



# **Microsoft SQL Server**

## Enterprise applications

NetApp  
January 02, 2026

# Inhalt

Microsoft SQL Server .....	1
Überblick .....	1
Microsoft SQL Server-Workloads .....	1
Datenbankkonfiguration .....	2
CPU-Konfiguration .....	2
Speicherkonfiguration .....	5
Shared Instance oder dedizierte Instanz .....	8
Tempdb-Dateien .....	9
Storage-Konfiguration auf AFF/FAS Systemen .....	10
Überblick .....	10
Datenbankdateien und Dateigruppen .....	12
Storage-Effizienz .....	17
Datensicherung .....	22
Disaster Recovery .....	25
Storage-Konfiguration auf ASA r2-Systemen .....	46
Überblick .....	46
Datenbankdateien und Dateigruppen .....	48
Datensicherung .....	53
Disaster Recovery .....	54
Datensicherheit .....	70
Snapshots .....	70
Manipulationssichere Snapshots .....	70
SnapMirror Replizierung .....	71
Storage Virtual Machines .....	71
Administrative RBAC .....	71
Multi-Faktor-Authentifizierung (MFA) .....	72
API RBAC .....	72
Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV) .....	72

# Microsoft SQL Server

## Überblick

ONTAP bietet eine Sicherheits- und Performance-Lösung der Enterprise-Klasse für Ihre Microsoft SQL Server Datenbanken und stellt gleichzeitig erstklassige Tools für das Management Ihrer Umgebung bereit.



Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4590: Best Practice Guide for Microsoft SQL Server with ONTAP*

NetApp geht davon aus, dass der Leser über die folgenden Kenntnisse verfügt:

- ONTAP
- Architektur und Administration von Microsoft SQL Server
- NetApp SnapCenter als Backup-Software, einschließlich:
  - SnapCenter Plug-in für Microsoft Windows
  - SnapCenter Plug-in für SQL Server

Dieser Abschnitt zu Best Practices beschränkt sich auf technisches Design basierend auf den von NetApp für die Storage-Infrastruktur empfohlenen Prinzipien und bevorzugten Standards. Die End-to-End-Implementierung ist nicht im Umfang enthalten.

Informationen zur Kompatibilität der NetApp-Produkte finden Sie unter "["NetApp Interoperabilitäts-Matrix-Tool \(IMT\)"](#)".

## Microsoft SQL Server-Workloads

Vor der Bereitstellung von SQL Server müssen Sie die Workload-Anforderungen der von Ihren SQL Server-Datenbankinstanzen unterstützten Applikationen kennen. Jede Applikation hat unterschiedliche Anforderungen an Kapazität, Performance und Verfügbarkeit. Daher sollte jede Datenbank für eine optimale Unterstützung dieser Anforderungen entworfen werden. Viele Unternehmen klassifizieren Datenbanken in mehrere Management-Tiers unter Verwendung von Anwendungsanforderungen zur Definition von SLAs. SQL Server-Workloads werden häufig wie unten beschrieben kategorisiert:

- OLTP sind häufig die kritischsten Datenbanken in einem Unternehmen. Diese Datenbanken stehen in der Regel kundenorientierten Applikationen gegenüber und werden als unverzichtbar für die Kernprozesse des Unternehmens angesehen. Für geschäftskritische OLTP-Datenbanken und die von ihnen unterstützten Applikationen gibt es oft SLAs, die hohe Performance erfordern, nur mit Einschränkungen bei der Performance verbunden sind und maximale Verfügbarkeit erfordern. Sie können auch Kandidaten für „Always On“-Failover-Cluster oder „Always On“-Verfügbarkeitsgruppen sein. Der I/O-Mix bei diesen Datenbanktypen ist in der Regel durch 75 bis 90 % zufällige Lesevorgänge und 25 bis 10 % Schreibzugriffe gekennzeichnet.
- Decision Support System (DSS)-Datenbanken, auch als Data Warehouses bezeichnet. Diese Datenbanken sind für viele Unternehmen, die auf Analysen für ihr Geschäft vertrauen, geschäftskritisch. Diese Datenbanken sind sensibel für die CPU-Auslastung und Lesevorgänge von der Festplatte, wenn Abfragen ausgeführt werden. In vielen Unternehmen sind DSS-Datenbanken zum Monats-, Quartals- und Jahresende am wichtigsten. Dieser Workload verfügt in der Regel über eine I/O-Kombination mit Lesevorgängen von fast 100 % und der I/O-Durchsatz ist oft wichtiger als IOPS.

# Datenbankkonfiguration

## CPU-Konfiguration

Die SQL Server-Performance weist mehrere Abhängigkeiten von der CPU- und Kernkonfiguration auf.

### Hyper-Threading

Hyper-Threading bezieht sich entweder auf die Implementierung von simultanem Multithreading (SMT), wodurch die Parallelisierung von Berechnungen auf x86-Prozessoren verbessert wird. SMT ist sowohl für Intel als auch für AMD Prozessoren verfügbar.

Hyper-Threading führt zu logischen CPUs, die dem Betriebssystem als physische CPUs angezeigt werden. SQL Server erkennt dann die zusätzlichen CPUs und nutzt sie so, als gäbe es mehr Kerne als physisch vorhanden. Durch eine stärkere Parallelisierung kann die Performance erheblich gesteigert werden.

Der Nachteil hierbei ist, dass jede SQL Server-Version ihre eigenen Einschränkungen hinsichtlich der Rechenleistung hat, die sie verwenden kann. Weitere Informationen finden Sie unter ["Kapazitätsbeschränkungen für die Datenverarbeitung nach Edition von SQL Server"](#).

### Kerne und Lizenzierung

Es gibt zwei Optionen für die Lizenzierung von SQL Server. Die erste wird als Server + Client Access License (CAL)-Modell bezeichnet; die zweite ist das pro Prozessor-Core-Modell. Obwohl Sie mit der Server + CAL-Strategie auf alle in SQL Server verfügbaren Produktfunktionen zugreifen können, gibt es eine Hardwaregrenze von 20 CPU-Kernen pro Sockel. Selbst wenn Sie SQL Server Enterprise Edition + CAL für einen Server mit mehr als 20 CPU-Kernen pro Socket verwenden, kann die Anwendung nicht alle diese Kerne gleichzeitig auf dieser Instanz verwenden.

Das Bild unten zeigt die SQL Server-Protokollmeldung nach dem Start, die die Durchsetzung des Core-Limits anzeigt.

```

2017-01-11 07:16:30.71 Server      Microsoft SQL Server 2016
(RTM) - 13.0.1601.5 (X64)
Apr 29 2016 23:23:58
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows Server 2016
Datacenter 6.3 <X64> (Build 14393: )

2017-01-11 07:16:30.71 Server      UTC adjustment: -8:00
2017-01-11 07:16:30.71 Server      (c) Microsoft Corporation.
2017-01-11 07:16:30.71 Server      All rights reserved.
2017-01-11 07:16:30.71 Server      Server process ID is 10176.
2017-01-11 07:16:30.71 Server      System Manufacturer:
'FUJITSU', System Model: 'PRIMERGY RX2540 M1'.
2017-01-11 07:16:30.71 Server      Authentication mode is MIXED.
2017-01-11 07:16:30.71 Server      Logging SQL Server messages
in file 'C:\Program Files\Microsoft SQL Server
\MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG'.
2017-01-11 07:16:30.71 Server      The service account is 'SEA-
TM\FUJIA2R30$'. This is an informational message; no user action
is required.
2017-01-11 07:16:30.71 Server      Registry startup parameters:
  -d C:\Program Files\Microsoft SQL Server
  \MSSQL13.MSSQLSERVER\MSSQL\DATA\master.mdf
  -e C:\Program Files\Microsoft SQL Server
  \MSSQL13.MSSQLSERVER\MSSQL\Log\ERRORLOG
  -l C:\Program Files\Microsoft SQL Server
  \MSSQL13.MSSQLSERVER\MSSQL\DATA\mastlog.ldf
  -T 3502
  -T 834
2017-01-11 07:16:30.71 Server      Command Line Startup
Parameters:
  -s "MSSQLSERVER"
2017-01-11 07:16:30.72 Server      SQL Server detected 2 sockets
with 18 cores per socket and 36 logical processors per socket,
72 total logical processors; using 40 logical processors based
on SQL Server licensing. This is an informational message; no
user action is required.
2017-01-11 07:16:30.72 Server      SQL Server is starting at

```

Um alle CPUs zu verwenden, sollten Sie daher die Prozessorkern-Lizenz verwenden. Weitere Informationen zur SQL Server-Lizenziierung finden Sie unter "["SQL Server 2022: Ihre moderne Datenplattform"](#)".

## CPU-Affinität

Es ist unwahrscheinlich, dass Sie die Standardeinstellungen für die Prozessoraffinität ändern müssen, es sei denn, Sie stoßen auf Leistungsprobleme, aber es lohnt sich immer noch zu verstehen, was sie sind und wie sie funktionieren.

SQL Server unterstützt die Prozessoraffinität durch zwei Optionen:

- CPU-Affinitätsmaske
- Affinity-E/A-Maske

SQL Server verwendet alle CPUs, die über das Betriebssystem verfügbar sind (wenn die Prozessorkern-Lizenz gewählt wird). Es erstellt auch Scheduler für jede CPU, um die Ressourcen für jeden beliebigen Workload optimal zu nutzen. Beim Multitasking kann das Betriebssystem oder andere Anwendungen auf dem Server die Prozess-Threads von einem Prozessor zum anderen wechseln. SQL Server ist eine ressourcenintensive Applikation und die Performance kann in diesem Fall beeinträchtigt werden. Um die Auswirkungen zu minimieren, können Sie die Prozessoren so konfigurieren, dass die gesamte SQL Server-Last an eine vorgewählte Prozessorgruppe weitergeleitet wird. Dies wird durch die CPU Affinitätsmaske erreicht.

Die Affinity I/O-Maskenoption bindet SQL Server-Festplatten-I/O an eine Teilmenge von CPUs. In SQL Server-OLTP-Umgebungen kann diese Erweiterung die Performance von SQL Server-Threads, die I/O-Vorgänge ausgeben, erheblich verbessern.

## Max. Parallelitätsgrad (MAXDOP)

Standardmäßig verwendet SQL Server während der Abfrageausführung alle verfügbaren CPUs, wenn die Prozessorkern-Lizenz ausgewählt wurde.

Dies ist zwar hilfreich bei umfangreichen Abfragen, kann jedoch zu Leistungsproblemen und zur Begrenzung der Parallelität führen. Ein besserer Ansatz besteht darin, die Parallelität auf die Anzahl der physischen Kerne in einem einzelnen CPU-Socket zu beschränken. Beispielsweise sollte auf einem Server mit zwei physischen CPU-Sockeln mit 12 Kernen pro Socket, unabhängig von Hyper-Threading, MAXDOP auf 12 gesetzt werden. MAXDOP Die zu verwendende CPU kann nicht eingeschränkt oder diktiert werden. Stattdessen beschränkt es die Anzahl der CPUs, die von einer einzelnen Batch-Abfrage verwendet werden können.

