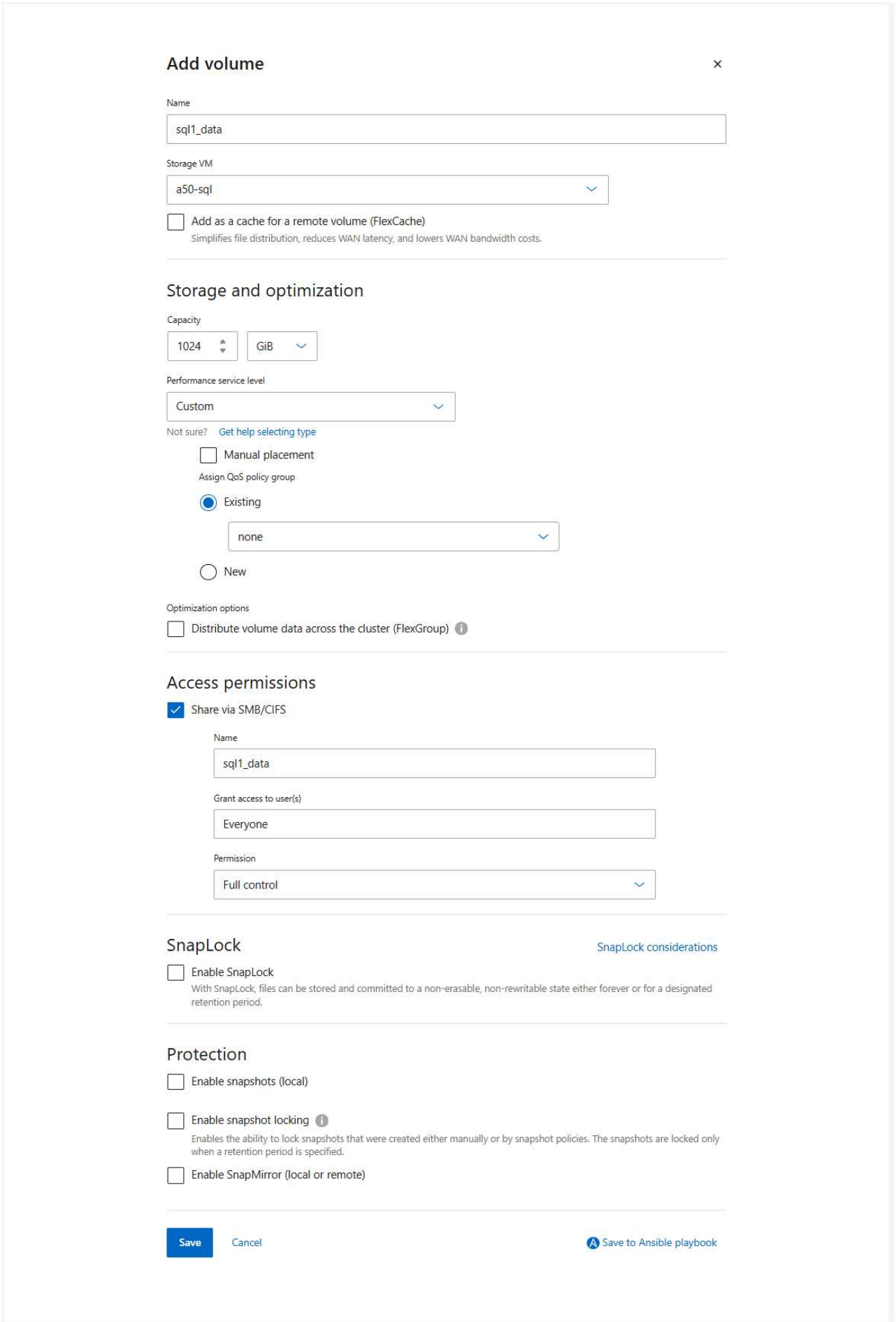
3. Erstellung des `sql1_data` Volume und der zugehörigen SMB-Freigabe für die Datendateien der Benutzerdatenbank.

a. Im Dialogfeld **Volume hinzufügen** sind die folgenden Werte einzugeben:

   - **Name**: `sql1_data`
   - **Storage-VM**: `a50-sql`
   - **Kapazität**: `1024 GiB`
   - **Performance Service Level**: **Benutzerdefiniert**, **QoS-Richtliniengruppe zuweisen**: **Vorhanden** > `none`
   - **Zugriffsberechtigungen**: **Freigabe über SMB/CIFS** auswählen. Freigabename `sql1_data`, Zugriff für Benutzer `Everyone`, Berechtigung **Vollzugriff**.
   - **Schutz**: **Snapshots aktivieren (lokal)** bleibt deaktiviert. Applikationskonsistente Backups werden von NetApp SnapCenter erstellt.

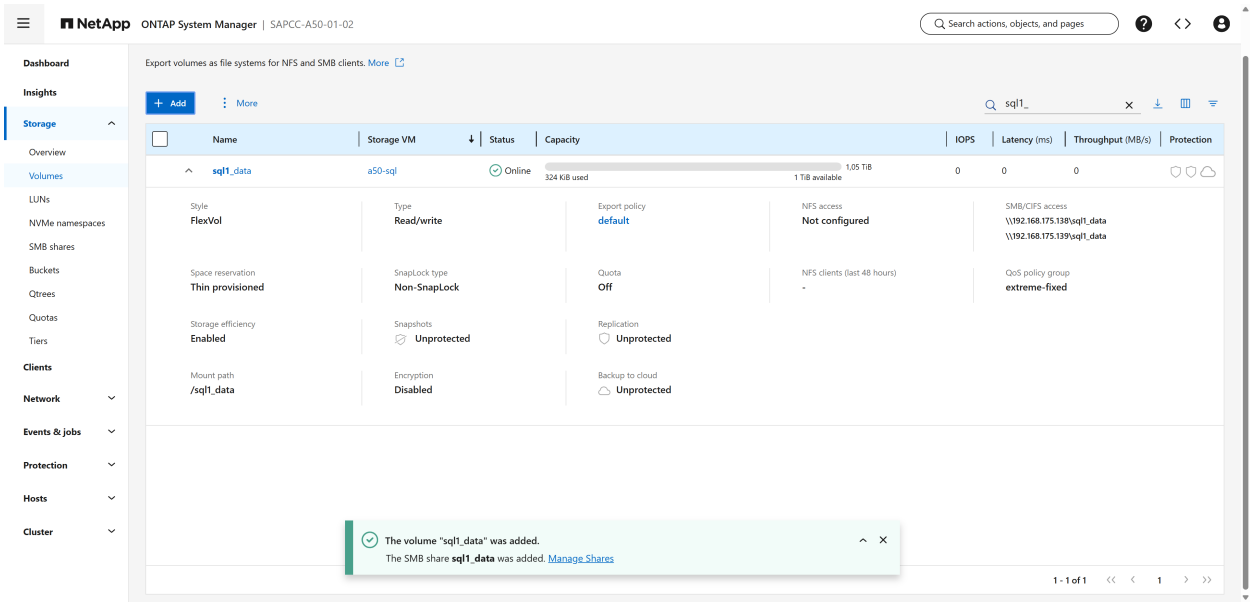
     Anschließend erfolgt die Auswahl von **Save**.

▼ Beispiel anzeigen


Add volume
Name
sql1_data
Storage VM
a50-sql
Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.
Storage and optimization
Capacity
1024
GiB
Performance service level
Custom
Not sure? Get help selecting type
Manual placement
Assign QoS policy group
Existing
none
New
Optimization options
Distribute volume data across the cluster (FlexGroup)
Access permissions
Share via SMB/CIFS
Name
sql1_data
Grant access to user(s)
Everyone
Permission
Full control
SnapLock
SnapLock considerations
Enable SnapLock
With SnapLock, files can be stored and committed to a non-erasable, non-rewritable state either forever or for a designated retention period.
Protection
Enable snapshots (local)
Enable snapshot locking
Enables the ability to lock snapshots that were created either manually or by snapshot policies. The snapshots are locked only when a retention period is specified.
Enable SnapMirror (local or remote)
Save
Cancel
Save to Ansible playbook

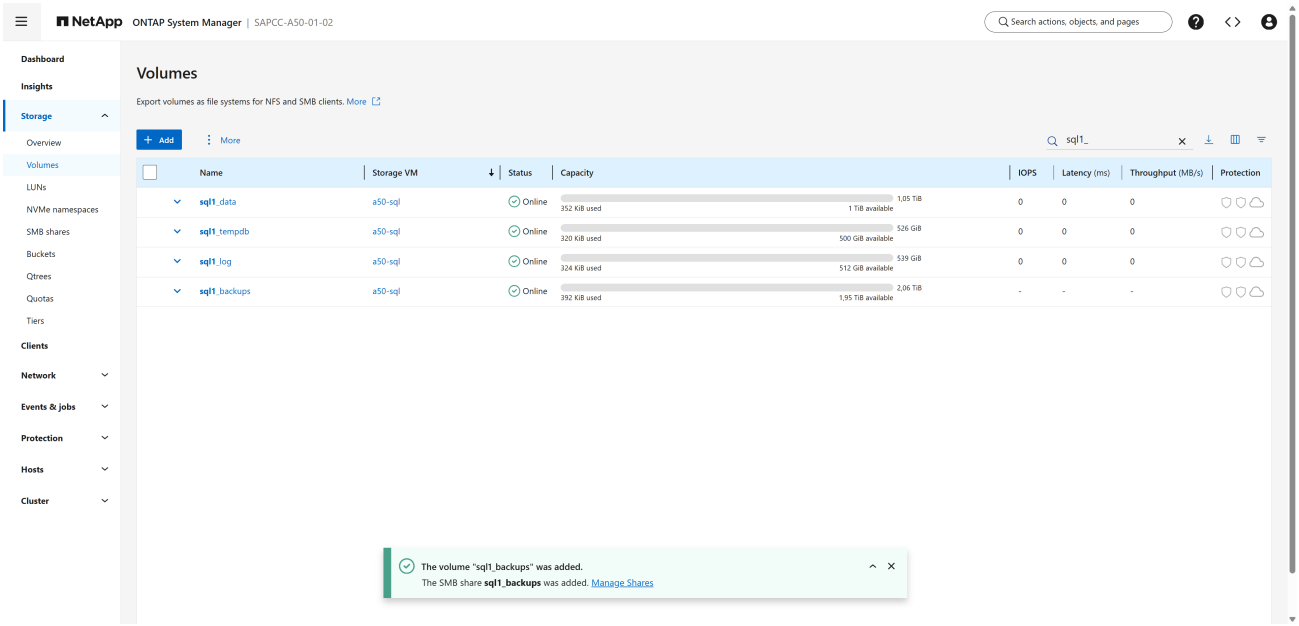
a. Das Volume wurde erstellt und wird als **Online** angezeigt. Nach dem Erweitern der Volume-Zeile werden die Details angezeigt: NTFS-Sicherheitsstil, SMB-Zugriffspfade über beide LIFs (`\\192.168.175.138\sql1_data` und `\\192.168.175.139\sql1_data`), sowie die QoS-Richtliniengruppe.

▼ **Beispiel anzeigen**



4. Für die Log-, TempDB- und Backup-Volumes gelten dieselben Schritte mit den in Laborumgebung aufgeführten Größen und Namen.

▼ **Beispiel anzeigen**



Im Labor wird aus Gründen der Einfachheit auf Freigabeebene **Everyone / Full control** gewährt. In Produktionsumgebungen ist die Beschränkung der Freigabe-ACL auf das SQL Server-Dienstkonto, das SQL Server Agent-Konto und die DBA-Verwaltungsgruppe erforderlich, zum Beispiel:

```
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. Die Befehle sind für `sql1_log`, `sql1_tempdb` und `sql1_backups` zu wiederholen. Das Dienstkonto benötigt außerdem **Vollzugriff** auf die NTFS-Berechtigungen des Stammverzeichnisses der Freigabe. SQL Server Setup überprüft dies, wie in Schritt 7 gezeigt.

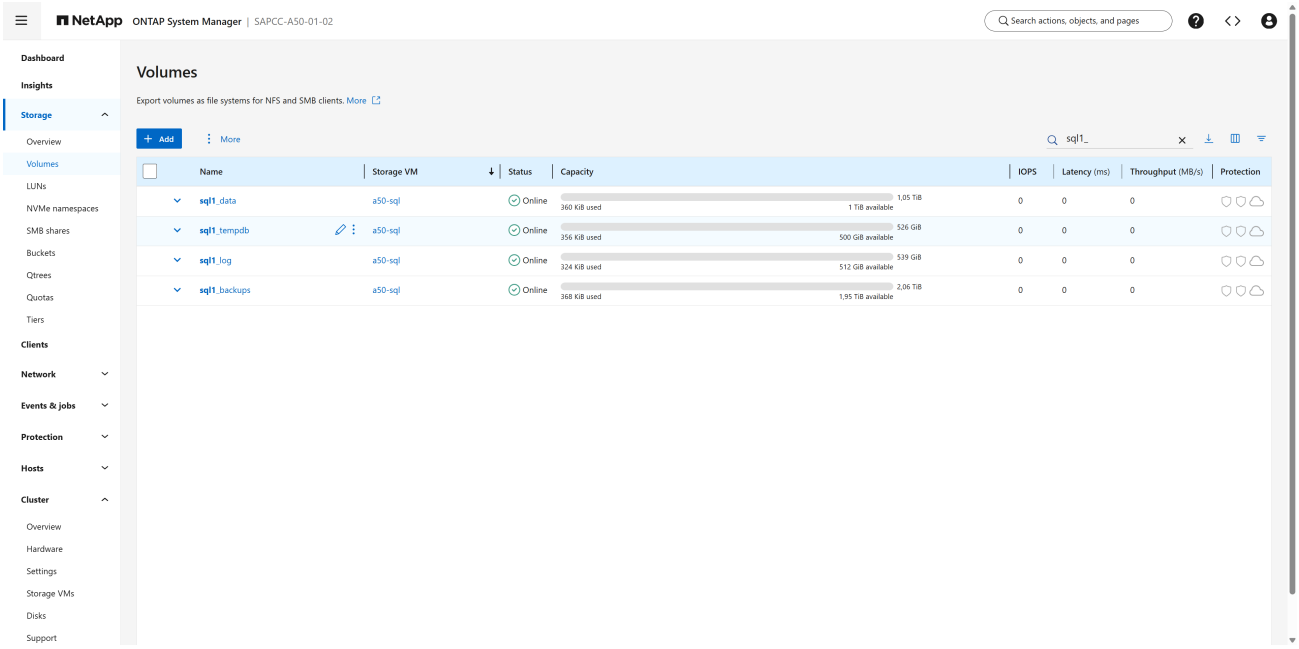
Schritt 4: Anpassen der Volume-Einstellungen

Überprüfung und Anpassung der Speicherplatz- und Snapshot-Einstellungen jedes SQL Server Volumes.

Schritte

1. In der Volume-Liste den Mauszeiger auf das Volume bewegen und auf das Stiftsymbol (**Bearbeiten**) klicken.

▼ **Beispiel anzeigen**



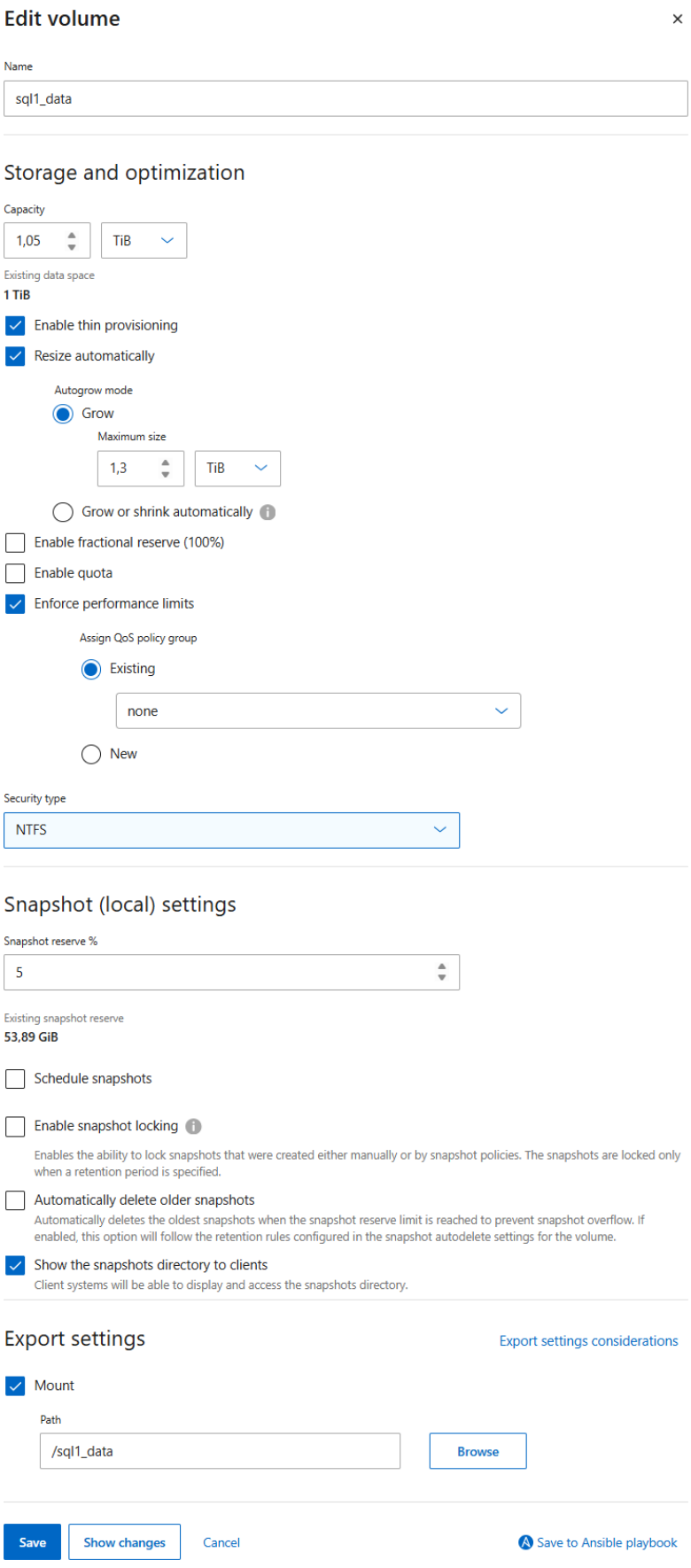
2. Die Konfiguration des Volumens erfolgt wie folgt (dargestellt für `sql1_data`):

   - **Thin Provisionierung aktivieren**: ausgewählt
   - **Automatische Größenanpassung**: ausgewählt, **Autogrow-Modus**: **Wachsen**, **Maximale Größe**: zum Beispiel `1.3 TiB` (ca. 125–130 % der Volumengröße)
   - **Teilreserve aktivieren (100%)**: deaktiviert
   - **Sicherheitstyp**: `NTFS`

- **Snapshot-Reserve %**: `5` (`0` für `sql1_tempdb`)
- **Snapshots planen**: deaktiviert. Snapshots, die nicht applikationskonsistent sind, sind für SQL Server nutzlos; stattdessen kommt NetApp SnapCenter zum Einsatz.
- **Snapshot-Verzeichnis für Clients anzeigen**: optional (im Labor war diese Option ausgewählt; durch Deaktivieren wird `~snapshot` in der Freigabe ausgeblendet)

  Nach einem Klick auf **Speichern** ist der Vorgang für `sql1_log`, `sql1_tempdb` und `sql1_backups` zu wiederholen.

▼ **Beispiel anzeigen**


Edit volume
Name
sql1_data
Storage and optimization
Capacity
1,05
TiB
Existing data space
1 TiB
Enable thin provisioning
Resize automatically
Autogrow mode
Grow
Maximum size
1,3
TiB
Grow or shrink automatically
Enable fractional reserve (100%)
Enable quota
Enforce performance limits
Assign QoS policy group
Existing
none
New
Security type
NTFS
Snapshot (local) settings
Snapshot reserve %
5
Existing snapshot reserve
53,89 GiB
Schedule snapshots
Enable snapshot locking
Enables the ability to lock snapshots that were created either manually or by snapshot policies. The snapshots are locked only when a retention period is specified.
Automatically delete older snapshots
Automatically deletes the oldest snapshots when the snapshot reserve limit is reached to prevent snapshot overflow. If enabled, this option will follow the retention rules configured in the snapshot autodelete settings for the volume.
Show the snapshots directory to clients
Client systems will be able to display and access the snapshots directory.
Export settings
Export settings considerations
Mount
Path
/sql1_data
Browse
Save
Show changes
Cancel
Save to Ansible playbook

```
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
```



Auf AFF sollte die Storage-Effizienz (Deduplizierung, Komprimierung, Verdichtung) aktiviert bleiben. Sie erfolgt inline und hat keine messbaren Auswirkungen auf die Performance von SQL Server.

Schritt 5: Kontinuierliche Verfügbarkeit für die SMB-Freigaben aktivieren

Die kontinuierliche Verfügbarkeit ist die wichtigste Einstellung für SQL Server auf SMB. Ohne sie verliert SQL Server während einer ONTAP Übernahme oder LIF-Migration seine offenen Dateihandles, und die Datenbanken wechseln in den Status „suspect“.

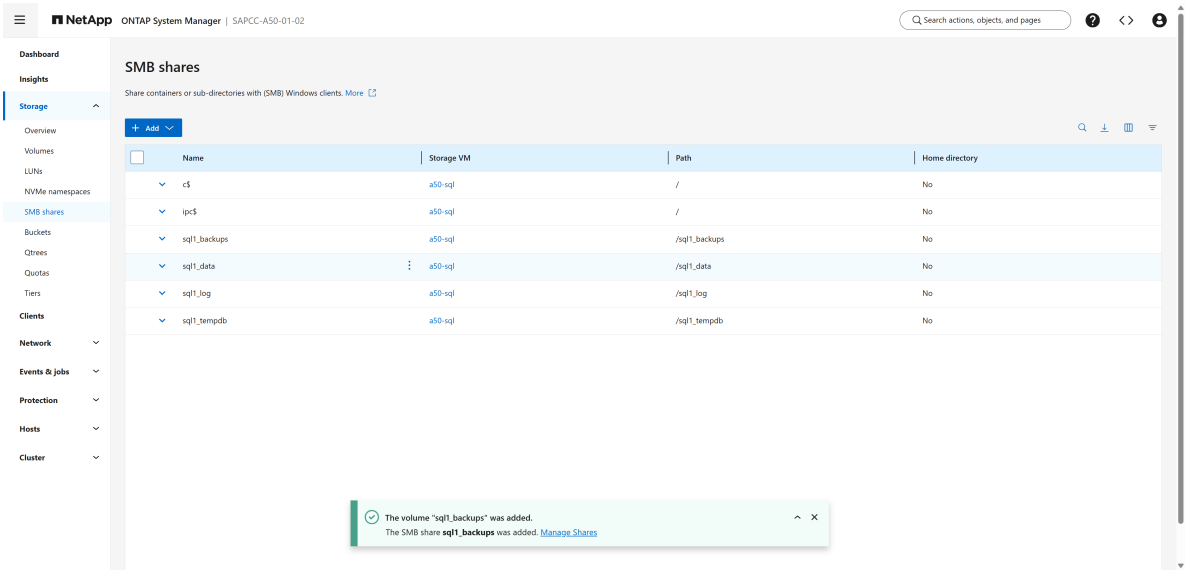
Schritte

1. Die Aktivierung der kontinuierlichen Verfügbarkeit auf den SMB-Freigaben erfolgt mit System Manager oder der CLI:

System Manager

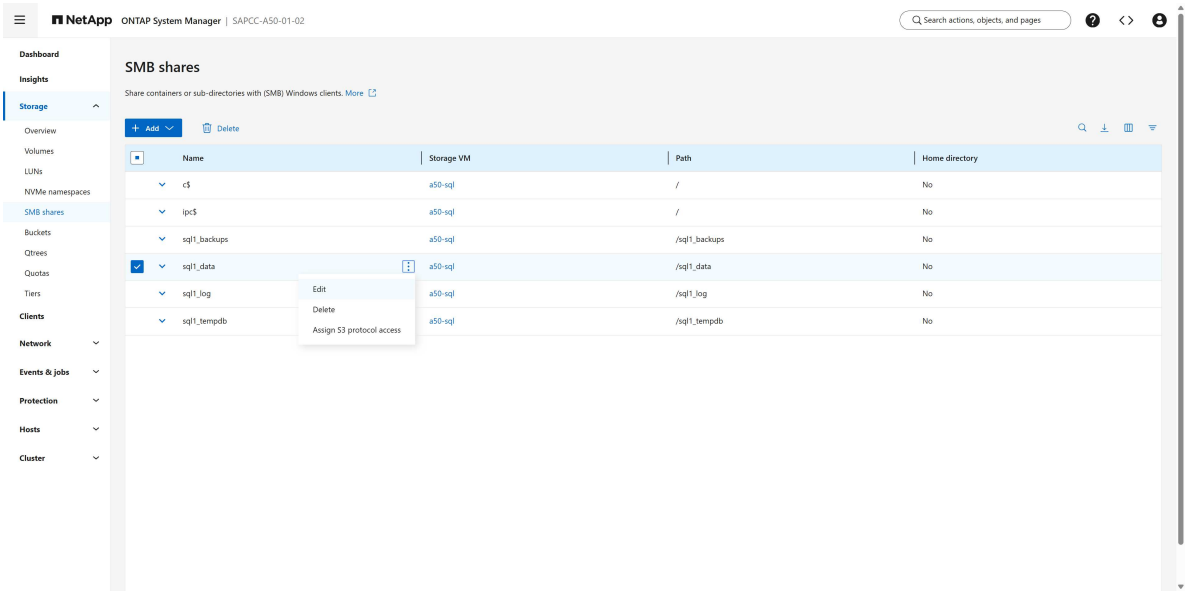
a. Der Zugriff erfolgt über Menü:Storage[SMB-Freigaben]. Die Liste zeigt die vier neuen Freigaben sowie die standardmäßigen administrativen Freigaben `c$` und `ipc$`.

▼ **Beispiel anzeigen**



b. Neben der Freigabe `sql1_data` erfolgt die Auswahl des Symbols „Mehr“ (⋮) und anschließend von **Bearbeiten**.

▼ **Beispiel anzeigen**



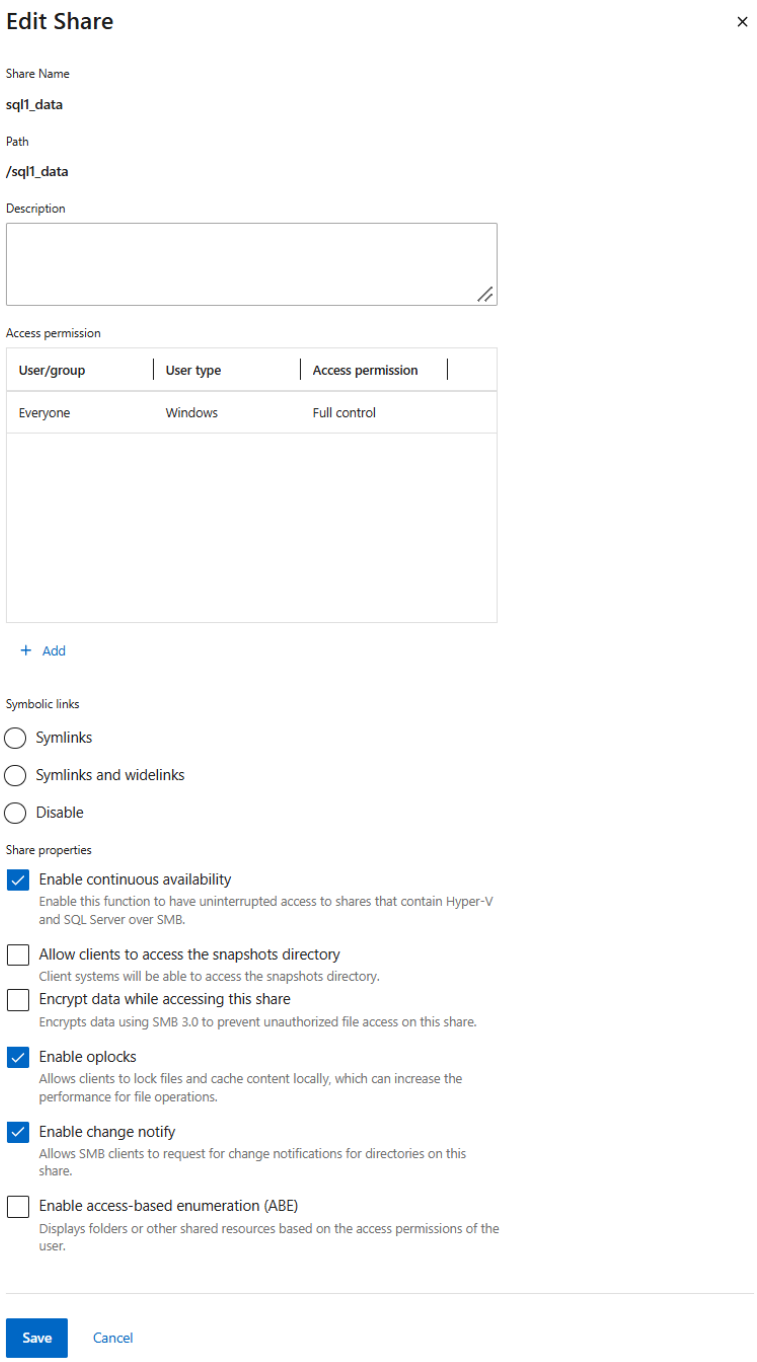
c. Unter **Freigabeeigenschaften** sind die folgenden Einstellungen vorzunehmen:

- **Kontinuierliche Verfügbarkeit aktivieren**: **ausgewählt**
- **Clients Zugriff auf das Snapshot-Verzeichnis erlauben**: deaktiviert
- **Daten beim Zugriff auf diese Freigabe verschlüsseln**: deaktiviert (optional, abhängig von Ihren Sicherheitsanforderungen)
- **Oplocks aktivieren**: ausgewählt

- **Änderungsbenachrichtigung aktivieren**: ausgewählt
- **Zugriffsbasierte Enumeration (ABE) aktivieren**: deaktiviert

Anschließend erfolgt die Auswahl von **Save**.

▼ **Beispiel anzeigen**



d. Dieselben Schritte gelten für `sql1_log`, `sql1_tempdb` und `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
```

Schritt 6: Windows Server 2025 vorbereiten

Die folgenden Schritte erfolgen auf dem SQL Server Host `sql-1` als Domänenadministrator.