 **NetApp empfiehlt** für DSS wie Data Warehouses, beginnen Sie mit MAXDOP 50 und erkunden Sie Tuning auf oder ab, falls erforderlich. Stellen Sie sicher, dass Sie die kritischen Abfragen in Ihrer Anwendung messen, wenn Sie Änderungen vornehmen.

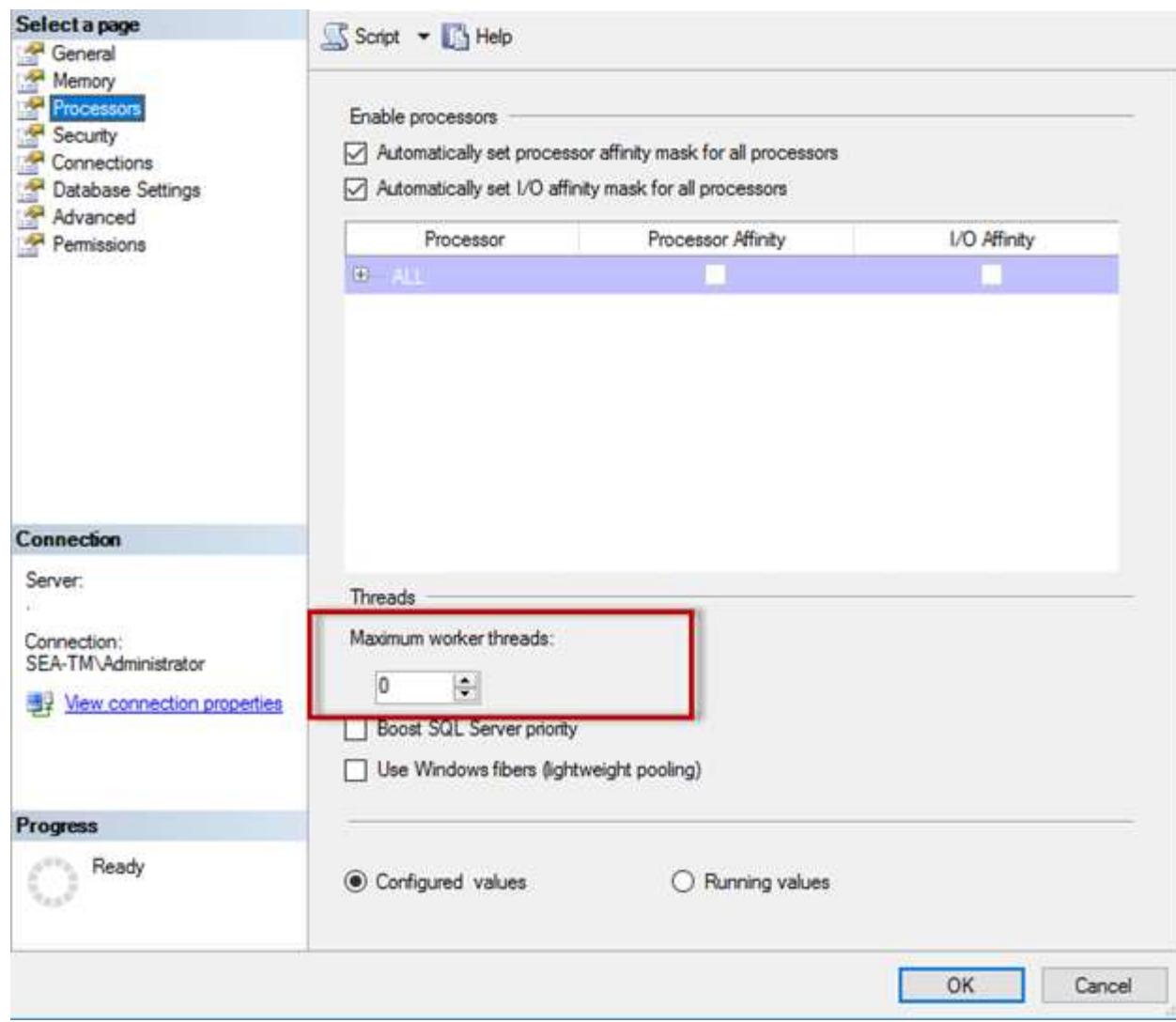
## Max. Worker-Threads

Die Option Max. Worker-Threads hilft, die Leistung zu optimieren, wenn eine große Anzahl von Clients mit SQL Server verbunden ist.

Normalerweise wird für jede Abfrage ein separater Betriebssystem-Thread erstellt. Wenn Hunderte von gleichzeitigen Verbindungen zu SQL Server hergestellt werden, kann eine Konfiguration mit einem Thread pro Abfrage übermäßige Systemressourcen beanspruchen. Die `max worker threads` Option verbessert die Leistung, indem SQL Server in die Lage versetzt wird, einen Pool von Worker-Threads zu erstellen, die gemeinsam eine größere Anzahl von Abfrage-Anforderungen verarbeiten können.

Der Standardwert ist 0, wodurch SQL Server die Anzahl der Worker-Threads beim Start automatisch konfigurieren kann. Dies funktioniert für die meisten Systeme. Max Worker-Threads sind eine erweiterte Option und sollten nicht ohne Unterstützung durch einen erfahrenen Datenbankadministrator (DBA) geändert werden.

Wann sollten Sie SQL Server so konfigurieren, dass mehr Worker-Threads verwendet werden? Wenn die durchschnittliche Länge der Arbeitswarteschlange für jeden Scheduler über 1 liegt, können Sie vom Hinzufügen weiterer Threads zum System profitieren, jedoch nur, wenn die Last nicht CPU-gebunden ist oder andere schwere Wartezeiten auftritt. Wenn einer dieser Vorgänge stattfindet, sind weitere Threads nicht hilfreich, da sie schließlich auf andere Systemengpässe warten müssen. Weitere Informationen zu max worker Threads finden Sie unter "[Konfigurieren Sie die Option max Worker Threads Server Configuration](#)".



#### Konfigurieren von max Worker-Threads mit SQL Server Management Studio

Das folgende Beispiel zeigt, wie Sie die Option Max. Work Threads mit T-SQL konfigurieren.

```
EXEC sp_configure 'show advanced options', 1;
GO
RECONFIGURE ;
GO
EXEC sp_configure 'max worker threads', 900 ;
GO
RECONFIGURE;
GO
```

#### Speicherkonfiguration

Im folgenden Abschnitt werden die SQL Server-Speichereinstellungen erläutert, die zur Optimierung der Datenbankleistung erforderlich sind.

## Max. Serverspeicher

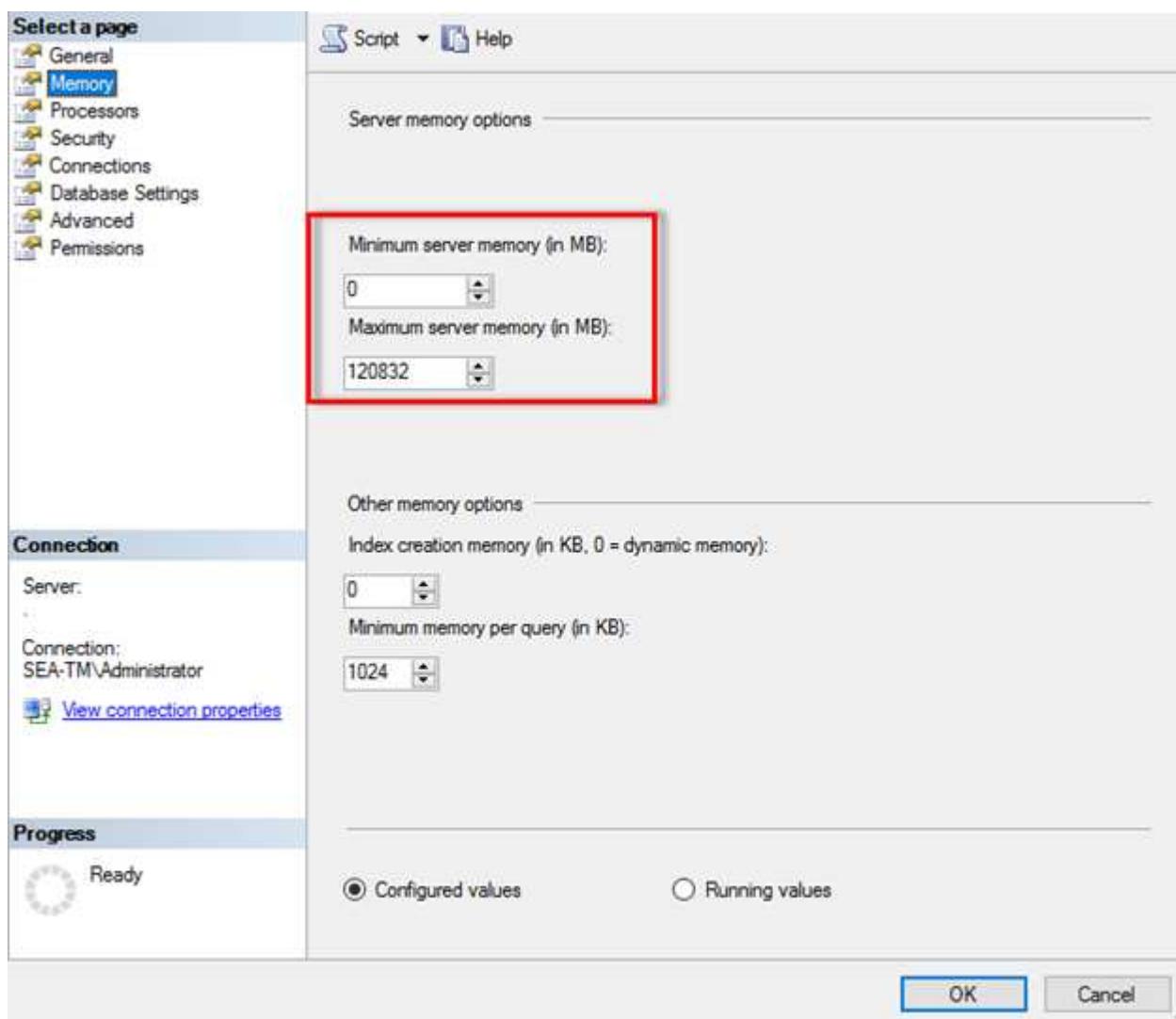
Mit der Option „Max. Serverspeicher“ wird die maximale Speichergröße festgelegt, die die SQL Server-Instanz verwenden kann. Sie wird in der Regel verwendet, wenn mehrere Anwendungen auf demselben Server ausgeführt werden, auf dem SQL Server ausgeführt wird, und Sie sicherstellen möchten, dass diese Anwendungen über genügend Arbeitsspeicher verfügen, um ordnungsgemäß zu funktionieren.