Schritte

1. Es ist zu überprüfen, ob der Server der Domäne beigetreten ist und ob der CIFS-Server aufgelöst werden kann (siehe Konfigurieren der SMB-Serveroptionen).
2. Voraussetzung ist, dass das SQL Server-Dienstkonto in Active Directory vorhanden ist, z. B. `SAPCC\sql1admin`. Dabei wird entweder dasselbe Konto für die Datenbank-Engine und für SQL Server Agent verwendet, oder es wird für jede Komponente ein separates Konto verwendet. Unabhängig von der gewählten Option benötigt jedes Konto Zugriff auf alle vier Freigaben.
3. Test des Zugriffs auf die Freigaben im Sicherheitskontext des Dienstkontos:

```
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. Öffnen des SQL Server Ports in der Windows-Firewall:

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

5. Überprüfung der SMB-Verbindung zur SVM. Der Dialekt muss 3.x sein und `ContinuouslyAvailable` muss `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
```

Windows Server 2025 erfordert standardmäßig die SMB-Signierung für alle ausgehenden SMB-Verbindungen. ONTAP unterstützt die SMB-Signierung und handelt sie automatisch aus. Die Signierung erhöht die CPU-Last auf beiden Seiten; dieser Aspekt sollte in den Performance-Tests berücksichtigt werden. Eine Deaktivierung der Signierung ohne vorherige Sicherheitsprüfung wird nicht empfohlen.

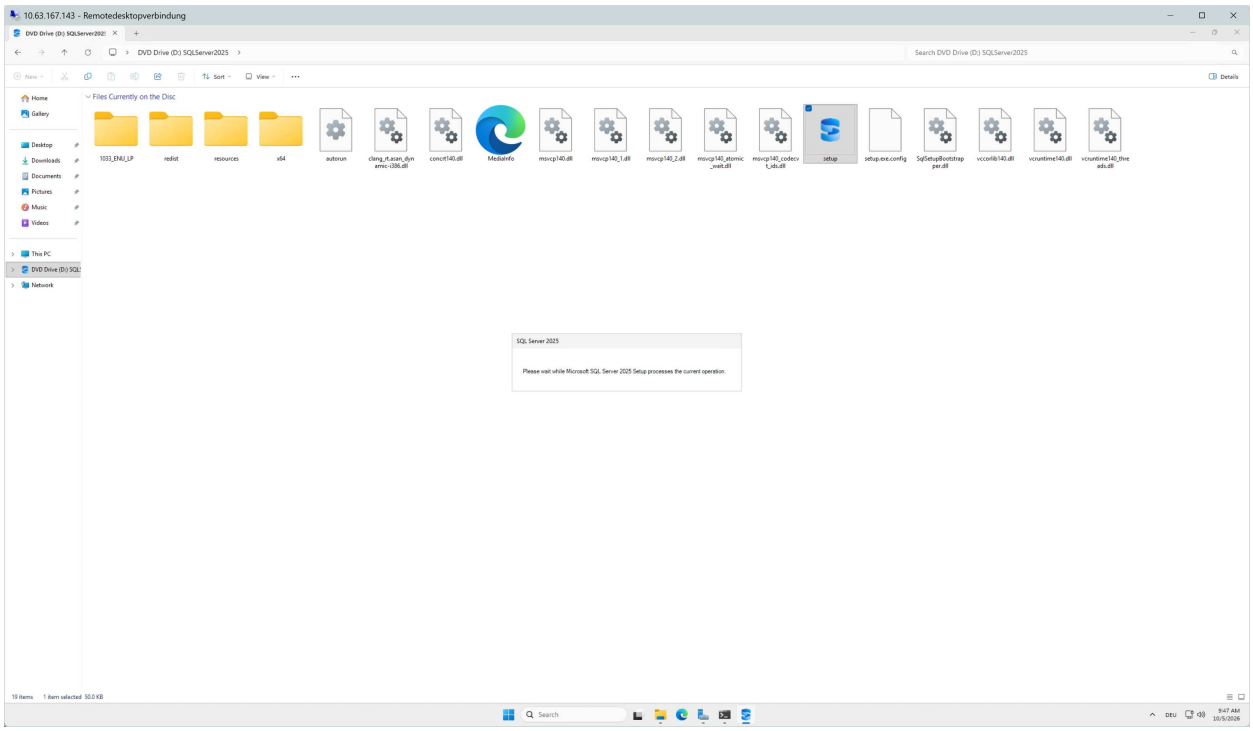
Schritt 7: Installation von SQL Server 2025

SQL Server 2025 wird mithilfe des Setup-Assistenten auf dem Windows Server Host installiert. Die Binärdateien und Systemdatenbanken werden auf dem lokalen Datenträger installiert, und für Benutzerdatenbank, Transaktionsprotokoll, TempDB und Sicherungsspeicherorte werden die erstellten SMB-Freigaben angegeben.

Schritte

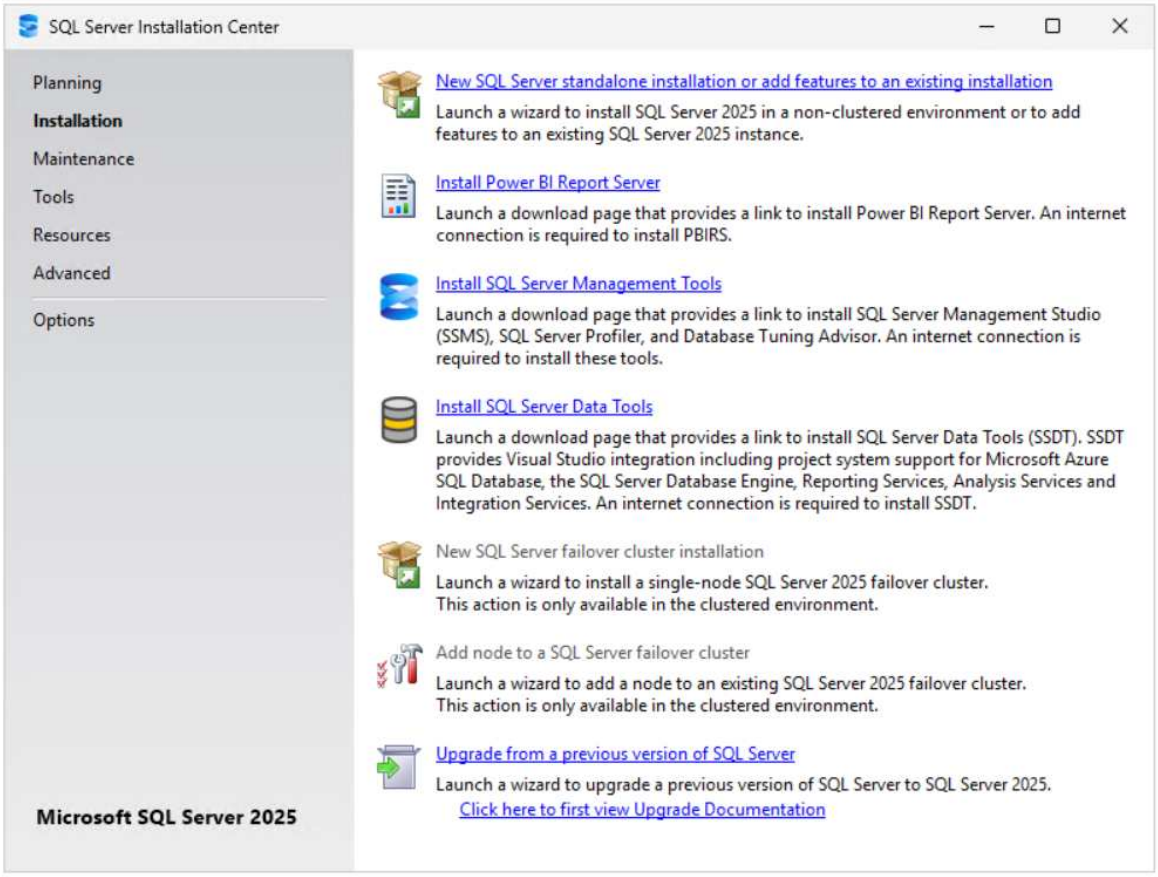
1. Der Start der eigenständigen Installation erfolgt über das SQL Server Installation Center.
   a. Das ISO-Image von SQL Server 2025 einbinden. Im Datei-Explorer das DVD-Laufwerk (`D:` im Labor) öffnen und auf **setup** doppelklicken.

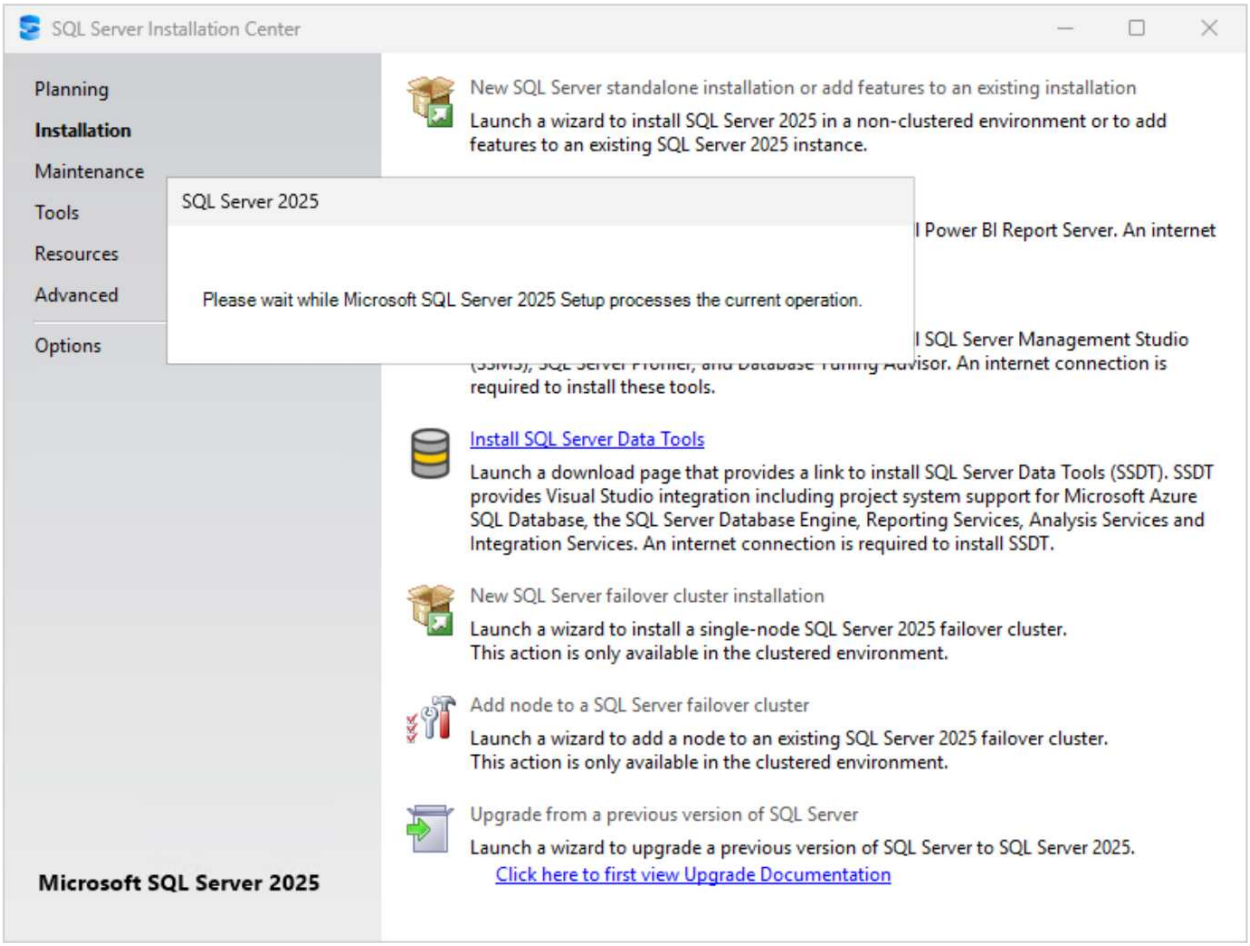
      ▼ **Beispiel anzeigen**

   b. Das **SQL Server Installation Center** wird geöffnet. Im linken Bereich wird **Installation** ausgewählt und anschließend auf **New SQL Server standalone installation or add features to an existing installation** geklickt.