Einige Anwendungen verwenden nur den verfügbaren Speicher, wenn sie starten, und fordern keinen zusätzlichen Speicher an, selbst wenn sie unter Speicherdruck stehen. Hier kommt die maximale Serverspeichereinstellung ins Spiel.

Auf einem SQL Server-Cluster mit mehreren SQL Server-Instanzen könnte jede Instanz mit Ressourcen konkurrieren. Durch die Festlegung einer Speichergrenze für jede SQL Server-Instanz kann eine optimale Performance für jede Instanz gewährleistet werden.



**NetApp empfiehlt**, mindestens 4 GB bis 6 GB RAM für das Betriebssystem zu belassen, um Leistungsprobleme zu vermeiden.



## Anpassen des minimalen und maximalen Serverspeichers mit SQL Server Management Studio

Die Verwendung von SQL Server Management Studio zur Anpassung des minimalen oder maximalen Serverspeichers erfordert einen Neustart des SQL Server-Dienstes. Sie können den Serverspeicher auch

mithilfe von Transact SQL (T-SQL) anpassen, indem Sie diesen Code verwenden:

```
EXECUTE sp_configure 'show advanced options', 1
GO
EXECUTE sp_configure 'min server memory (MB)', 2048
GO
EXEC sp_configure 'max server memory (MB)', 120832
GO
RECONFIGURE WITH OVERRIDE
```

## **Uneinheitlicher Speicherzugriff**

NUMA (Ununiform Memory Access) ist eine Technologie zur Optimierung des Speicherzugriffs, die dazu beiträgt, eine zusätzliche Belastung des Prozessorbusses zu vermeiden.

Wenn NUMA auf einem Server konfiguriert ist, auf dem SQL Server installiert ist, ist keine zusätzliche Konfiguration erforderlich, da SQL Server NUMA-fähig ist und auf NUMA-Hardware eine gute Performance erzielt.

## **Index Speicher erstellen**

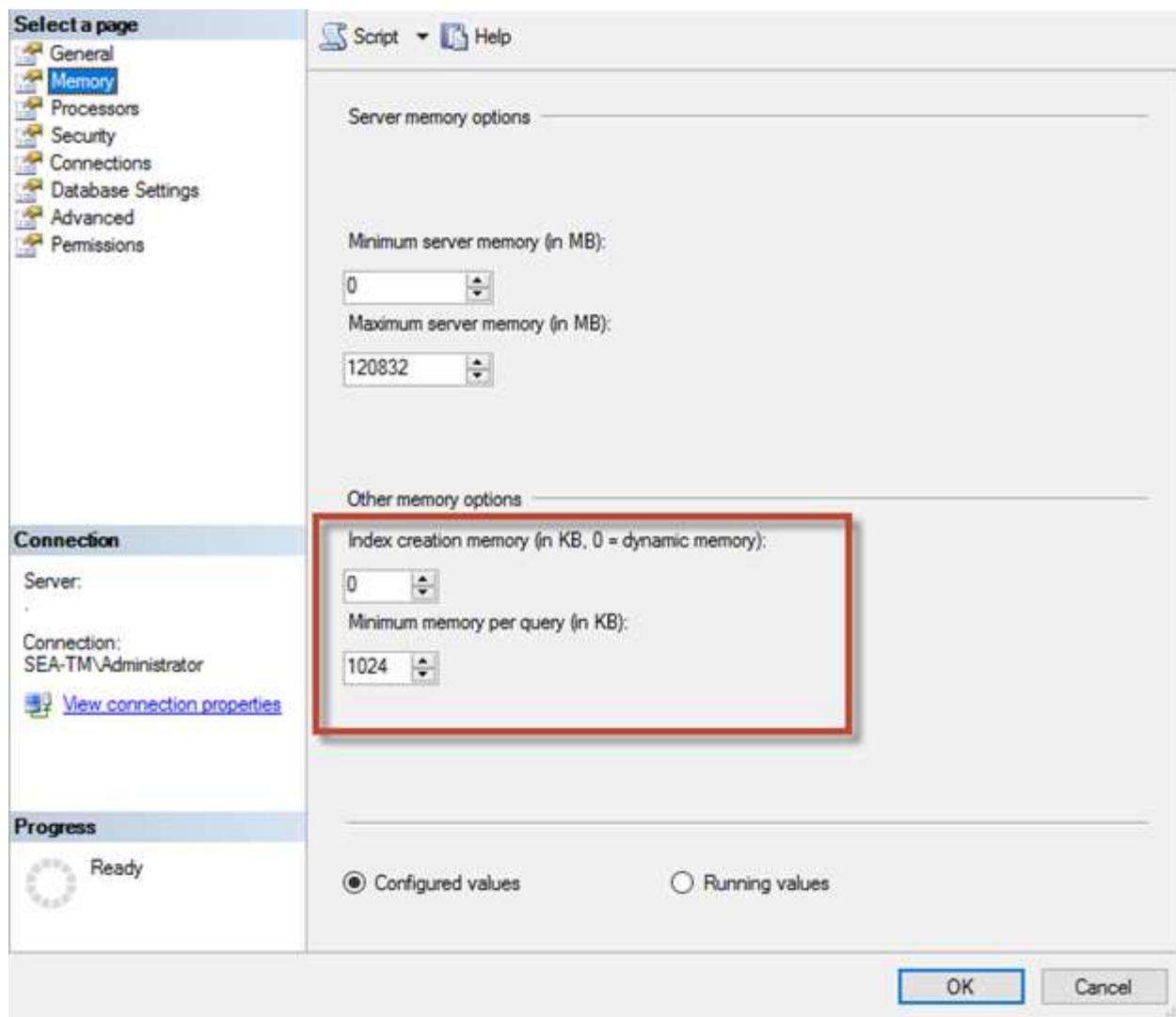
Die Option Index create Memory ist eine weitere erweiterte Option, die normalerweise nicht von den Standardwerten geändert werden muss.

Er steuert die maximale RAM-Größe, die ursprünglich für die Erstellung von Indizes zugewiesen wurde. Der Standardwert für diese Option ist 0, was bedeutet, dass sie von SQL Server automatisch verwaltet wird. Wenn Sie jedoch Schwierigkeiten beim Erstellen von Indizes haben, sollten Sie den Wert dieser Option erhöhen.

## **Min. Arbeitsspeicher pro Abfrage**

Wenn eine Abfrage ausgeführt wird, versucht SQL Server, die optimale Speichergröße für eine effiziente Ausführung zuzuweisen.

Standardmäßig weist die Einstellung Min. Speicher pro Abfrage >= bis 1024 KB für jede auszufüllende Abfrage zu. Es empfiehlt sich, diese Einstellung auf den Standardwert zu belassen, damit SQL Server die für Indexerstellung zugewiesene Speichermenge dynamisch verwalten kann. Wenn SQL Server jedoch über mehr RAM verfügt, als für eine effiziente Ausführung erforderlich ist, kann die Leistung einiger Abfragen erhöht werden, wenn Sie diese Einstellung erhöhen. Solange also auf dem Server, der nicht von SQL Server verwendet wird, Speicher verfügbar ist, können andere Anwendungen oder das Betriebssystem diese Einstellung erhöhen, was die gesamte SQL Server-Leistung verbessern kann. Wenn kein freier Speicher verfügbar ist, kann eine Erhöhung dieser Einstellung die Gesamtleistung beeinträchtigen.



## Shared Instance oder dedizierte Instanz

SQL Server kann als einzelne Instanz pro Server oder als mehrere Instanzen konfiguriert werden. Die richtige Entscheidung hängt in der Regel von Faktoren ab, z. B. ob der Server für die Produktion oder Entwicklung verwendet werden soll, ob die Instanz für den Geschäftsbetrieb und die Leistungsziele entscheidend ist.

Konfigurationen für gemeinsam genutzte Instanzen sind zwar zunächst einfacher zu konfigurieren, können jedoch zu Problemen führen, bei denen Ressourcen aufgeteilt oder gesperrt werden. Dies führt wiederum zu Leistungsproblemen für andere Anwendungen, bei denen Datenbanken auf der gemeinsam genutzten SQL Server-Instanz gehostet werden.

Die Fehlerbehebung bei Performance-Problemen kann kompliziert sein, da Sie herausfinden müssen, welche Instanz die eigentliche Ursache ist. Diese Frage wird gegen die Kosten von Betriebssystemlizenzen und SQL Server-Lizenzen abgewogen. Wenn die Applikations-Performance oberste Priorität hat, ist eine dedizierte Instanz sehr empfehlenswert.

Microsoft lizenziert SQL Server pro Kern auf Serverebene und nicht pro Instanz. Aus diesem Grund sind Datenbankadministratoren versucht, so viele SQL Server-Instanzen zu installieren, wie der Server verarbeiten kann, um Lizenzierungskosten zu sparen, was später zu größeren Performanceproblemen führen kann.



**NetApp empfiehlt**, wenn möglich dedizierte SQL Server-Instanzen zu wählen, um optimale Leistung zu erzielen.

## Tempdb-Dateien

Die Tempdb-Datenbank kann stark genutzt werden. Neben der optimalen Platzierung von Benutzerdatenbankdateien auf ONTAP ist die Platzierung von tempdb-Datendateien auch wichtig, um die Zuweisungskonflikte zu verringern. Tempdb sollte auf einer separaten Festplatte abgelegt und nicht für Benutzerdaten dateien freigegeben werden.