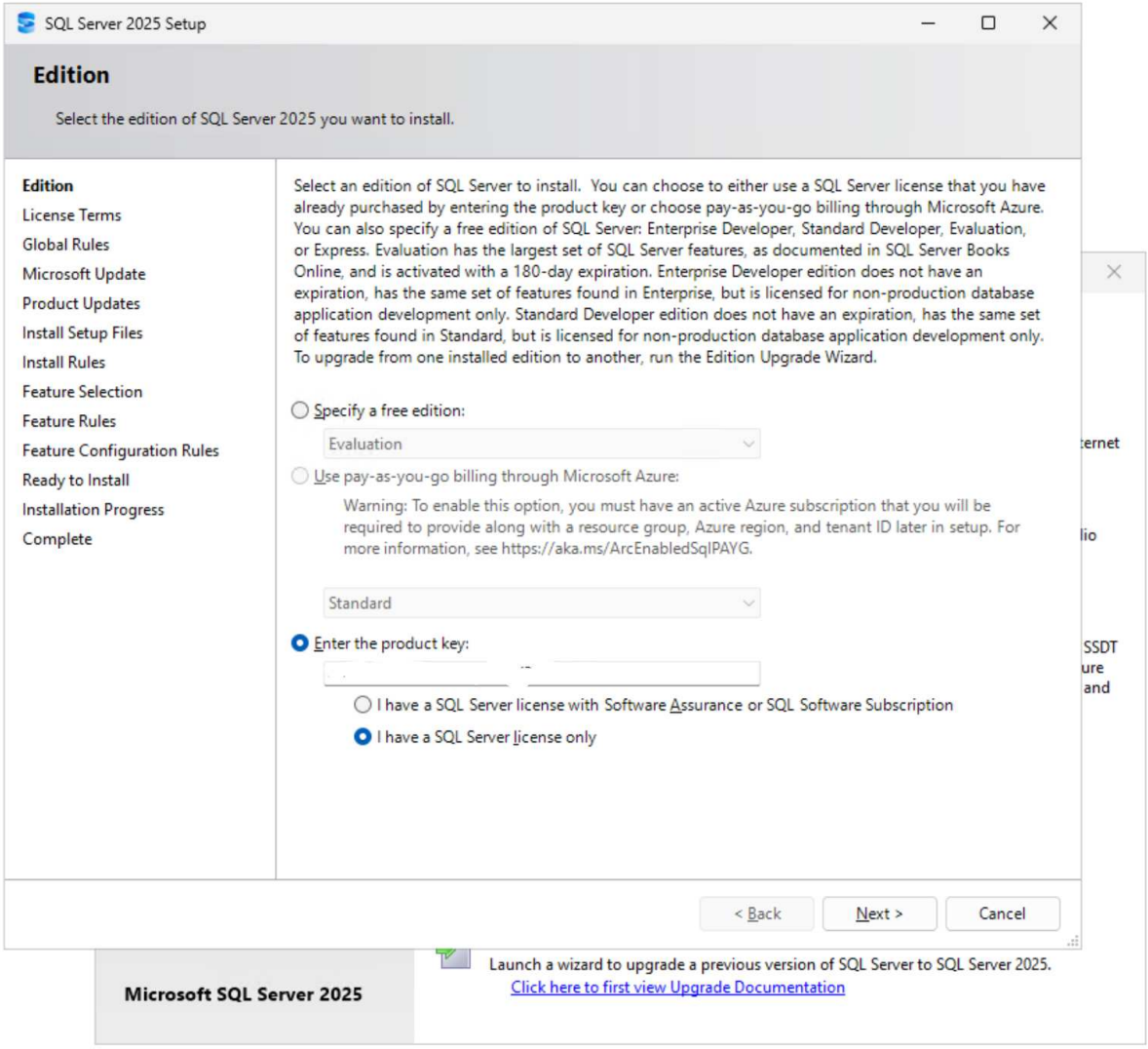
      ▼ **Beispiel anzeigen**


SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
Microsoft SQL Server 2025
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



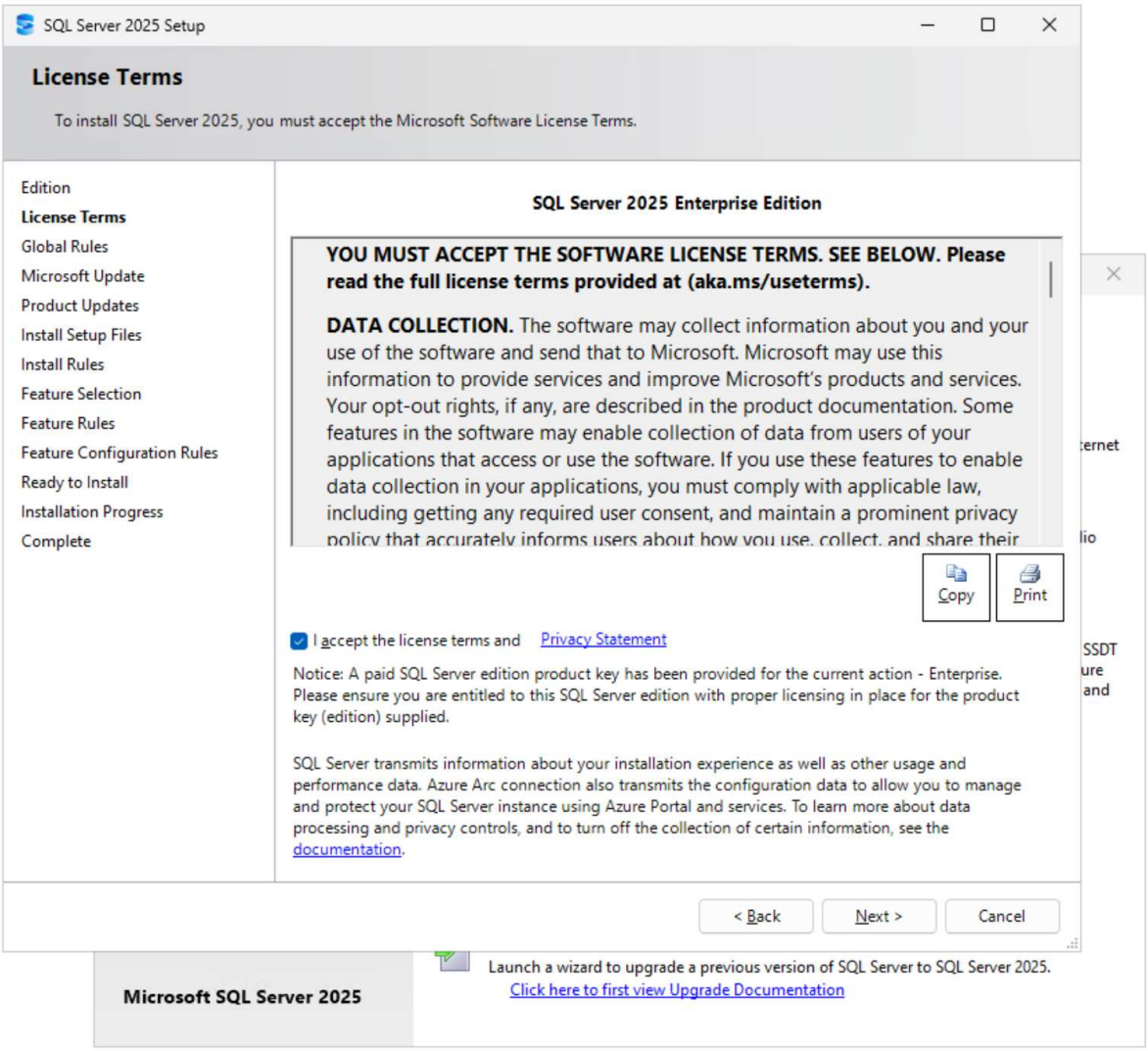
2. Die SQL Server Edition wird ausgewählt, die Lizenzbedingungen werden akzeptiert, und Setup sucht nach Produktaktualisierungen.
   a. Auf der Seite **Edition Enter the product key** auswählen und den Produktschlüssel eingeben oder eine kostenlose Edition (Evaluation, Enterprise Developer, Standard Developer oder Express) auswählen. Den zutreffenden Lizenztyp (**I have a SQL Server license only** im Lab) auswählen und auf **Next** klicken.

      ▼ Beispiel anzeigen



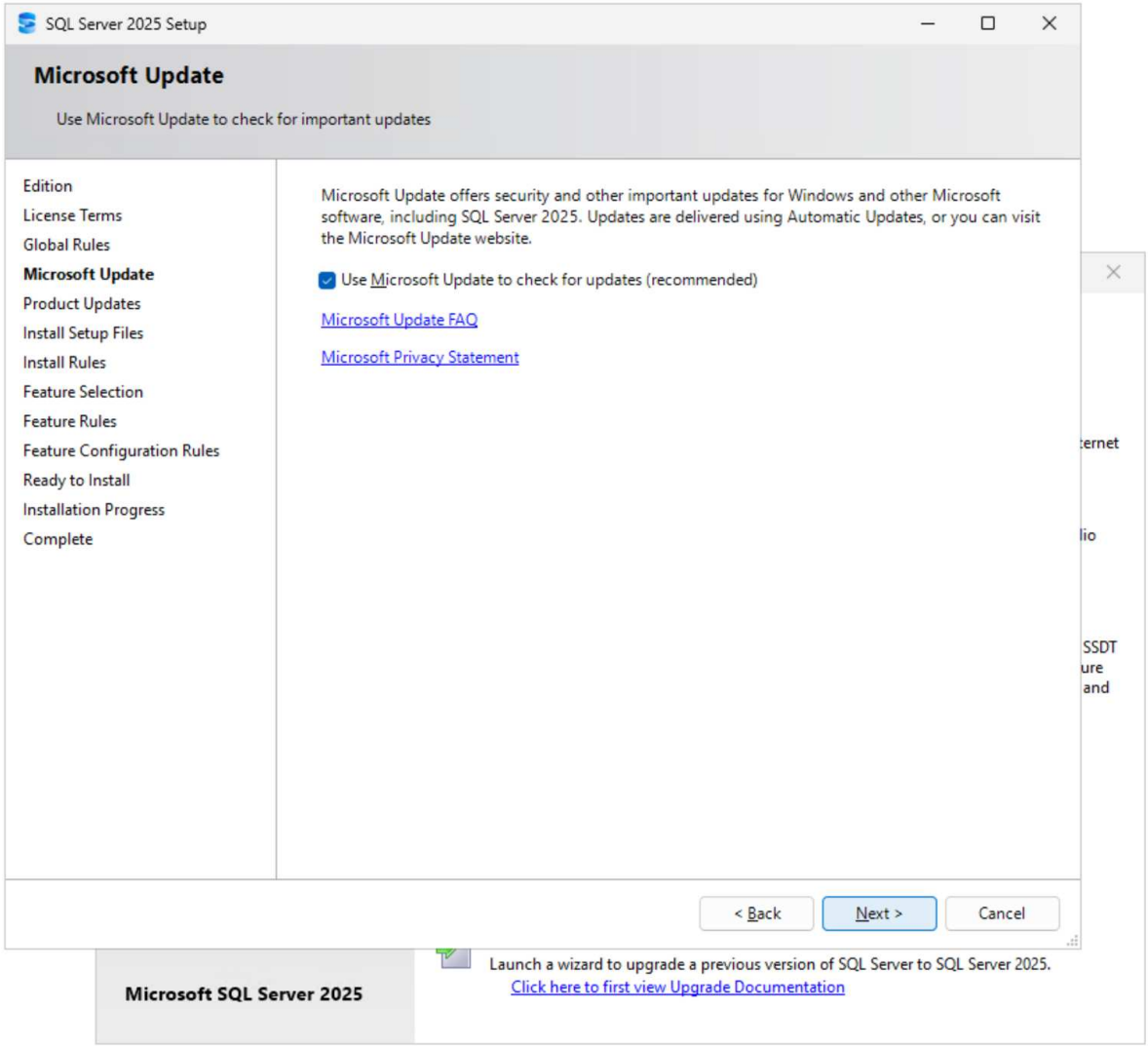
b. Auf der Seite **Lizenzbedingungen** nach dem Lesen der Bedingungen **Ich akzeptiere die Lizenzbedingungen und die Datenschutzerklärung** auswählen und auf **Weiter** klicken.

▼ Beispiel anzeigen



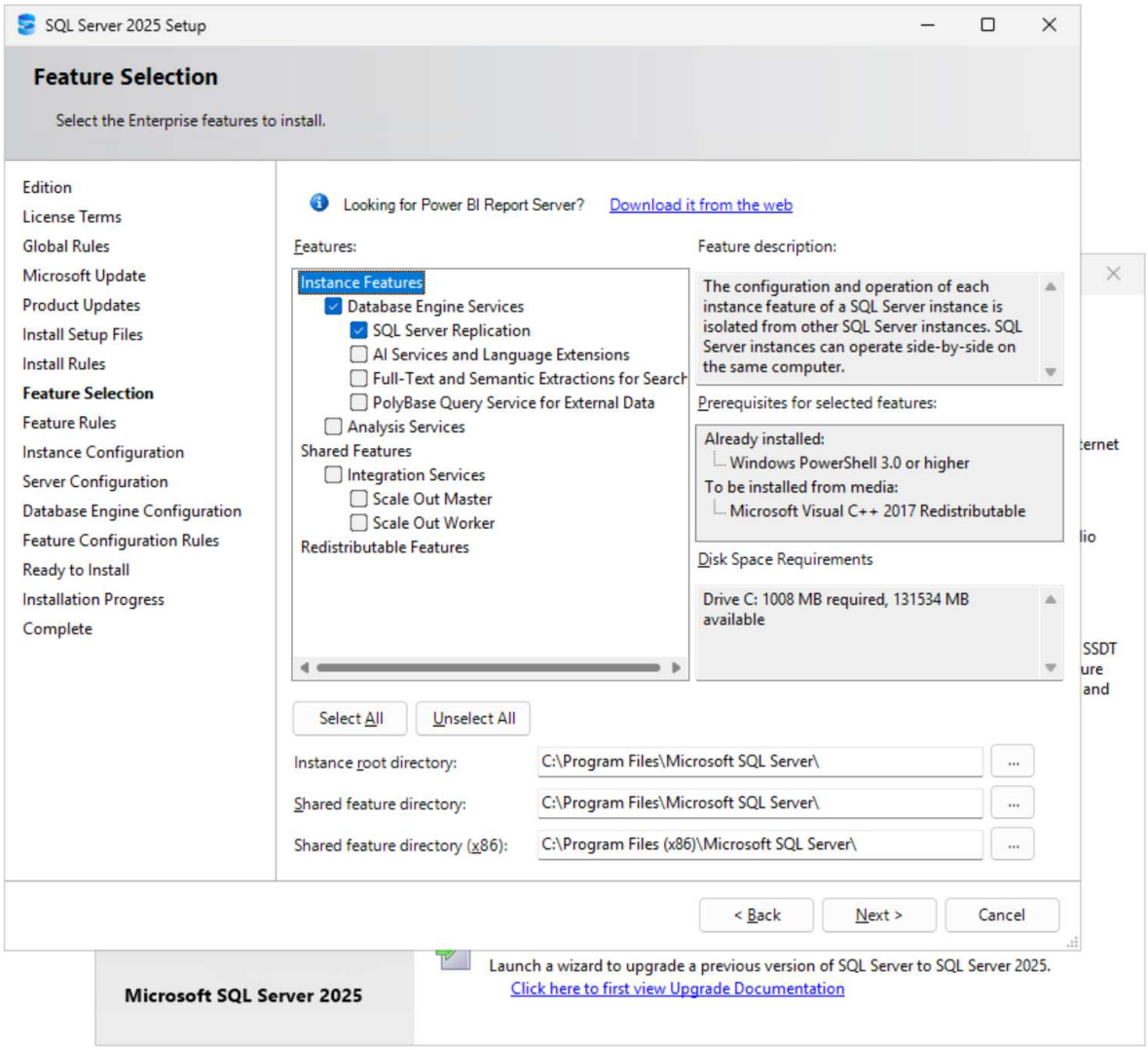
c. Auf der Seite **Microsoft Update** wird die Option **Microsoft Update zum Suchen nach Updates verwenden (empfohlen)** ausgewählt und anschließend auf **Weiter** geklickt. Setup führt dann die Prüfungen **Globale Regeln**, **Produktupdates**, **Setupdateien installieren** und **Installationsregeln** aus.