Seitenkonflikte können auf den Seiten Global Allocation Map (GAM), Shared Global Allocation Map (SGAM) oder Page Free Space (PFS) auftreten, wenn SQL Server auf spezielle Systemseiten schreiben muss, um neue Objekte zuzuweisen. Verriegelungen sperren diese Seiten im Speicher. In einer stark ausgelasteten SQL Server-Instanz kann es lange dauern, bis ein Latch auf einer Systemseite in tempdb abgerufen wird. Dies führt zu längeren Abfragezeiten und wird als Latch Contention bezeichnet. Lesen Sie die folgenden Best Practices für das Erstellen von tempdb-Datendateien:

- Für < oder = bis 8 Kerne: Tempdb-Datendateien = Anzahl der Kerne
- Für > 8 Kerne: 8 tempdb-Datendateien
- Die tempdb-Datendatei sollte mit gleicher Größe erstellt werden

Mit dem folgenden Beispielskript wird tempdb geändert, indem acht tempdb-Dateien gleicher Größe erstellt und tempdb auf den Mount-Punkt für SQL Server 2012 und höher verschoben C:\MSSQL\tempdb wird.

```
use master

go

-- Change logical tempdb file name first since SQL Server shipped with
logical file name called tempdev

alter database tempdb modify file (name = 'tempdev', newname =
'tempdev01');

-- Change location of tempdev01 and log file

alter database tempdb modify file (name = 'tempdev01', filename =
'C:\MSSQL\tempdb\tempdev01.mdf');

alter database tempdb modify file (name = 'templog', filename =
'C:\MSSQL\tempdb\templog.ldf');

GO

-- Assign proper size for tempdev01
```

```

ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'tempdev01', SIZE = 10GB );

ALTER DATABASE [tempdb] MODIFY FILE ( NAME = N'templog', SIZE = 10GB );

GO

-- Add more tempdb files

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev02', FILENAME =
N'C:\MSSQL\tempdb\tempdev02.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev03', FILENAME =
N'C:\MSSQL\tempdb\tempdev03.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev04', FILENAME =
N'C:\MSSQL\tempdb\tempdev04.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev05', FILENAME =
N'C:\MSSQL\tempdb\tempdev05.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev06', FILENAME =
N'C:\MSSQL\tempdb\tempdev06.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev07', FILENAME =
N'C:\MSSQL\tempdb\tempdev07.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

ALTER DATABASE [tempdb] ADD FILE ( NAME = N'tempdev08', FILENAME =
N'C:\MSSQL\tempdb\tempdev08.ndf' , SIZE = 10GB , FILEGROWTH = 10%);

GO

```

Ab SQL Server 2016 wird die Anzahl der für das Betriebssystem sichtbaren CPU-Kerne während der Installation automatisch erkannt. Auf Basis dieser Anzahl berechnet und konfiguriert SQL Server die Anzahl der für eine optimale Performance erforderlichen tempdb-Dateien.

## Storage-Konfiguration auf AFF/FAS Systemen

### Überblick

Die Kombination aus ONTAP Storage-Lösungen und Microsoft SQL Server ermöglicht Datenbank-Storage-Designs der Enterprise-Klasse, die auch die anspruchsvollsten Applikationsanforderungen von heute erfüllen.

Um eine SQL Server auf ONTAP-Lösung zu optimieren, müssen Sie das I/O-Muster und die Merkmale des SQL Servers kennen. Ein gut konzipiertes Storage Layout für eine SQL Server Datenbank muss die Performance-Anforderungen von SQL Server unterstützen und gleichzeitig maximale Management-Fähigkeit

der Infrastruktur als Ganzes bieten. Ein gutes Storage-Layout ermöglicht außerdem eine erfolgreiche Erstimplementierung und ein reibungsloses Wachstum der Umgebung im Laufe der Zeit, während das Unternehmen wächst.

## Datenspeicher Design

Für SQL Server-Datenbanken, die keine Backups mit SnapCenter durchführen, empfiehlt Microsoft, die Daten und Log-Dateien auf separaten Laufwerken zu platzieren. Bei Anwendungen, die gleichzeitig Daten aktualisieren und anfordern, ist die Protokolldatei schreibintensiv und die Datendatei (je nach Anwendung) ist Lese-/schreibintensiv. Für den Datenabruf wird die Protokolldatei nicht benötigt. Daher können Datenanfragen aus der Datendatei auf dem eigenen Laufwerk bearbeitet werden.

Wenn Sie eine neue Datenbank erstellen, empfiehlt Microsoft, getrennte Laufwerke für die Daten und Protokolle anzugeben. Um Dateien nach der Datenbankerstellung zu verschieben, muss die Datenbank offline geschaltet werden. Weitere Empfehlungen von Microsoft finden Sie unter "[Platzieren Sie Daten- und Protokolldateien auf separaten Laufwerken](#)".

## Aggregate

Aggregate sind die Storage-Container der niedrigsten Ebene für NetApp Storage-Konfigurationen. Im Internet gibt es eine ältere Dokumentation, die die Trennung von E/A auf verschiedene Sätze zugrunde liegender Laufwerke empfiehlt. Dies wird bei ONTAP nicht empfohlen. NetApp hat verschiedene I/O-Workload-Merkmalstests mit gemeinsam genutzten und dedizierten Aggregaten mit getrennten Datendateien und Transaktions-Log-Dateien durchgeführt. Tests zeigen, dass ein großes Aggregat mit mehr RAID-Gruppen und -Laufwerken die Storage Performance optimiert und verbessert und Administratoren aus zwei Gründen einfacher zu managen sind:

- Ein großes Aggregat macht die I/O-Funktionen aller Laufwerke für alle Dateien verfügbar.
- Ein großes Aggregat ermöglicht die effizienteste Nutzung von Festplattenspeicher.

Platzieren Sie für Hochverfügbarkeit (HA) das sekundäre synchrone Replikat der SQL Server Always On Availability Group auf einer separaten Storage Virtual Machine (SVM) im Aggregat. Platzieren Sie zum Zweck der Disaster Recovery das asynchrone Replikat in einem Aggregat, das Teil eines separaten Storage-Clusters am DR-Standort ist, und Inhalte werden mithilfe der NetApp SnapMirror Technologie repliziert. NetApp empfiehlt eine Verfügbarkeit von mindestens 10 % freien Speicherplatz in einem Aggregat zugunsten der optimalen Storage-Performance.

## Volumes

Volumes werden erstellt und befinden sich in den Aggregaten. Dieser Begriff verursacht manchmal Verwirrung, weil ein ONTAP Volume keine LUN ist. Ein ONTAP Volume ist ein Management-Container für Daten. Ein Volume kann Dateien, LUNs oder sogar S3 Objekte enthalten. Ein Volume benötigt keinen Speicherplatz, sondern wird nur für das Management der enthaltenen Daten verwendet.

## Überlegungen zum Volume-Design

Bevor Sie ein Datenbank-Volume-Design erstellen, ist es wichtig zu wissen, wie das I/O-Muster und die Merkmale von SQL Server je nach Workload und Backup- und Recovery-Anforderungen variieren. Beachten Sie die folgenden NetApp Empfehlungen für flexible Volumes:

- Vermeiden Sie die gemeinsame Nutzung von Volumes zwischen Hosts. Beispielsweise wäre es möglich, 2 LUNs in einem einzelnen Volume zu erstellen und jede LUN mit einem anderen Host zu teilen. Dies sollte jedoch vermieden werden, da das Management dadurch komplizierter wird. Vermeiden Sie bei der Ausführung mehrerer SQL Server-Instanzen auf demselben Host, sofern Sie sich nicht nahe an der

Volume-Grenze auf einem Node befinden, die gemeinsame Nutzung von Volumes und stattdessen ein separates Volume pro Instanz pro Host zur Vereinfachung des Datenmanagements.

- Verwenden Sie NTFS-Bereitstellungspunkte anstelle von Laufwerksbuchstaben, um die Beschränkung auf 26 Laufwerksbuchstaben in Windows zu überschreiten. Bei der Verwendung von Volume-Mount-Punkten wird generell empfohlen, dem Volume-Label den gleichen Namen wie dem Mount-Punkt zu geben.
- Konfigurieren Sie bei Bedarf eine Richtlinie für die automatische Größenanpassung von Volumes, um Speicherplatzbelegung zu verhindern.
- Wenn Sie SQL Server auf einer SMB-Freigabe installieren, stellen Sie sicher, dass Unicode auf den SMB-Volumes zum Erstellen von Ordnern aktiviert ist.
- Setzen Sie den Wert der Snapshot-Reserve im Volume auf null, um die Überwachung aus betrieblicher Sicht zu vereinfachen.
- Snapshot Zeitpläne und Aufbewahrungsrichtlinien deaktivieren. Stattdessen können Sie SnapCenter verwenden, um Snapshot Kopien der SQL Server-Daten-Volumes zu koordinieren.
- Platzieren Sie die SQL Server Systemdatenbanken auf einem dedizierten Volume.
- Tempdb ist eine Systemdatenbank, die von SQL Server als temporärer Arbeitsbereich verwendet wird, insbesondere für I/O-intensive DBCC-CHECKDB-Vorgänge. Platzieren Sie diese Datenbank daher auf einem dedizierten Volume mit einem separaten Satz von Spindeln. In großen Umgebungen, in denen die Volume-Anzahl eine Herausforderung ist, können Sie tempdb in weniger Volumes konsolidieren und im gleichen Volume wie andere Systemdatenbanken nach einer sorgfältigen Planung speichern. Datenschutz für tempdb hat keine hohe Priorität, da diese Datenbank bei jedem Neustart von SQL Server neu erstellt wird.
- Legen Sie Benutzerdatendateien (.mdf) auf separaten Volumes, da es sich um zufällige Lese-/Schreib-Workloads handelt. Es ist üblich, Transaktions-Log-Backups häufiger zu erstellen als Datenbank-Backups. Legen Sie daher Transaktions-Log-Dateien (.ldf) auf ein separates Volume oder VMDK aus den Datendateien, so dass für jedes Volume unabhängige Backup-Zeitpläne erstellt werden können. Durch diese Trennung werden auch die I/O-Vorgänge bei sequenziellen Schreibvorgängen aus den I/O-Vorgängen für zufällige Lese-/Schreibzugriffe von Datendateien isoliert und die SQL Server Performance deutlich verbessert.

## LUNs

- Stellen Sie sicher, dass sich die Benutzerdatenbankdateien und das Protokollverzeichnis für das Protokoll-Backup auf separaten Volumes befinden, damit die Aufbewahrungsrichtlinie Snapshots bei Verwendung der SnapVault-Technologie nicht überschreibt.
- Mischen Sie keine Datenbank- und nicht-Datenbankdateien, wie z. B. Dateien mit Volltextsuche, auf denselben LUN.
- Wenn sekundäre Datenbankdateien (als Teil einer Dateigruppe) auf separate Volumes platziert werden, wird die Performance der SQL Server Datenbank verbessert. Diese Trennung ist nur gültig, wenn die Datei der Datenbank .mdf ihre LUN nicht mit anderen Dateien teilt .mdf.
- Wenn Sie LUNs mit DiskManager oder anderen Werkzeugen erstellen, stellen Sie sicher, dass die Größe der Zuordnungseinheit beim Formatieren der LUNs auf 64K für Partitionen festgelegt ist.
- Siehe "[Microsoft Windows und natives MPIO unter den Best Practices von ONTAP für modernes SAN](#)" So wenden Sie Multipathing-Unterstützung unter Windows auf iSCSI-Geräte in den MPIO-Eigenschaften an.

## Datenbankdateien und Dateigruppen

Die korrekte Platzierung von SQL Server-Datenbankdateien auf ONTAP ist in der ersten Implementierungsphase entscheidend. Dies sorgt für optimale Performance,

Speicherplatz-Management, Backup- und Wiederherstellungszeiten, die Ihren geschäftlichen Anforderungen entsprechend konfiguriert werden können.

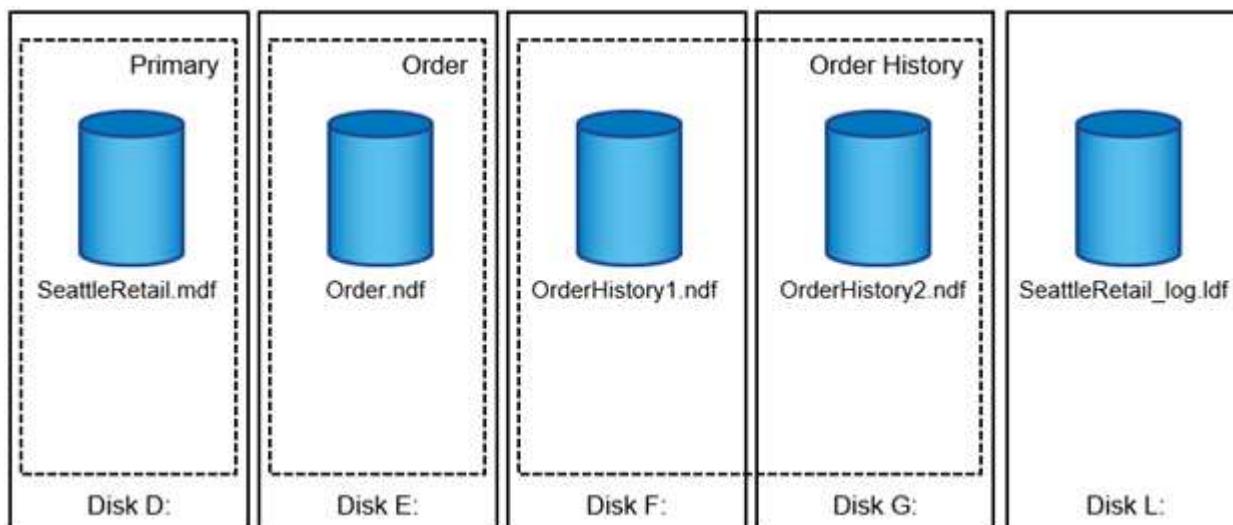
Theoretisch unterstützt SQL Server (64-Bit) 32.767 Datenbanken pro Instanz und 524.272 TB Datenbankgröße, obwohl die typische Installation normalerweise über mehrere Datenbanken verfügt. Die Anzahl der Datenbanken, die SQL Server verarbeiten kann, hängt jedoch von der Last und der Hardware ab. Es ist nicht ungewöhnlich, dass SQL Server Instanzen Dutzende, Hunderte oder sogar Tausende kleine Datenbanken hosten.

#### Datenbankdateien & Dateigruppe

Jede Datenbank besteht aus einer oder mehreren Datendateien und einer oder mehreren Transaktions-Log-Dateien. Das Transaktionsprotokoll speichert die Informationen über Datenbanktransaktionen und alle von jeder Sitzung vorgenommenen Datenänderungen. Jedes Mal, wenn die Daten geändert werden, speichert SQL Server genügend Informationen im Transaktionsprotokoll, um die Aktion rückgängig zu machen (Rollback) oder zu wiederholen (Replay). Ein SQL Server-Transaktionsprotokoll ist ein integraler Bestandteil des Rufs von SQL Server für Datenintegrität und Robustheit. Das Transaktionsprotokoll ist für die Atomizität, Konsistenz, Isolation und Strapazierfähigkeit (ACID) von SQL Server von entscheidender Bedeutung. SQL Server schreibt in das Transaktionsprotokoll, sobald eine Änderung an der Datenseite erfolgt. Jede DML-Anweisung (Data Manipulation Language) (z. B. SELECT, Insert, Update oder delete) ist eine vollständige Transaktion, und das Transaktionsprotokoll stellt sicher, dass der gesamte Set-basierte Vorgang durchgeführt wird, um die Atomizität der Transaktion sicherzustellen.

Jede Datenbank verfügt über eine primäre Datendatei, die standardmäßig über die Erweiterung .mdf verfügt. Darüber hinaus kann jede Datenbank sekundäre Datenbankdateien enthalten. Diese Dateien haben standardmäßig .ndf-Erweiterungen.

Alle Datenbankdateien werden in Dateigruppen gruppiert. Eine Dateigruppe ist die logische Einheit, die die Datenbankverwaltung vereinfacht. Sie ermöglichen die Trennung zwischen einer logischen Objektplatzierung und physischen Datenbankdateien. Wenn Sie die Tabellen für Datenbankobjekte erstellen, geben Sie an, in welcher Dateigruppe sie platziert werden sollen, ohne sich um die zugrunde liegende Datendateikonfiguration zu sorgen.



Die Fähigkeit, mehrere Datendateien innerhalb der Dateigruppe zu speichern, ermöglicht es Ihnen, die Last auf verschiedene Speichergeräte zu verteilen, wodurch die I/O-Performance des Systems verbessert wird. Der Kontrast für die Transaktionsprotokollanmeldung profitiert nicht von den mehreren Dateien, da SQL Server in sequenzieller Weise in das Transaktionsprotokoll schreibt.

Die Trennung zwischen der Platzierung logischer Objekte in den Dateigruppen und physischen Datenbankdateien ermöglicht es Ihnen, das Layout von Datenbankdateien zu optimieren und so das Storage-Subsystem optimal zu nutzen. Die Anzahl der Datendateien, die einen mitgebenden Workload unterstützen, kann nach Bedarf variiert werden, um I/O-Anforderungen und erwartete Kapazität ohne Auswirkungen auf die Applikation zu erfüllen. Diese Variationen im Datenbank-Layout sind für Anwendungsentwickler transparent, die die Datenbankobjekte in Dateigruppen statt in Datenbankdateien platzieren.

 **NetApp empfiehlt** die Verwendung der primären Dateigruppe für alles andere als Systemobjekte zu vermeiden. Das Erstellen einer separaten Dateigruppe oder einer Gruppe von Dateigruppen für die Benutzerobjekte vereinfacht die Datenbankverwaltung und Disaster Recovery, insbesondere bei großen Datenbanken.

#### Initialisierung der Datenbankinstanzdatei

Sie können die ursprüngliche Dateigröße und die automatischen Wachstumsparameter angeben, wenn Sie die Datenbank erstellen oder neue Dateien zu einer vorhandenen Datenbank hinzufügen. SQL Server verwendet einen proportionalen Füllalgorithmus bei der Auswahl der Datendatei, in die Daten geschrieben werden sollen. Es schreibt eine Datenmenge proportional zum verfügbaren freien Speicherplatz in den Dateien. Je mehr Speicherplatz in der Datei verfügbar ist, desto mehr Schreibvorgänge werden verarbeitet.

 **NetApp empfiehlt**, dass alle Dateien in der einzelnen Dateigruppe die gleiche Anfangsgröße und die gleichen Autogrowth-Parameter haben, wobei die Grow-Größe in Megabyte und nicht in Prozentsätzen definiert ist. Dies hilft dem proportionalen Füllalgorithmus, Schreibaktivitäten gleichmäßig über Datendateien hinweg auszugleichen.

Jedes Mal, wenn SQL Server Dateien vergrößert, füllt es neu zugewiesenen Speicherplatz mit Nullen. Dieser Prozess blockiert alle Sitzungen, die in die entsprechende Datei geschrieben werden müssen, oder generiert im Falle eines Wachstums des Transaktionsprotokolls Transaktionsprotokolle.

SQL Server löscht das Transaktionsprotokoll immer auf Null, und dieses Verhalten kann nicht geändert werden. Sie können jedoch festlegen, ob Datendateien auf Null gesetzt werden, indem Sie die sofortige Dateiinitialisierung aktivieren oder deaktivieren. Durch die sofortige Dateiinitialisierung wird das Wachstum von Datendateien beschleunigt und der Zeitaufwand für die Erstellung oder Wiederherstellung der Datenbank verringert.

Mit der sofortigen Dateiinitialisierung ist ein kleines Sicherheitsrisiko verbunden. Wenn diese Option aktiviert ist, können nicht zugewiesene Teile der Datendatei Informationen aus zuvor gelöschten Betriebssystemdateien enthalten. Datenbankadministratoren können solche Daten prüfen.

Sie können die sofortige Dateiinitialisierung aktivieren, indem Sie dem SQL Server-Startkonto die Berechtigung SA\_MANAGE\_VOLUME\_NAME, auch bekannt als „Perform Volume Maintenance Task“, hinzufügen. Sie können dies unter der Anwendung zur Verwaltung lokaler Sicherheitsrichtlinien (secpol.msc) tun, wie in der folgenden Abbildung dargestellt. Öffnen Sie die Eigenschaften für die Berechtigung zum Ausführen von Volume-Wartungsaufgaben und fügen Sie das SQL Server-Startkonto zur Liste der Benutzer dort hinzu.

Policy	Security Setting
Increase a process working set	Users
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators, Backup ...
Log on as a service	SEA-TM\Administrator, ...
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for ano...	Administrators
<b>Perform volume maintenance tasks</b>	<b>Administrators</b>
Profile single process	Administrators
Profile system performance	Administrators, NT SERVI...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE, NETWO...
Restore files and directories	Administrators, Backup ...
Shut down the system	Administrators, Backup ...
Synchronize directory service data	
Take ownership of files or other objects	Administrators