▼ Beispiel anzeigen



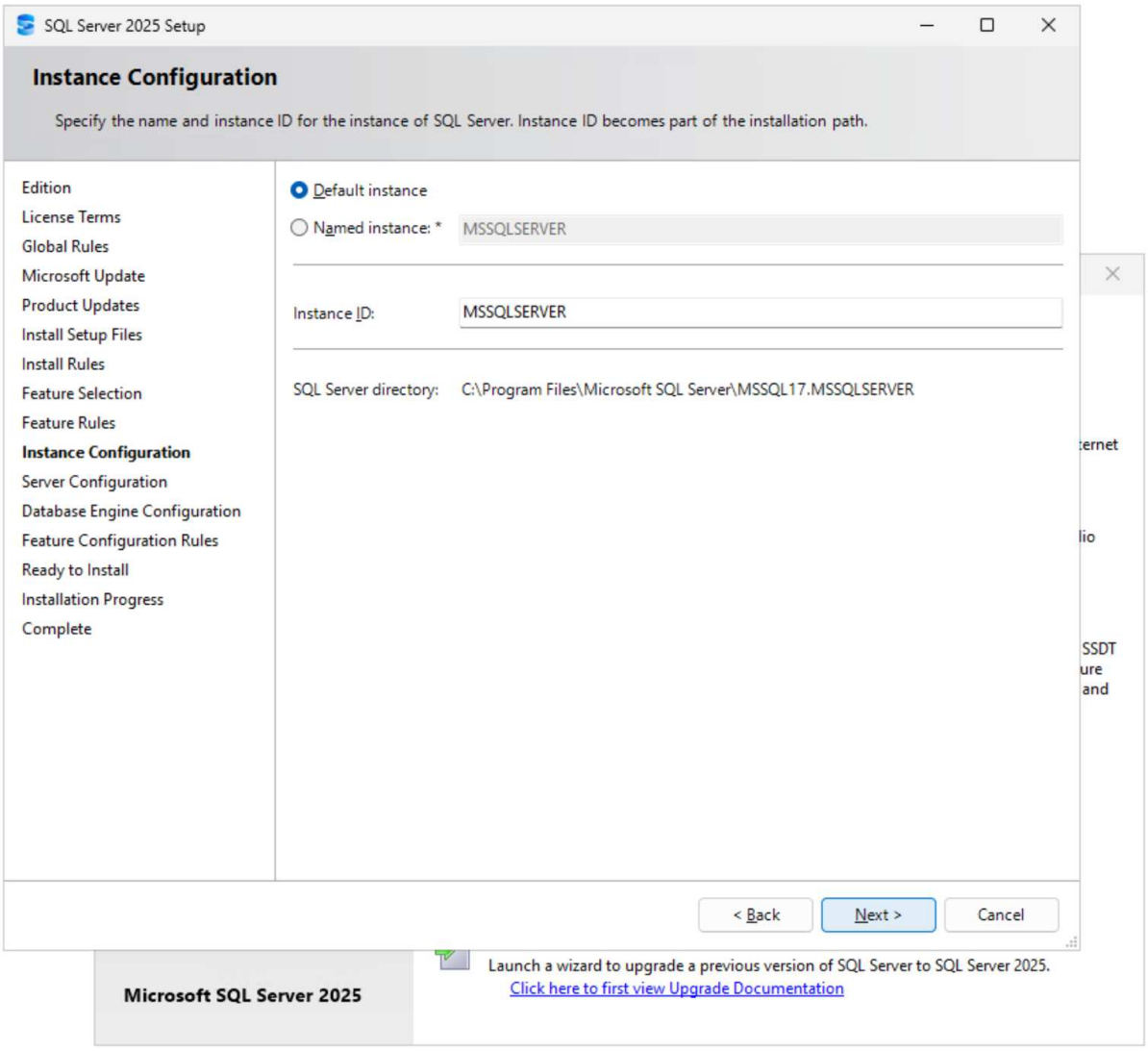
3. Auszuwählen sind die SQL Server-Funktionen und die zu installierende Instanz. Die Binärdateien verbleiben auf der lokalen Festplatte; nur die Datenbankdateien werden auf den SMB-Freigaben abgelegt.
   a. Auf der Seite **Feature Selection** sind **Database Engine Services** und alle zusätzlich benötigten Funktionen auszuwählen (im Lab war zusätzlich **SQL Server Replication** ausgewählt). **Instance root directory** und **Shared feature directory** verbleiben auf der lokalen Festplatte `C:`. Die Binärdateien werden lokal installiert; nur die Datenbankdateien befinden sich auf den SMB-Freigaben.

      ▼ Beispiel anzeigen



b. Auf der Seite **Instanzkonfiguration** erfolgt die Auswahl von **Standardinstanz** (`MSSQLSERVER`), oder es wird eine benannte Instanz eingegeben, und anschließend folgt ein Klick auf **Weiter**.

▼ Beispiel anzeigen



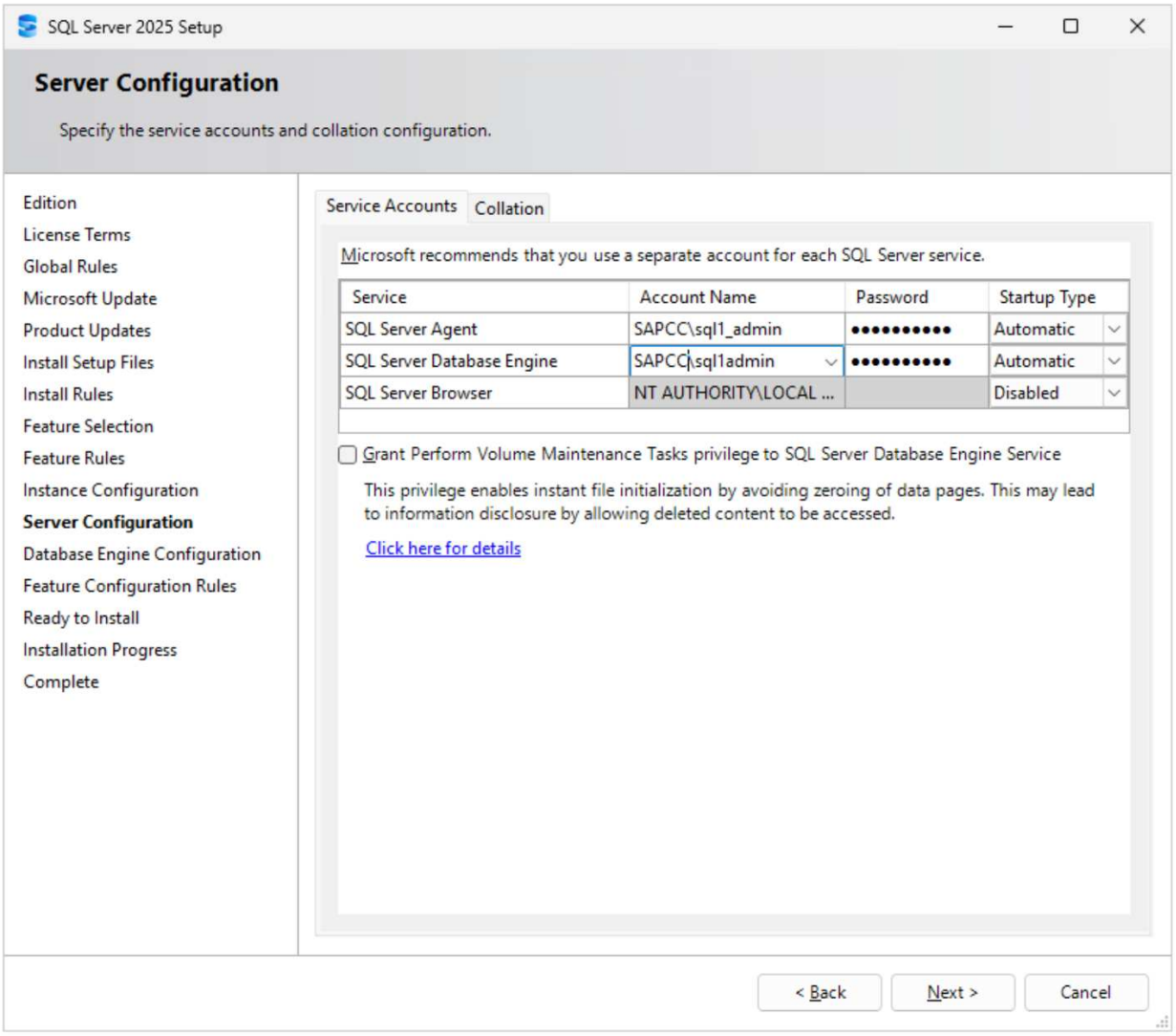
4. Die SQL Server Database Engine und die SQL Server Agent Services sollten für die Ausführung unter einem Domänenkonto konfiguriert werden, das Zugriff auf die SMB-Freigaben hat.

   a. Auf der Seite **Serverkonfiguration** auf der Registerkarte **Dienstkonten** werden das Domänenkonto und das Kennwort für **SQL Server Agent** und **SQL Server Database Engine** angegeben, und der **Starttyp** wird auf **Automatisch** festgelegt.

> Zu verwenden ist das Domänenkonto mit Vollzugriff auf die SMB-Freigaben. Der Screenshot zeigt zwei unterschiedliche Schreibweisen (`SAPCC\sql1_admin` und `SAPCC\sql1admin`). Jedes eingegebene Konto muss in Active Directory vorhanden sein und Zugriff auf alle vier Freigaben haben.

> Die Option „Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service“ wird ausgewählt. Dadurch wird die sofortige Dateiinitialisierung ermöglicht, was die Datenbankerstellung, das Dateiwachstum und Wiederherstellungen erheblich beschleunigt.

▼ Beispiel anzeigen

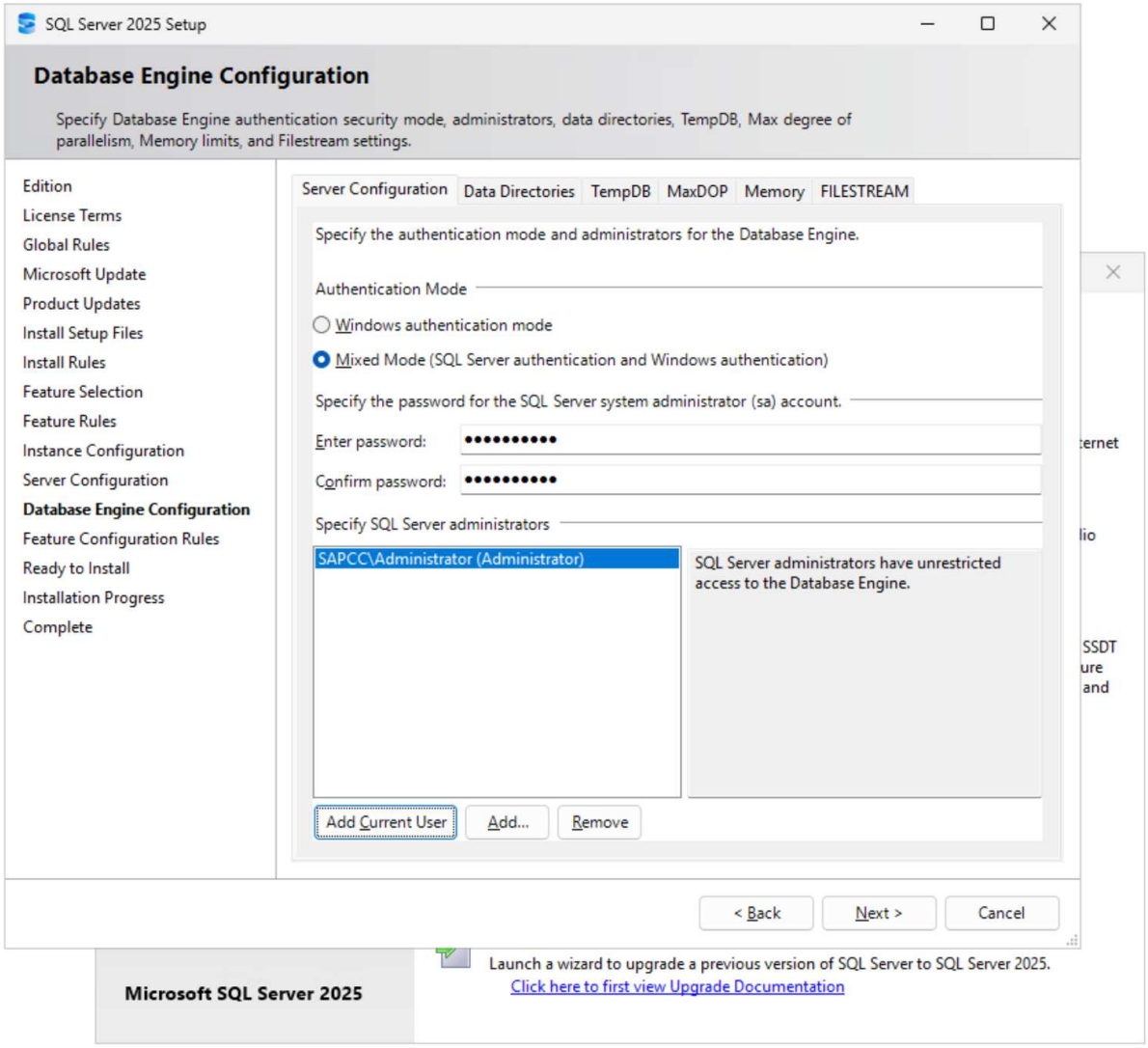


5. Der Authentifizierungsmodus und die SQL Server-Administratoren werden festgelegt, und die UNC-Pfade der SMB-Freigaben für die Benutzerdatenbank, das Transaktionsprotokoll sowie die Sicherungs- und TempDB-Dateien werden eingegeben.

   a. Auf der Seite **Database Engine Configuration**, Registerkarte **Server Configuration**, erfolgt die Auswahl des Authentifizierungsmodus. Im Lab wird **Mixed Mode** mit einem sicheren Passwort für das `sa` Konto verwendet. Mit **Add Current User** und **Add…** werden die SQL Server-Administratoren (Benutzer oder vorzugsweise eine Active Directory-Gruppe) hinzugefügt.