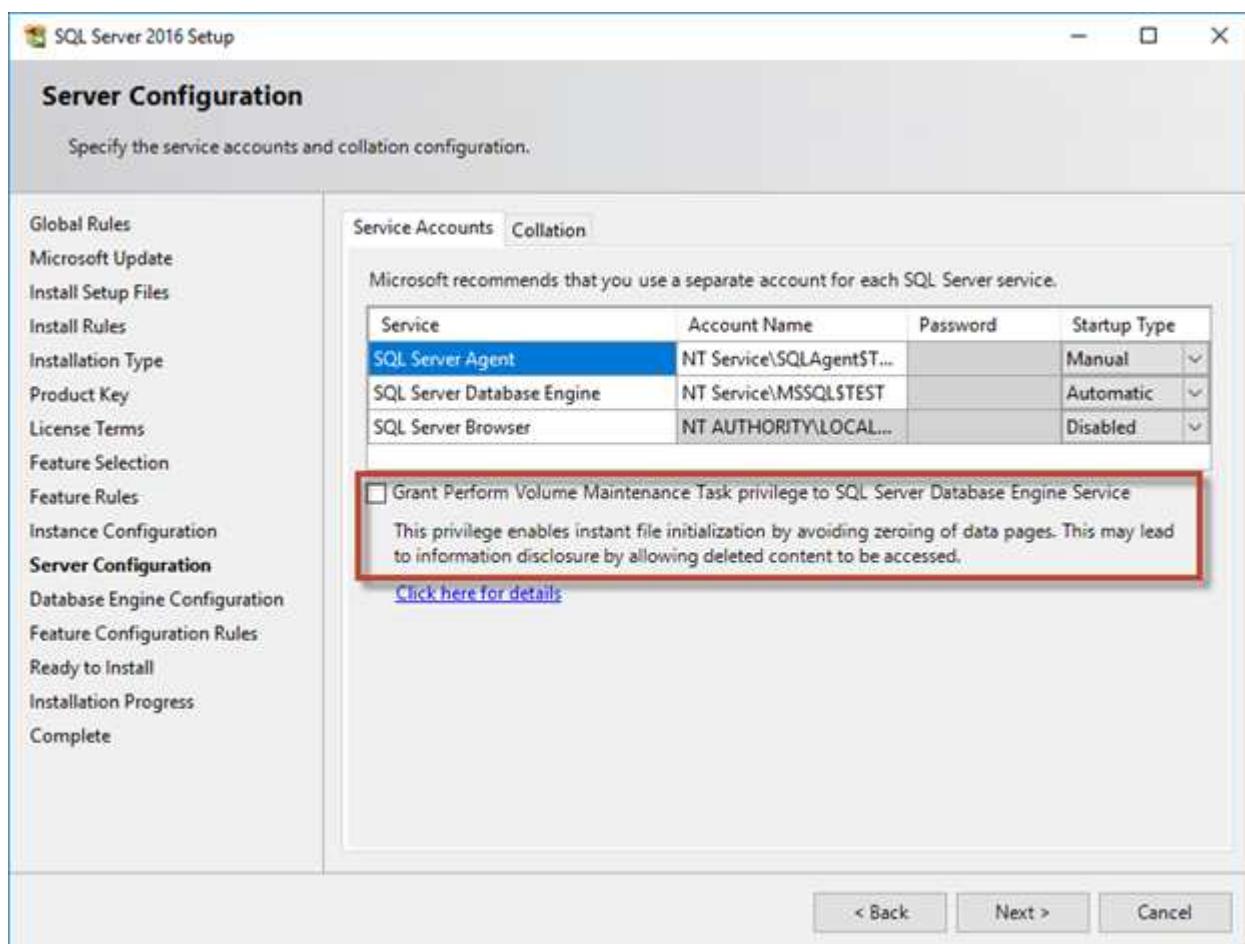
Um zu überprüfen, ob die Berechtigung aktiviert ist, können Sie den Code aus dem folgenden Beispiel verwenden. Dieser Code setzt zwei Trace-Flags, die SQL Server zwingen, zusätzliche Informationen in das Fehlerprotokoll zu schreiben, eine kleine Datenbank zu erstellen und den Inhalt des Protokolls zu lesen.

```
DBCC TRACEON(3004,3605,-1)
GO
CREATE DATABASE DelMe
GO
EXECUTE sp_readerrorlog
GO
DROP DATABASE DelMe
GO
DBCC TRACEOFF(3004,3605,-1)
GO
```

Wenn die sofortige Dateiinitialisierung nicht aktiviert ist, zeigt das SQL Server-Fehlerprotokoll an, dass SQL Server die mdf-Datendatei zusätzlich zum Nullsetzen der ldf-Protokolldatei auf Null setzt, wie im folgenden Beispiel gezeigt. Wenn die sofortige Dateiinitialisierung aktiviert ist, wird nur das Nullsetzen der Protokolldatei angezeigt.

	LogDate	ProcessInfo	Text
365	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 flush delta counts.
366	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 logging active xact info.
367	2017-02-09 08:10:07.750	spid53	Ckpt dbid 3 phase 1 ended (8)
368	2017-02-09 08:10:07.750	spid53	About to log Checkpoint end.
369	2017-02-09 08:10:07.880	spid53	Ckpt dbid 3 complete
370	2017-02-09 08:10:08.130	spid53	Starting up database 'DelMe'.
371	2017-02-09 08:10:08.150	spid53	Fixup Log Tail(progress) zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.mdf
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.mdf
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.mdf
374	2017-02-09 08:10:08.710	spid53	Ckpt dbid 6 started
375	2017-02-09 08:10:08.710	spid53	About to log Checkpoint begin.

Die Aufgabe „Volume Maintenance durchführen“ wird in SQL Server 2016 vereinfacht und später während des Installationsprozesses als Option bereitgestellt. In dieser Abbildung wird die Option angezeigt, dem SQL Server-Datenbank-Engine-Service die Berechtigung zum Ausführen der Volume-Wartungsaufgabe zu gewähren.



Eine weitere wichtige Datenbankoption, die die Größe der Datenbankdateien steuert, ist Autoshrink. Wenn diese Option aktiviert ist, verkleinert SQL Server die Datenbankdateien regelmäßig, reduziert deren Größe und gibt Speicherplatz für das Betriebssystem frei. Dieser Vorgang ist ressourcenintensiv und nur selten sinnvoll, da die Datenbankdateien nach einiger Zeit wieder wachsen, wenn neue Daten in das System gelangen. Autoshrink sollte in der Datenbank nicht aktiviert sein.

## Protokollverzeichnis

Das Protokollverzeichnis wird in SQL Server angegeben, um die Backup-Daten des Transaktionsprotokolls auf Hostebene zu speichern. Wenn Sie SnapCenter zum Sichern von Protokolldateien verwenden, muss für jeden von SnapCenter verwendeten SQL Server-Host ein Hostprotokollverzeichnis konfiguriert sein, um Protokollsicherungen durchzuführen. Bei SnapCenter gibt es ein Datenbank-Repository, sodass Metadaten, die mit Backup-, Restore- oder Klonvorgängen verbunden sind, in einem zentralen Datenbank-Repository gespeichert werden.

Die Größe des Host-Log-Verzeichnisses wird wie folgt berechnet:

$$\text{Größe des Host-Log-Verzeichnisses} = ((\text{maximale DB-LDF-Größe} \times \text{tägliche Log-Änderungsrate \%}) \times (\text{Snapshot-Aufbewahrung}) \div (1 - \text{LUN Overhead-Speicherplatz \%}))$$

Die Formel zur Größenbestimmung des Host-Protokollverzeichnisses nimmt einen LUN Overhead von 10 % an

Platzieren Sie das Protokollverzeichnis auf einem dedizierten Volume oder LUN. Die Datenmenge im Host-Log-Verzeichnis hängt von der Größe der Backups und der Anzahl der Tage ab, die Backups aufbewahrt werden. SnapCenter erlaubt nur ein Host-Protokollverzeichnis pro SQL Server-Host. Sie können die Host-Protokollverzeichnisse unter SnapCenter → Host → Configure Plug-in konfigurieren.

### NetApp empfiehlt für ein Host-Log-Verzeichnis:

- Stellen Sie sicher, dass das Host-Protokollverzeichnis nicht von anderen Datentypen gemeinsam genutzt wird, die möglicherweise die Backup-Snapshot-Daten beschädigen können.
- Platzieren Sie keine Benutzerdatenbanken oder Systemdatenbanken auf einer LUN, die Bereitstellungspunkte hostet.
- Erstellen Sie das Host-Protokollverzeichnis auf einem dedizierten Volume, auf das SnapCenter Transaktionsprotokolle kopiert.
- Migrieren Sie Datenbanken mithilfe von SnapCenter-Assistenten in NetApp Storage, damit die Datenbanken an gültigen Speicherorten gespeichert werden und so erfolgreiche SnapCenter-Backup- und -Restore-Vorgänge ermöglichen. Beachten Sie, dass der Migrationsprozess für den Fall von Unterbrechungen verantwortlich ist und dazu führen kann, dass die Datenbanken offline gehen, während die Migration durchgeführt wird.
- Die folgenden Bedingungen müssen für Failover-Cluster-Instanzen (FCIs) von SQL Server gelten:
  - Wenn Sie eine Failover-Cluster-Instanz verwenden, muss das Host-Log-Verzeichnis LUN eine Cluster-Festplattenressource in derselben Cluster-Gruppe sein wie die SQL Server-Instanz, die SnapCenter gesichert wird.
  - Wenn Sie eine Failover-Cluster-Instanz verwenden, müssen Benutzerdatenbanken auf gemeinsam genutzte LUNs platziert werden, bei denen es sich um physische Festplatten-Cluster-Ressourcen handelt, die der Cluster-Gruppe zugewiesen sind, die der SQL Server-Instanz zugeordnet ist.



## Storage-Effizienz

Die ONTAP Storage-Effizienz wurde für das Speichern und Managen von SQL Server-Daten optimiert, sodass Sie den Speicherplatz auf ein Minimum beschränken und keine Auswirkungen auf die Performance haben.

Funktionen für Platzeffizienz wie Komprimierung, Data-Compaction und Deduplizierung sind darauf ausgelegt,

die Menge der logischen Daten zu einer bestimmten Menge des physischen Storage zu erhöhen. Das Ergebnis sind niedrigere Kosten und geringerer Management-Overhead.

Auf hohem Niveau ist Komprimierung ein mathematischer Prozess, bei dem Muster in Daten erkannt und so kodiert werden, dass der Platzbedarf reduziert wird. Dagegen erkennt die Deduplizierung tatsächlich wiederholte Datenblöcke und entfernt die fremden Kopien. Durch Data-Compaction können mehrere logische Datenblöcke denselben physischen Block auf den Medien gemeinsam nutzen.



In den nachfolgenden Abschnitten zu Thin Provisioning finden Sie eine Erläuterung des Wechselspiels zwischen Storage-Effizienz und fraktionaler Reservierung.

## Komprimierung

Vor der Verfügbarkeit von All-Flash-Storage-Systemen war die Array-basierte Komprimierung nur eingeschränkt verfügbar, da die meisten I/O-intensiven Workloads eine sehr große Anzahl von Spindeln erforderten, um eine akzeptable Performance zu erreichen. Als Nebeneffekt der großen Anzahl von Laufwerken enthielten Storage-Systeme grundsätzlich viel mehr Kapazität als erforderlich. Mit dem Trend hin zu Solid-State-Storage hat sich die Situation verändert. Eine enorme Überprovisionierung von Laufwerken entfällt, nur weil eine gute Performance erzielt werden kann. Der Speicherplatz in einem Storage-System kann den tatsächlichen Kapazitätsanforderungen angepasst werden.

Die gesteigerte IOPS-Fähigkeit von Solid-State-Laufwerken (SSDs) bringt im Vergleich zu rotierenden Laufwerken fast immer Kosteneinsparungen mit sich. Allerdings kann die Komprimierung durch eine höhere effektive Kapazität von Solid-State-Medien weitere Einsparungen erzielen.