   Der **Windows Authentifizierungsmodus** sollte verwendet werden, sofern Anwendungen keine SQL Server-Anmeldungen erfordern.

   ▼ Beispiel anzeigen



b. Auf der Registerkarte **Datenverzeichnisse** erfolgt die Eingabe der UNC-Pfade der SMB-Freigaben:

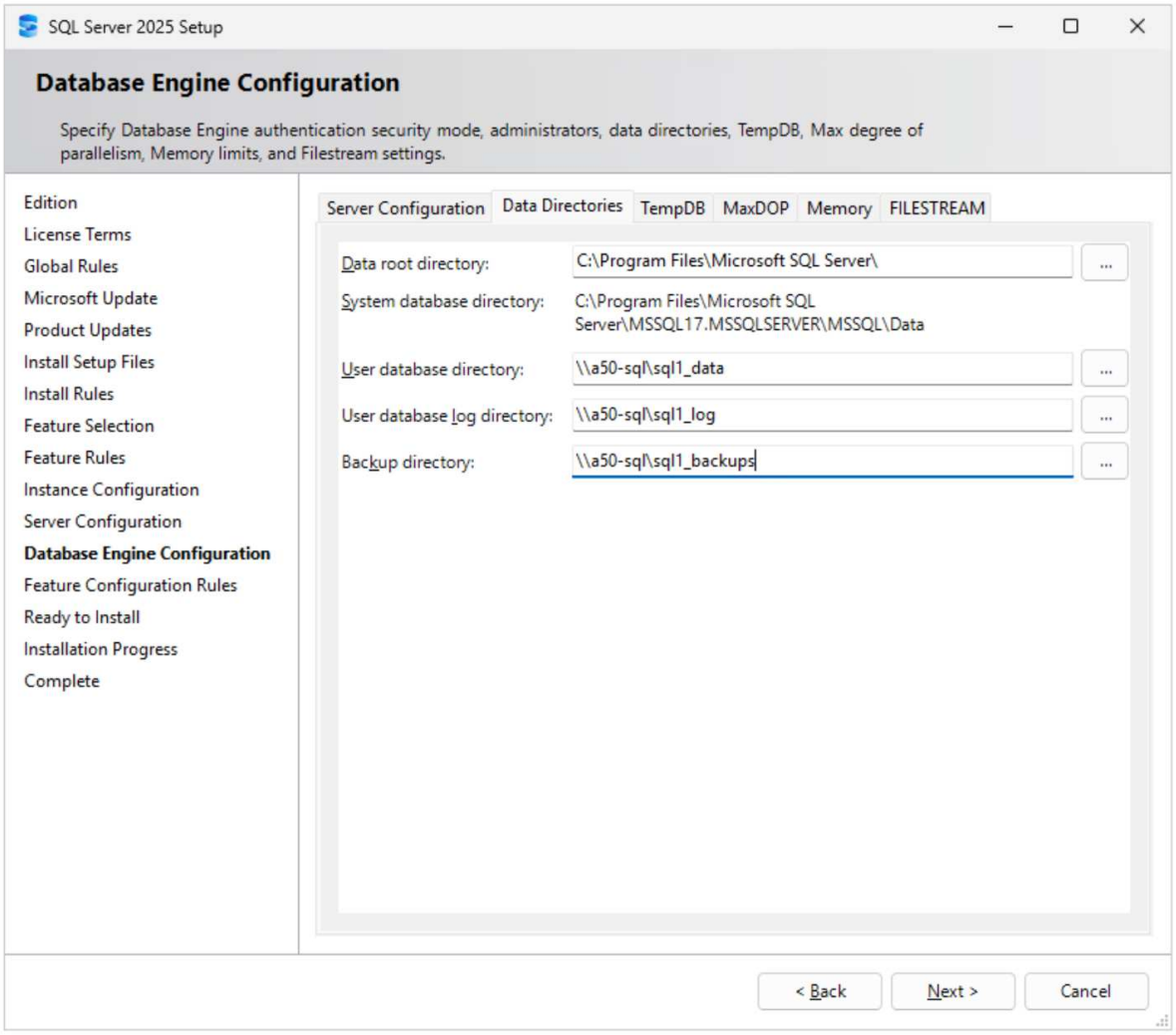
Einstellung	Wert
Daten-Root-Verzeichnis	`C:\Program Files\Microsoft SQL Server\` (lokal; Systemdatenbanken bleiben auf `C:`)
Benutzerdatenbankverzeichnis	`\\a50-sql\sql1_data`
Protokollverzeichnis der Benutzerdatenbank	`\\a50-sql\sql1_log`
Sicherungsverzeichnis	`\\a50-sql\sql1_backups`

Für die Platzierung der Systemdatenbanken (`master`, `model`, `msdb`) ebenfalls auf der SMB-Freigabe ist **Datenstammverzeichnis** auf einen UNC-Pfad festzulegen. Falls dies gewünscht ist, sollten für die Systemdatenbanken ein neues Volume und eine neue Freigabe erstellt werden.

Für die Verzeichnisse sind UNC-Pfade erforderlich, da zugeordnete Laufwerke nicht

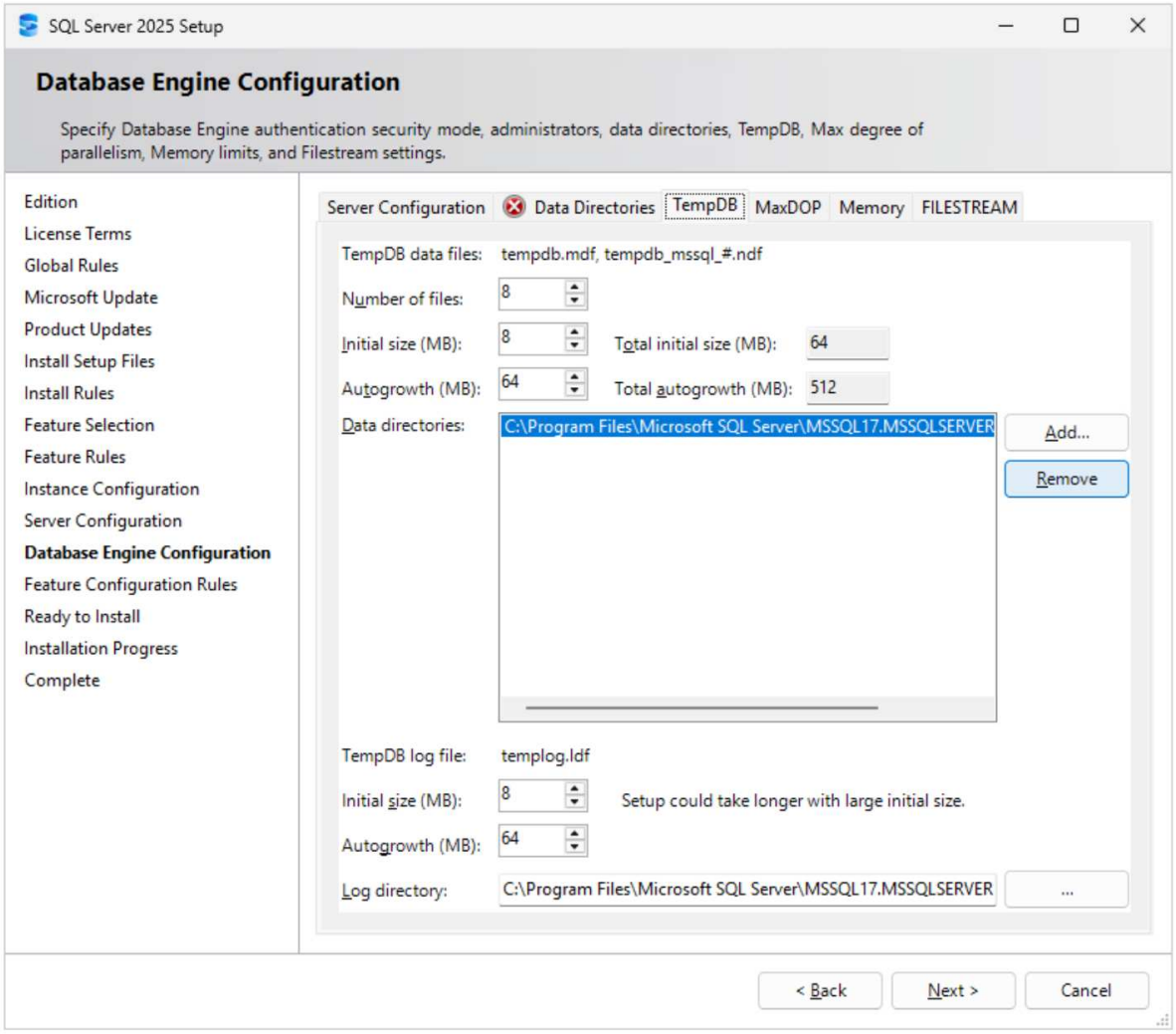
unterstützt werden.

▼ **Beispiel anzeigen**



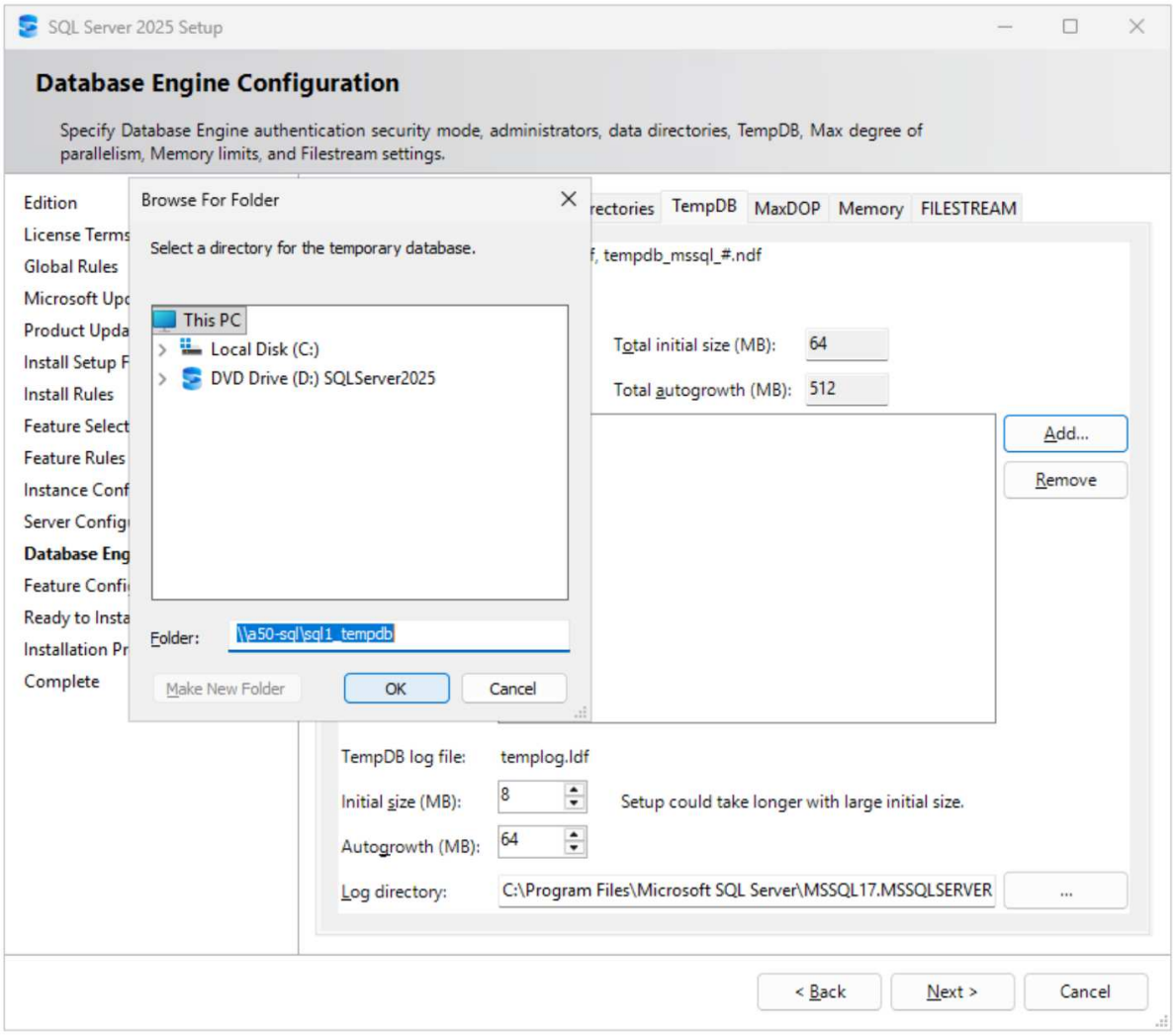
c. Auf der Registerkarte **TempDB** erfolgt die Auswahl des standardmäßigen lokalen Datenverzeichnisses, anschließend wird auf **Entfernen** geklickt.

▼ **Beispiel anzeigen**



d. **Add…** auswählen. Im Dialogfeld **Browse For Folder** den UNC-Pfad `\\a50-sql\sql1_tempdb\data` in das Feld **Folder** eingeben und **OK** auswählen.

▼ Beispiel anzeigen

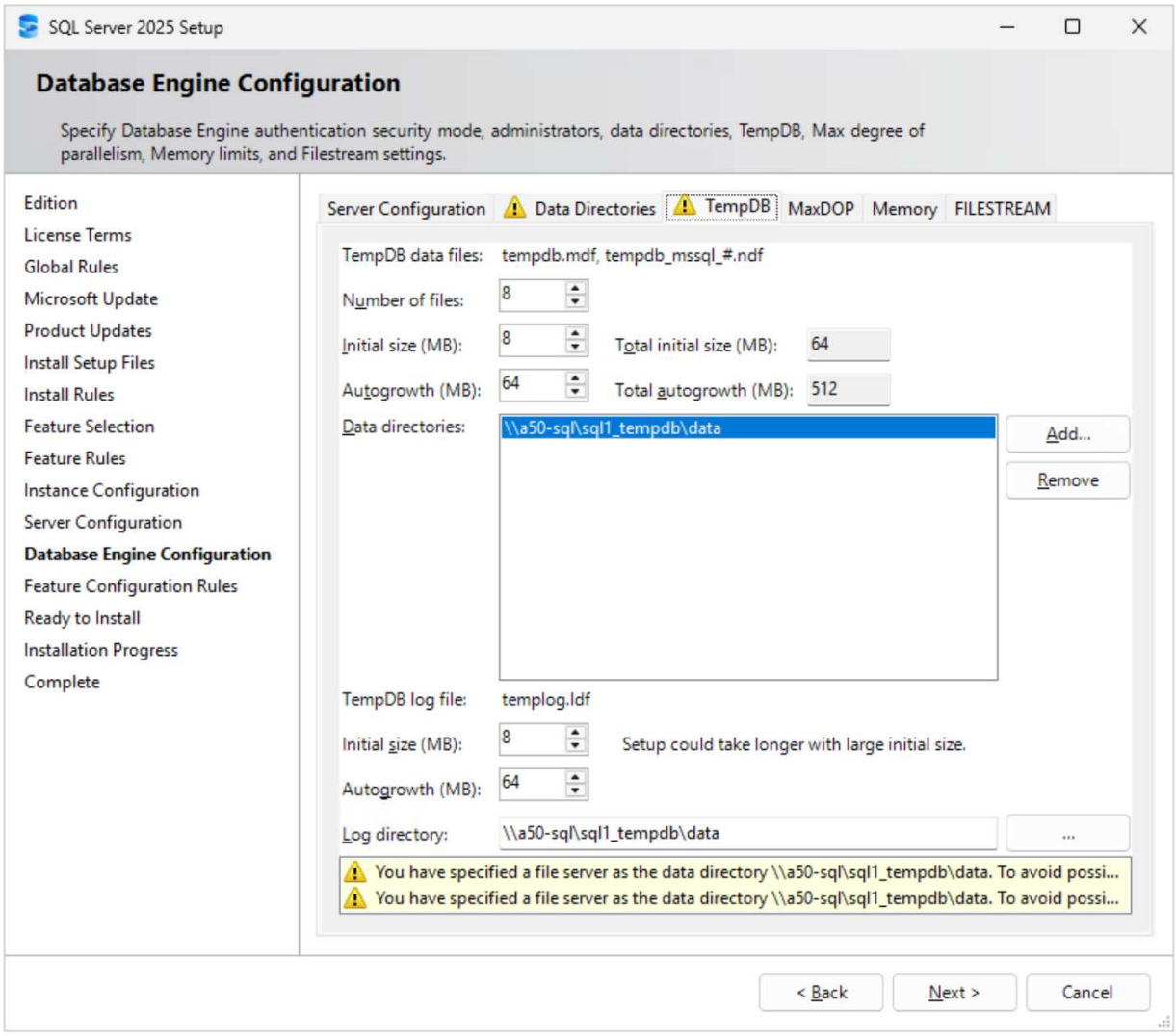


e. Das **Protokollverzeichnis** wird auf dieselbe Freigabe festgelegt (Klick auf **…**). Die Übung verwendet `\\a50-sql\sql1_tempdb\data` sowohl für TempDB-Datendateien als auch für die TempDB-Protokolldatei. Die gelben Warnungen, die darauf hinweisen, dass ein Dateiserver als Datenverzeichnis angegeben wurde, sind zu erwarten.

Es sollte pro logischem CPU-Kern eine TempDB-Datendatei verwendet werden, bis zu 8 Dateien. Die Anfangsgrößen sollten auf den erwarteten TempDB-Arbeitssatz festgelegt werden, sodass TempDB während des Betriebs nicht vergrößert werden muss. Alle Datendateien müssen die gleiche Größe und automatische Vergrößerung aufweisen.

Für die TempDB-Daten- und Protokolldateien ist ein Ordner erforderlich, da die Installation andernfalls fehlschlägt.

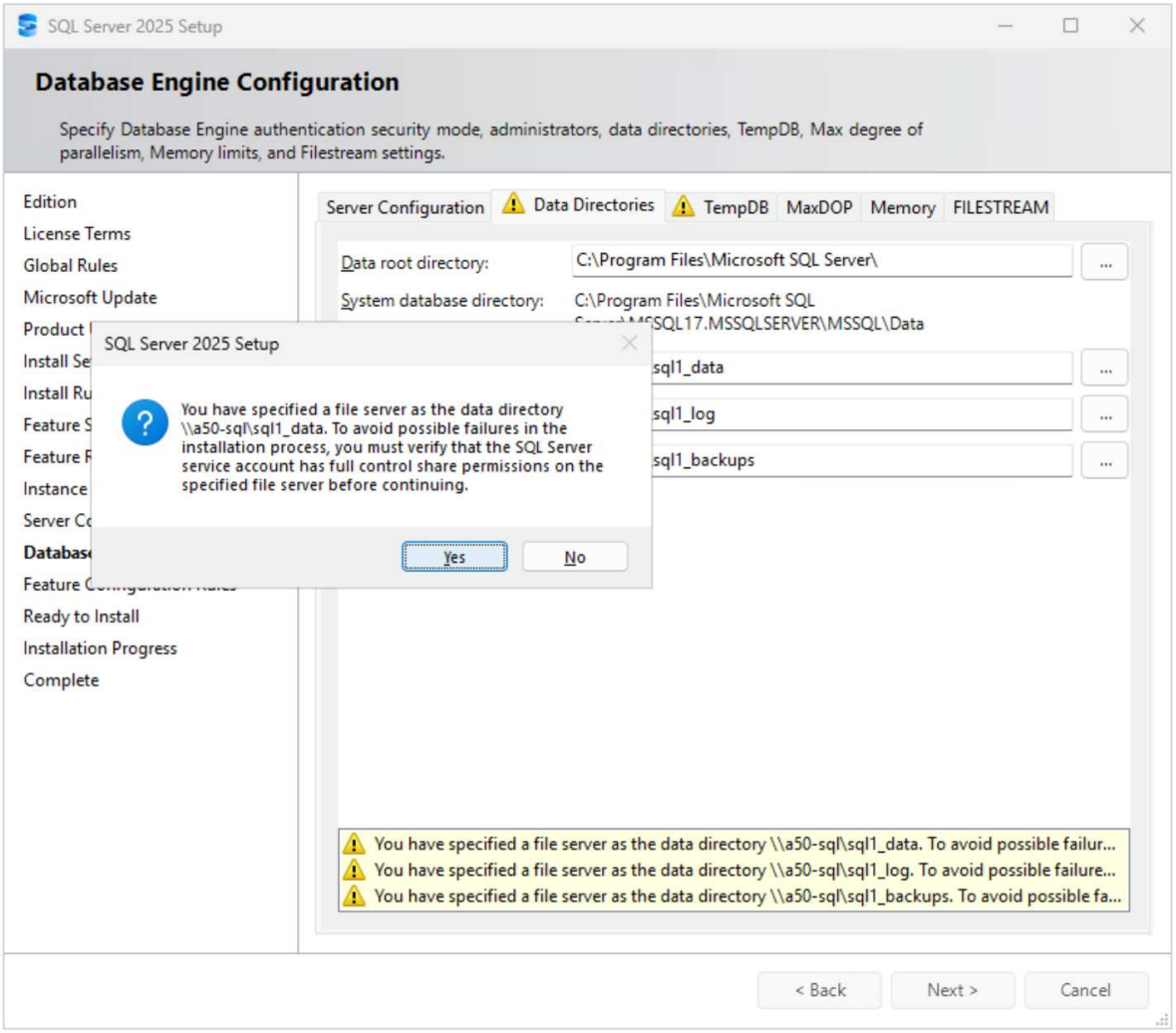
▼ **Beispiel anzeigen**



a. Die Registerkarten **MaxDOP** und **Speicher** werden entsprechend Ihrer Dimensionierung konfiguriert (die empfohlenen Standardwerte sind ein guter Ausgangspunkt); anschließend wird auf **Weiter** geklickt.

b. Für jeden UNC-Pfad zeigt Setup ein Dialogfeld an, in dem die Bestätigung angefordert wird, dass das SQL Server-Dienstkonto auf dem file server über Freigabeberechtigungen für **Full Control** verfügt. Nach der Überprüfung der Berechtigungen (siehe Schritt 3: Erstellen der SQL Server Volumes und SMB-Freigaben und Schritt 6: Windows Server 2025 vorbereiten) kann **Yes** ausgewählt werden.

▼ Beispiel anzeigen

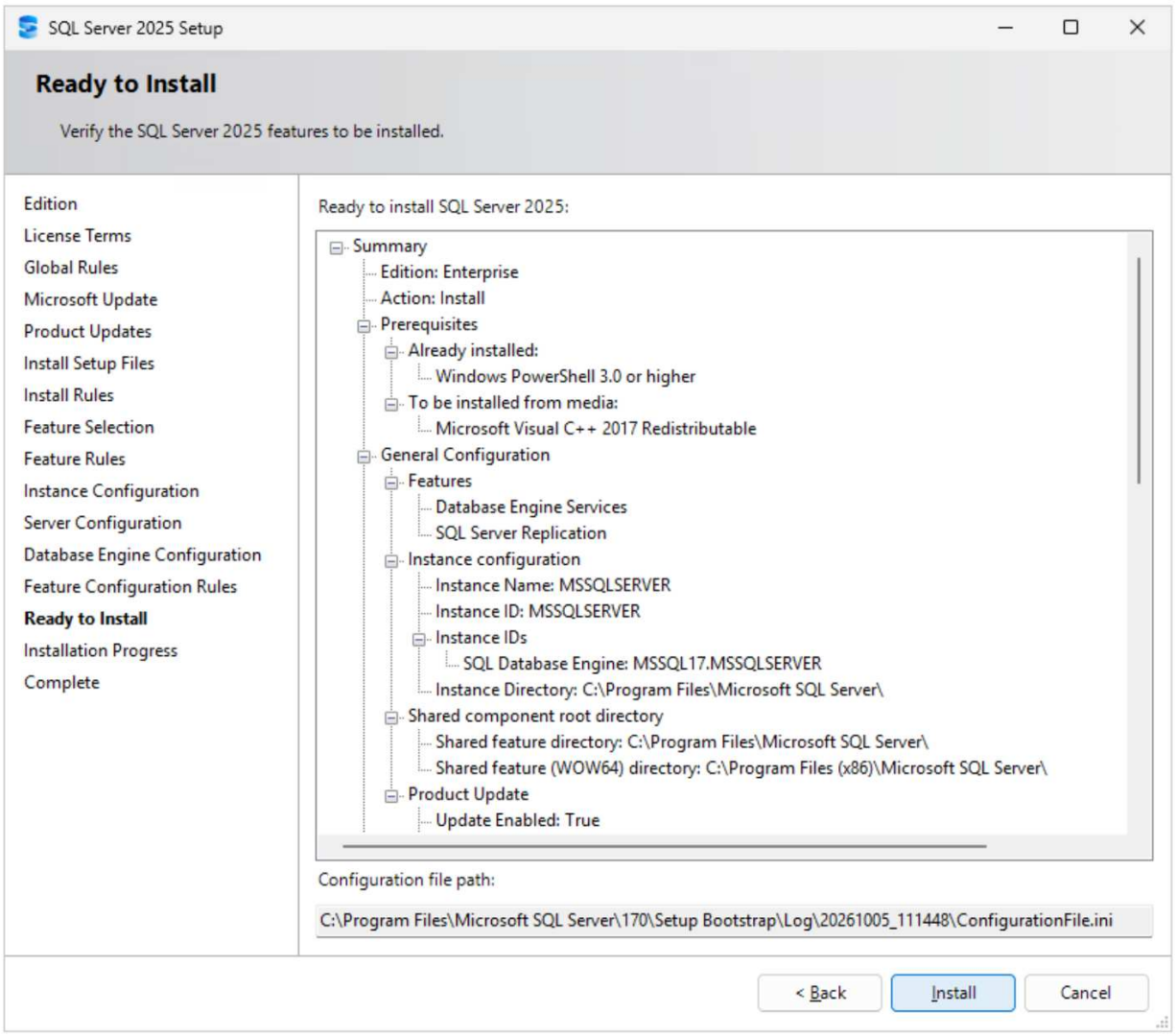


6. Die Installationszusammenfassung ist zu überprüfen, die Installation auszuführen und zu bestätigen, dass alle Funktionen erfolgreich installiert wurden.

   a. Auf der Seite **Bereit zur Installation** wird die Zusammenfassung überprüft; anschließend erfolgt ein Klick auf **Installieren**.

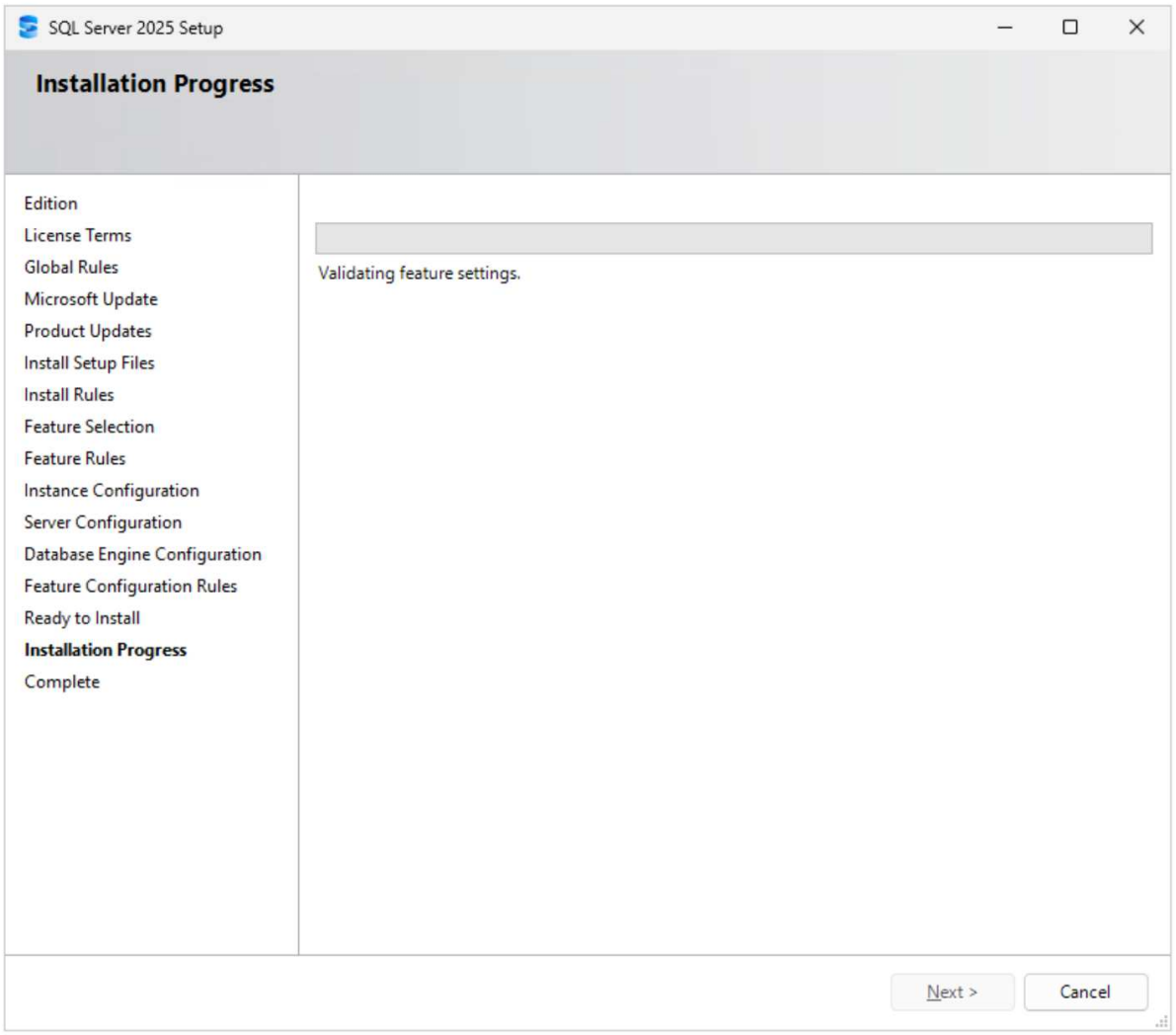
   Der unter **Konfigurationsdateipfad** angezeigte `ConfigurationFile.ini`Pfad lässt sich kopieren. Damit sind unbeaufsichtigte Installationen zusätzlicher SQL Server Hosts (`setup.exe /ConfigurationFile=<path>`möglich.