Es gibt verschiedene Möglichkeiten, Daten zu komprimieren. Viele Datenbanken verfügen über eigene Komprimierungsfunktionen, dies wird jedoch in Kundenumgebungen selten beobachtet. Der Grund dafür ist in der Regel die Performance-Einbußen bei einem **Wechsel** zu komprimierten Daten. Bei einigen Anwendungen fallen zudem hohe Lizenzierungskosten für die Komprimierung auf Datenbankebene an. Und schließlich gibt es noch die allgemeinen Performance-Auswirkungen auf die Datenbankvorgänge. Es macht wenig Sinn, für eine CPU, die Datenkomprimierung und -Dekomprimierung durchführt, hohe Lizenzkosten pro CPU zu zahlen, anstatt eine echte Datenbankarbeit zu erledigen. Eine bessere Option ist, die Komprimierungsarbeiten auf das Storage-System zu verlagern.

## Anpassungsfähige Komprimierung

Die adaptive Komprimierung wurde vollständig mit Enterprise-Workloads getestet, ohne dabei die Performance zu beeinträchtigen – selbst in einer All-Flash-Umgebung, in der die Latenz im Mikrosekunden-Bereich gemessen wird. Einige Kunden haben bei Verwendung der Komprimierung sogar eine Performance-Steigerung festgestellt, da die Daten im Cache komprimiert bleiben. Dadurch konnte die Menge des verfügbaren Cache in einem Controller erhöht werden.

ONTAP managt physische Blöcke in 4-KB-Einheiten. Die anpassungsfähige Komprimierung verwendet eine Standardkomprimierung von 8 KB. Dies bedeutet, dass Daten in 8-KB-Einheiten komprimiert werden. Dies entspricht der 8-KB-Blockgröße, die von relationalen Datenbanken am häufigsten verwendet wird. Kompressionsalgorithmen werden effizienter, da mehr Daten als eine Einheit komprimiert werden. Eine Komprimierungs-Blockgröße von 32 KB wäre spechereffizienter als eine Komprimierungsblockeinheit mit 8 KB. Das bedeutet, dass die adaptive Komprimierung bei Verwendung der standardmäßigen 8-KB-Blockgröße zu etwas niedrigeren Effizienzraten führt, jedoch bietet die Verwendung kleinerer Blockgrößen zur Komprimierung auch einen signifikanten Vorteil. Datenbank-Workloads umfassen einen großen Anteil an Überschreibungsaktivitäten. Beim Überschreiben eines komprimierten 32-KB-Datenblocks müssen die gesamten 32-KB-Daten zurückgelesen, dekomprimiert, der erforderliche 8-KB-Bereich aktualisiert, neu komprimiert und dann die gesamten 32-KB-Daten wieder auf die Laufwerke geschrieben werden. Dies ist für ein Storage-System ein sehr teurer Vorgang und der Grund dafür, dass bei einigen Storage Arrays anderer

Anbieter, die auf größeren Komprimierungsblockgrößen basieren, auch die Performance bei Datenbank-Workloads erheblich beeinträchtigt wird.



Die von der anpassungsfähigen Komprimierung verwendete Blockgröße kann auf bis zu 32 KB gesteigert werden. Dies kann die Speichereffizienz verbessern und sollte bei stillgelegten Dateien wie Transaktionsprotokollen und Backup-Dateien in Betracht gezogen werden, wenn eine große Menge solcher Daten auf dem Array gespeichert wird. In manchen Situationen profitieren aktive Datenbanken mit 16-KB- oder 32-KB-Blockgröße möglicherweise auch von der Erhöhung der Blockgröße der anpassungsfähigen Komprimierung. Wenden Sie sich an einen Mitarbeiter von NetApp oder einen unserer Partner, um Rat zu erhalten, ob diese Lösung für Ihren Workload geeignet ist.



Blockgrößen der Komprimierung von mehr als 8 KB sollten nicht zusammen mit der Deduplizierung an Streaming-Backup-Zielen verwendet werden. Der Grund dafür ist, dass kleine Änderungen an den gesicherten Daten das 32-KB-Komprimierungsfenster beeinflussen. Wenn sich das Fenster verschiebt, unterscheiden sich die resultierenden komprimierten Daten in der gesamten Datei. Die Deduplizierung erfolgt nach der Komprimierung. Das heißt, die Deduplizierungs-Engine sieht jedes komprimierte Backup unterschiedlich. Wenn eine Deduplizierung von Streaming-Backups erforderlich ist, sollte nur eine blockadaptive Komprimierung von 8 KB verwendet werden. Die adaptive Komprimierung ist vorzuziehen, da sie bei kleineren Blöcken arbeitet und die Deduplizierungseffizienz nicht stört. Aus ähnlichen Gründen wirkt sich die Host-seitige Komprimierung auch in die Effizienz der Deduplizierung aus.

### Kompressionsausrichtung

Die anpassungsfähige Komprimierung in einer Datenbankumgebung erfordert bestimmte Überlegungen zur Blockausrichtung der Komprimierung. Dies ist nur für Daten relevant, die Random Überschreibungen sehr spezifischer Blöcke unterliegen. Dieser Ansatz ähnelt im Konzept der gesamten Filesystem-Ausrichtung, wobei der Beginn eines Dateisystems an einer Grenze von 4K-Geräten ausgerichtet werden muss und die Blockgröße eines Dateisystems ein Vielfaches von 4K sein muss.

Ein Schreibvorgang von 8 KB in eine Datei wird beispielsweise nur komprimiert, wenn er an einer 8-KB-Grenze innerhalb des Dateisystems selbst ausgerichtet ist. Dieser Punkt bedeutet, dass er auf die ersten 8 KB der Datei, die zweiten 8 KB der Datei usw. fallen muss. Der einfachste Weg, um eine korrekte Ausrichtung zu gewährleisten, ist die Verwendung des korrekten LUN-Typs. Jede erstellte Partition sollte einen Offset vom Anfang des Geräts an haben, der ein Vielfaches von 8K ist, und eine Dateisystem-Blockgröße verwenden, die ein Vielfaches der Datenbank-Blockgröße ist.

Daten wie Backups oder Transaktions-Logs werden sequenziell geschrieben und umfassen mehrere Blöcke. Alle Blöcke werden komprimiert. Daher besteht keine Notwendigkeit, eine Ausrichtung zu erwägen. Das einzige I/O-Muster, das Bedenken aushinsichtlich des zufälligen Überschreibens von Dateien hat, ist das zufällige Überschreiben von Dateien.

### Data-Compaction

Data-Compaction ist eine Technologie, die die Komprimierungseffizienz verbessert. Wie bereits erwähnt, erzielt die anpassungsfähige Komprimierung allein schon Einsparungen von 2:1, da sie auf das Speichern eines 8-KB-I/O-Blocks in einem 4-KB-WAFL-Block beschränkt ist. Komprimierungsmethoden mit größeren Blockgrößen verbessern die Effizienz. Sie sind jedoch nicht für Daten geeignet, die mit Überschreibungen kleiner Blöcke verbunden sind. Die Dekomprimierung von 32-KB-Dateneinheiten durch die Aktualisierung eines 8-KB-Abschnitts, die Datenkomprimierung und das Zurückschreiben auf die Laufwerke verursacht Overhead.

Data-Compaction sorgt dafür, dass mehrere logische Blöcke innerhalb physischer Blöcke gespeichert werden

können. Beispielsweise kann eine Datenbank mit stark komprimierbaren Daten wie Text oder teilweise vollständigen Blöcken von 8 KB bis 1 KB komprimieren. Ohne Data-Compaction belegen diese 1 KB Daten immer noch einen gesamten 4-KB-Block. Durch die Inline-Data-Compaction können 1 KB komprimierte Daten zusammen mit anderen komprimierten Daten auf nur 1 KB physischen Speicherplatz gespeichert werden. Es handelt sich nicht um eine Komprimierungstechnologie. Es ist einfach eine effizientere Möglichkeit, Speicherplatz auf den Laufwerken zuzuweisen und sollte daher keine erkennbaren Performance-Auswirkungen verursachen.

Der Grad der erzielten Einsparungen variiert. Bereits komprimierte oder verschlüsselte Daten können in der Regel nicht weiter komprimiert werden. Daher profitieren diese Datensätze von der Data-Compaction nicht. Im Gegensatz dazu werden neu initialisierte Datendateien, die nur wenig mehr als Block-Metadaten und Nullen enthalten, mit bis zu 80 komprimiert.

### **Temperaturempfindliche Speichereffizienz**

Temperaturempfindliche Speichereffizienz (TSSE) ist ab ONTAP 9.8 verfügbar. Es basiert auf Block-Zugriffs-Heatmaps, um selten genutzte Blöcke zu identifizieren und sie effizienter zu komprimieren.

### **Deduplikierung**

Deduplikierung ist die Entfernung von Blockduplicaten aus einem Datensatz. Wenn beispielsweise derselbe 4-KB-Block in 10 verschiedenen Dateien vorhanden war, leitet die Deduplikierung diesen 4-KB-Block innerhalb aller 10 Dateien auf denselben physischen 4-KB-Block um. Im Ergebnis würde sich die Effizienz dieser Daten um 10:1 verbessern.

Daten wie Boot-LUNs von VMware lassen sich in der Regel sehr gut deduplizieren, da sie aus mehreren Kopien derselben Betriebssystemdateien bestehen. Es wurde eine Effizienz von 100:1 und höher festgestellt.

Einige Daten enthalten keine Datenduplikate. Ein Oracle-Block enthält beispielsweise einen Header, der global nur für die Datenbank gilt, und einen Trailer, der fast einzigartig ist. Aus diesem Grund führt die Deduplikierung einer Oracle Database selten zu Einsparungen von mehr als 1 %. Die Deduplikierung mit MS SQL Datenbanken ist etwas besser, aber eindeutige Metadaten auf Blockebene stellen immer noch eine Einschränkung dar.

In einigen Fällen wurde eine Speicherersparnis von bis zu 15 % bei Datenbanken mit 16 KB und großen Blockgrößen beobachtet. Die ersten 4-KB-Blöcke enthalten die global eindeutige Kopfzeile, und der letzte 4-KB-Block enthält den nahezu einzigartigen Trailer. Die internen Blöcke eignen sich für eine Deduplikierung, obwohl dies in der Praxis fast vollständig der Deduplikierung von gelöschten Daten zugeordnet ist.

Viele Arrays anderer Anbieter behaupten, Datenbanken unter der Annahme zu deduplizieren, dass eine Datenbank mehrfach kopiert wird. In dieser Hinsicht kann auch NetApp Deduplikierung eingesetzt werden, allerdings bietet ONTAP die bessere Option: NetApp FlexClone Technologie. Das Endergebnis ist das gleiche. Es werden mehrere Kopien einer Datenbank erstellt, die die meisten zugrunde liegenden physischen Blöcke nutzen. Ein Einsatz von FlexClone ist wesentlich effizienter, als Datenbankdateien zu kopieren und anschließend zu deduplizieren. Der Effekt ist die Nichtdeduplikierung und nicht die Deduplikierung, da ein Duplikat von vornirgends erstellt wird.