▼ **Beispiel anzeigen**



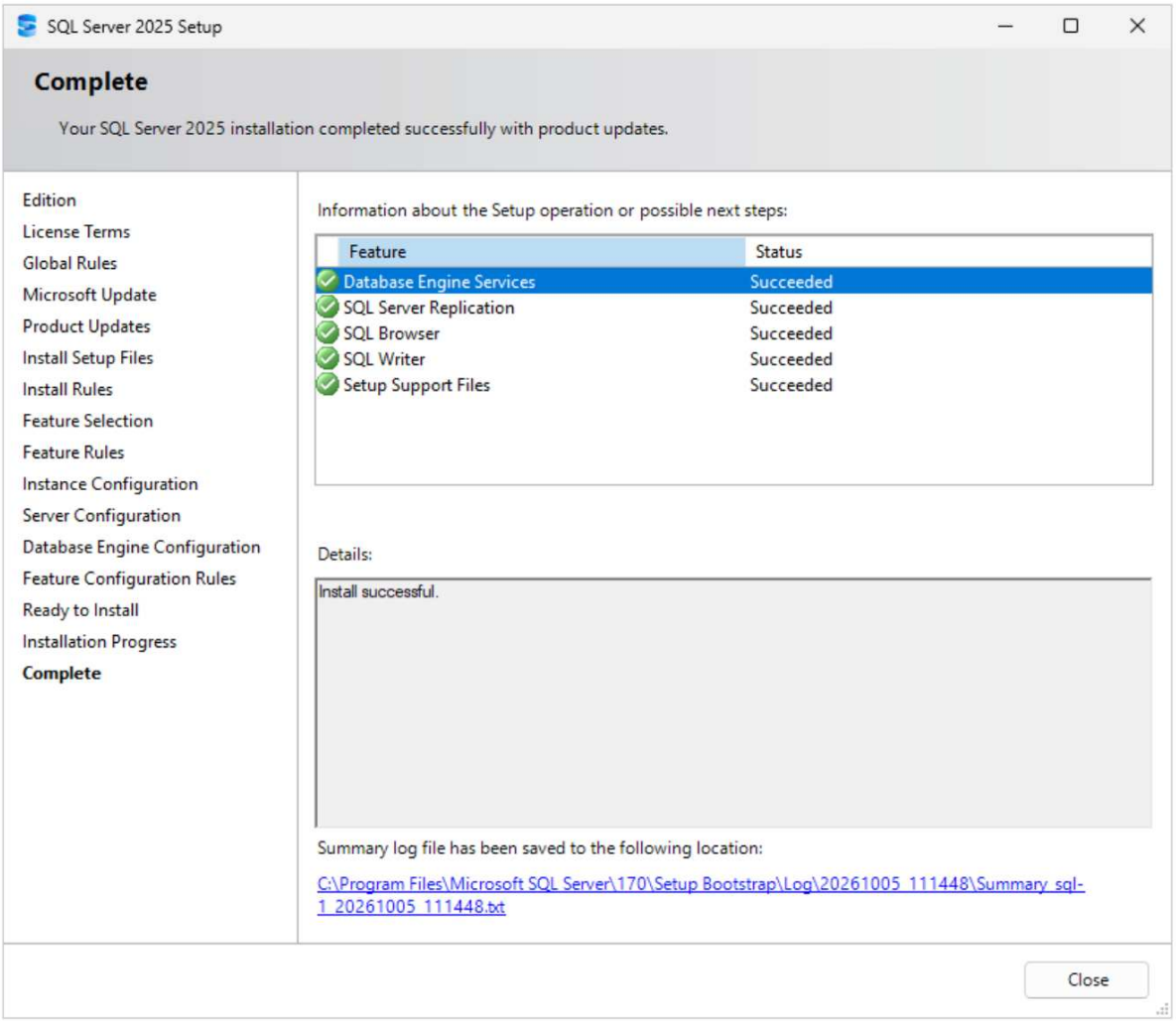
a. Während die Installation läuft, erfolgt eine kurze Wartezeit.

▼ Beispiel anzeigen



b. Nach Abschluss der Installation sollte bei allen Features **Succeeded** angezeigt werden; anschließend kann **Close** ausgewählt werden.

▼ Beispiel anzeigen



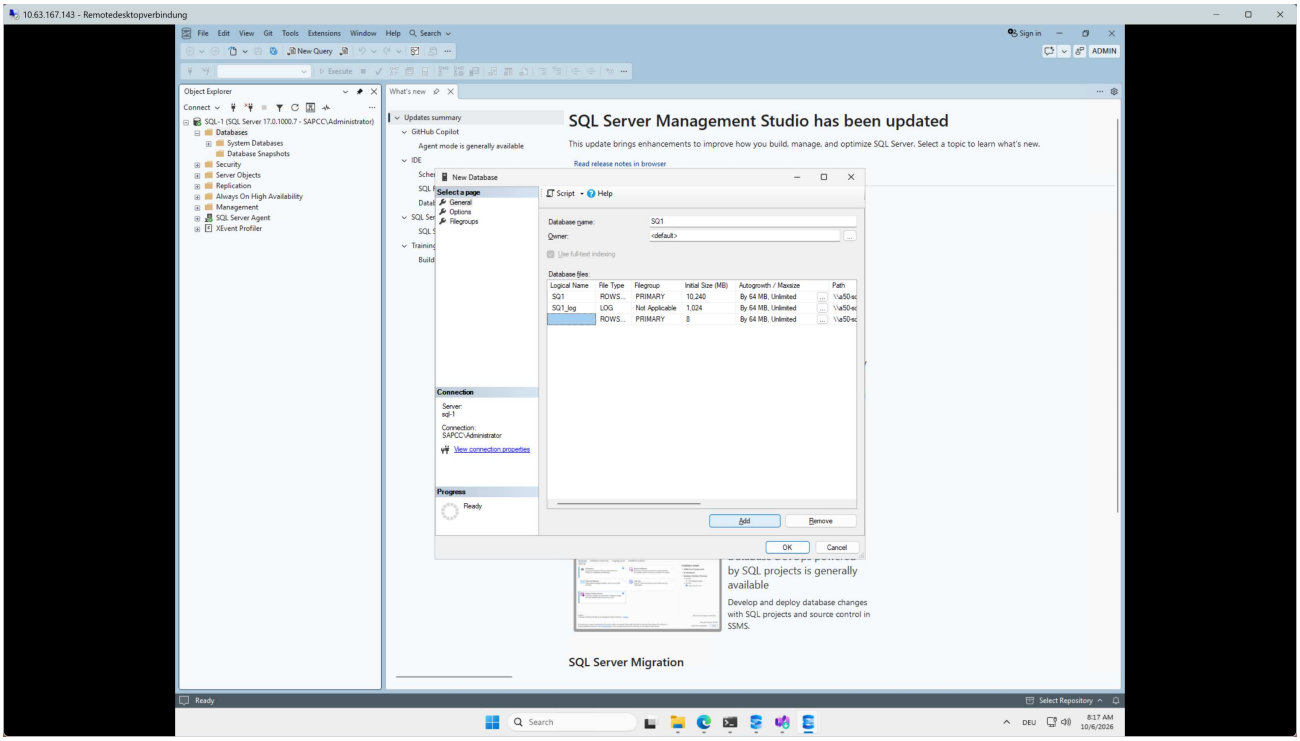
Schritt 8: Installation überprüfen und eine Datenbank erstellen

Eine Testdatenbank wird mit SQL Server Management Studio (SSMS) erstellt, und es wird überprüft, ob sich ihre Daten- und Protokolldateien auf den SMB-Freigaben befinden. Optional kann in ONTAP bestätigt werden, dass die geöffneten Dateien Continuous Availability nutzen.

Schritte

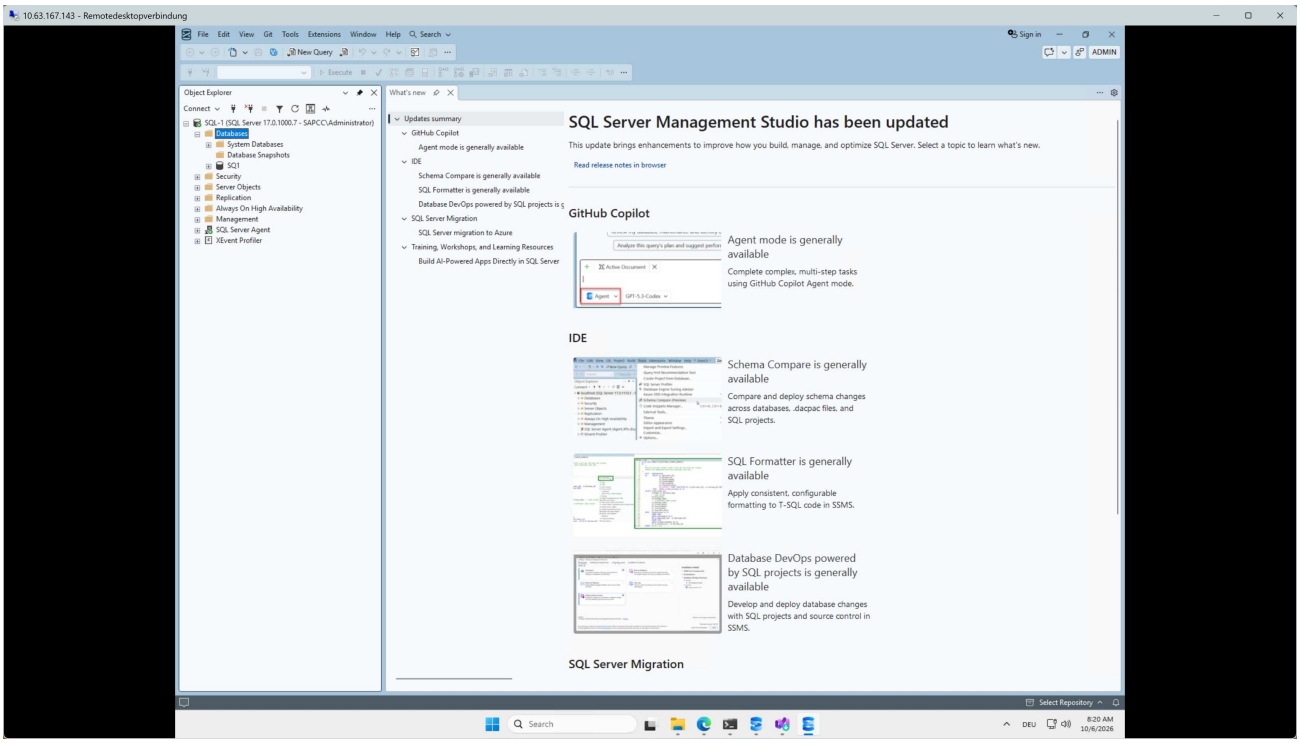
1. Die Installation von SQL Server Management Studio (SSMS) erfolgt über den Link **Install SQL Server Management Tools** im Installation Center oder über die Microsoft-Website.
2. Nach dem Start von SSMS erfolgt die Verbindung zur Instanz (`sql-1`) mit Windows-Authentifizierung.
3. Mit der rechten Maustaste auf **Datenbanken** klicken und **Neue Datenbank…** auswählen. Einen Datenbanknamen (`SQ1` im Lab) eingeben, die anfänglichen Dateigrößen festlegen und auf **OK** klicken. Die Pfade für Daten- und Protokolldateien sind standardmäßig auf `\\a50-sql\sql1_data` und `\\a50-sql\sql1_log` gesetzt.

▼ Beispiel anzeigen



4. Die neue Datenbank erscheint im **Object Explorer**.

▼ **Beispiel anzeigen**



5. Überprüfung der Dateispeicherorte mit 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: Überprüfung der kontinuierlichen Verfügbarkeit der geöffneten Dateien auf ONTAP:

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

Alle SQL Server-Dateien müssen angezeigt werden `continuously-available: Yes`.

Mit einem ONTAP CLI Skript lässt sich der Storage in einem Schritt konfigurieren

Das folgende Skript enthält die vollständige Storage-Konfiguration aus dieser Prozedur. Vor der Ausführung sind die Werte in spitzen Klammern zu ersetzen.

```
# --- 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
```

Sinnvoll ist eine Verteilung der Volumes auf die Aggregate beider Knoten, zum Beispiel Daten und Backups auf Knoten 1 sowie Protokolle und TempDB auf Knoten 2. So lassen sich die Ressourcen beider Controller nutzen.

Weitere Informationen

Weitere Informationen zu den in diesem Verfahren behandelten Themen finden Sie in den folgenden Quellen:

- NetApp: "Microsoft SQL Server und SMB mit ONTAP"
- NetApp: "ONTAP für Microsoft Hyper-V und SQL Server über SMB-Lösungen konfigurieren"
- NetApp: "SMB-Server- und Volume-Anforderungen für SQL Server über SMB"
- Microsoft: "Installation von SQL Server mit SMB Fileshare Storage"
- NetApp: "SnapCenter Plug-in für Microsoft SQL Server Übersicht"
- NetApp: "Interoperability Matrix Tool (IMT)"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.