### **Effizienz und Thin Provisioning**

Effizienzfunktionen sind Formen von Thin Provisioning. Beispielsweise kann eine 100-GB-LUN, die ein 100-GB-Volume belegt, bis zu 50 GB komprimiert werden. Es wurden noch keine tatsächlichen Einsparungen realisiert, da das Volume noch 100 GB beträgt. Das Volume muss zunächst verkleinert werden, damit der eingesparte Speicherplatz an anderer Stelle im System genutzt werden kann. Wenn spätere Änderungen an der 100GB-LUN dazu führen, dass die Daten weniger komprimierbar werden, dann vergrößert sich die LUN und das Volume könnte sich füllen.

Thin Provisioning wird nachdrücklich empfohlen, da es das Management vereinfachen und gleichzeitig eine deutliche Verbesserung der nutzbaren Kapazität mit den damit verbundenen Kosteneinsparungen ermöglichen kann. Der Grund hierfür ist einfach: Datenbankumgebungen enthalten oft viel leeren Speicherplatz, eine große Anzahl an Volumes und LUNs sowie komprimierbare Daten. Durch Thick Provisioning wird Speicherplatz auf Storage für Volumes und LUNs reserviert, für den Fall, dass sie eines Tages zu 100 % voll werden und 100 % nicht komprimierbare Daten enthalten. Das wird wohl nie passieren. Dank Thin Provisioning kann dieser Speicherplatz zurückgewonnen und an anderer Stelle verwendet werden. Das Kapazitätsmanagement kann auf dem Storage-System selbst basieren, anstatt auf vielen kleineren Volumes und LUNs.

Einige Kunden bevorzugen Thick Provisioning entweder für bestimmte Workloads oder generell basierend auf bestehenden Betriebs- und Beschaffungsmethoden.

 Bei einem Volume mit Thick Provisioning müssen unbedingt alle Effizienzfunktionen des Volumes deaktiviert werden, einschließlich der Dekomprimierung und der Entfernung der Deduplizierung mit dem `sis undo` Befehl. Die Lautstärke sollte nicht in der Ausgabe angezeigt `volume efficiency show` werden. Ist dies der Fall, ist das Volume für Effizienzfunktionen noch teilweise konfiguriert. Daher funktionieren Überschreibungsgarantien anders. Dies erhöht die Wahrscheinlichkeit, dass Konfigurationsübersehungen dazu führen, dass das Volume unerwartet aus dem Speicherplatz kommt und zu Datenbank-I/O-Fehlern führt.

## Best Practices für Effizienz

**NetApp empfiehlt** Folgendes:

### AFF-Standards

Volumes, die auf ONTAP erstellt wurden und auf einem rein Flash-basierten AFF System ausgeführt werden, werden über Thin Provisioning mit allen Inline-Effizienzfunktionen bereitgestellt. Obwohl Datenbanken im Allgemeinen nicht von der Deduplizierung profitieren und nicht komprimierbare Daten enthalten können, sind die Standardeinstellungen dennoch für fast alle Workloads geeignet. ONTAP wurde mit dem Ziel entwickelt, alle Arten von Daten und I/O-Muster effizient zu verarbeiten. Dabei spielt es keine Rolle, ob es zu Einsparungen kommt oder nicht. Standardwerte sollten nur dann geändert werden, wenn die Gründe vollständig verstanden sind und es einen Vorteil gibt, dass sie abweichen.

### Allgemeine Empfehlungen

- Wenn Volumes und/oder LUNs nicht über Thin Provisioning bereitgestellt werden, müssen Sie alle Effizienzeinstellungen deaktivieren, da die Verwendung dieser Funktionen keine Einsparungen bietet. Die Kombination von Thick Provisioning mit aktiverter Speicherplatzeffizienz kann zu unerwartetem Verhalten führen, einschließlich Fehlern aufgrund von Speicherplatzout.
- Wenn Daten nicht überschrieben werden, wie etwa bei Backups oder Datenbanktransaktionsprotokollen, können Sie die Effizienz steigern, indem Sie TSSE mit einem niedrigen Kühlzeitraum aktivieren.
- Einige Dateien enthalten möglicherweise eine beträchtliche Menge an nicht komprimierbaren Daten. Ein Beispiel: Wenn die Komprimierung bereits auf Applikationsebene aktiviert ist, werden Dateien verschlüsselt. Wenn eines dieser Szenarien zutrifft, sollten Sie die Komprimierung deaktivieren, um einen effizienteren Betrieb auf anderen Volumes mit komprimierbaren Daten zu ermöglichen.
- Verwenden Sie für Datenbank-Backups nicht sowohl die 32-KB-Komprimierung als auch die Deduplizierung. Siehe Abschnitt [Anpassungsfähige Komprimierung](#) Entsprechende Details.

### Datenbankkomprimierung

SQL Server selbst verfügt auch über Funktionen zur Komprimierung und zum effizienten Management von Daten. SQL Server unterstützt derzeit zwei Arten der Datenkomprimierung: Row Compression und Page

## Compression.

Durch die Zeilenkomprimierung wird das Datenspeicherformat geändert. So werden beispielsweise ganze Zahlen und Dezimalzahlen anstelle des nativen Formats mit fester Länge in das Format mit variabler Länge geändert. Außerdem werden Zeichenketten mit fester Länge durch das Entfernen von Leerzeichen in das Format mit variabler Länge geändert. Die Seitenkomprimierung implementiert die Zeilenkomprimierung und zwei weitere Komprimierungsstrategien (Prefix-Komprimierung und Wörterbuchkomprimierung). Weitere Details zur Seitenkomprimierung finden Sie unter "["Implementierung Der Seitenkomprimierung"](#)".

Die Datenkomprimierung wird derzeit in den Enterprise-, Developer- und Evaluation-Editionen von SQL Server 2008 und höher unterstützt. Obwohl die Komprimierung von der Datenbank selbst durchgeführt werden kann, ist dies in einer SQL Server Umgebung nur selten der Fall.

Hier sind die Empfehlungen für die Verwaltung von Speicherplatz für SQL Server-Datendateien

- Verwenden Sie Thin Provisioning in SQL Server-Umgebungen, um die Speicherplatzauslastung zu verbessern und bei Einsatz der Speicherplatzgarantiefunktion den gesamten Storage-Bedarf zu senken.
  - Verwenden Sie Autogrow für die meisten gängigen Implementierungskonfigurationen, da der Storage-Administrator nur die Speicherplatznutzung im Aggregat überwachen muss.
- Aktivieren Sie die Deduplizierung auf keinen Volumes auf FAS mit SQL Server-Datendateien, es sei denn, das Volume ist bekannt, dass es mehrere Kopien derselben Daten enthält, wie beispielsweise die Wiederherstellung von Datenbanken aus Backups auf einem einzelnen Volume.

## Speicherplatzrückgewinnung

Die Rückgewinnung von ungenutztem Speicherplatz in einer LUN kann regelmäßig gestartet werden. Bei SnapCenter können Sie den folgenden PowerShell Befehl verwenden, um die Rückgewinnung von ungenutztem Speicherplatz zu starten.

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

Wenn Sie die Speicherplatzrückgewinnung durchführen müssen, sollte dieser Prozess in Zeiten geringer Aktivität ausgeführt werden, da er anfangs Hostzyklen beansprucht.

## Datensicherung

Strategien für Datenbank-Backups sollten auf den ermittelte geschäftliche Anforderungen basieren, nicht auf theoretischen Möglichkeiten. Durch die Kombination der Snapshot Technologie von ONTAP und der Nutzung der Microsoft SQL Server APIs können Sie schnell applikationskonsistente Backups unabhängig von der Größe der Benutzerdatenbanken erstellen. Für erweiterte oder horizontal skalierbare Datenmanagement-Anforderungen bietet NetApp SnapCenter.

## SnapCenter

SnapCenter ist die NetApp Datensicherungssoftware für Enterprise-Applikationen. Mit dem SnapCenter Plug-in für SQL Server und den vom SnapCenter Plug-in für Microsoft Windows verwalteten Betriebssystemvorgängen können SQL Server Datenbanken schnell und einfach gesichert werden.

Bei der SQL Server-Instanz kann es sich um eine eigenständige Einrichtung oder eine Failover-Cluster-Instanz handeln oder um eine Always-On-Verfügbarkeitsgruppe. Im Ergebnis können Datenbanken über eine zentrale

Konsole geschützt, geklont und aus der primären oder sekundären Kopie wiederhergestellt werden. Mit SnapCenter lassen sich SQL Server Datenbanken sowohl vor Ort, in der Cloud als auch in hybriden Konfigurationen managen. Datenbankkopien können für Entwicklungszwecke oder für Berichte in wenigen Minuten auf dem ursprünglichen oder alternativen Host erstellt werden.

SQL Server erfordert außerdem eine Koordination zwischen OS und Storage, um sicherzustellen, dass bei der Erstellung die korrekten Daten in Snapshots vorhanden sind. In den meisten Fällen ist die einzige sichere Methode, dies mit SnapCenter oder T-SQL zu tun. Ohne diese zusätzliche Koordination erstellte Snapshots sind unter Umständen nicht zuverlässig wiederherstellbar.

Weitere Informationen zum SQL Server-Plug-in für SnapCenter finden Sie unter "["TR-4714: Best Practice Guide für SQL Server mit NetApp SnapCenter"](#)".

### Datenbanken mit T-SQL -Snapshots werden gesichert

In SQL Server 2022 hat Microsoft T-SQL Snapshots eingeführt, die einen Pfad zu Skripting und Automatisierung von Backup-Vorgängen bieten. Anstatt Kopien in voller Größe zu erstellen, können Sie die Datenbank für Snapshots vorbereiten. Sobald die Datenbank für das Backup bereit ist, können Sie Snapshots mithilfe der ONTAP REST-APIs erstellen.

Im Folgenden finden Sie ein Beispiel für einen Backup-Workflow:

1. Eine Datenbank mit dem Befehl ALTER fixieren. Dadurch wird die Datenbank auf einen konsistenten Snapshot auf dem zugrunde liegenden Speicher vorbereitet. Nach dem Einfrieren können Sie die Datenbank auftauen und den Snapshot mit dem BACKUP-Befehl aufzeichnen.
2. Führen Sie Snapshots mehrerer Datenbanken auf den Speichervolumes gleichzeitig mit den neuen Befehlen BACKUP-GRUPPE und BACKUP-SERVER durch.
3. Führen Sie VOLLSTÄNDIGE Backups oder COPY\_ONLY VOLLSTÄNDIGE Backups durch. Diese Backups werden auch in msdb aufgezeichnet.
4. Durchführung einer zeitpunktgenauen Recovery mithilfe von Protokoll-Backups, die mit dem normalen Streaming-Ansatz nach dem VOLLSTÄNDIGEN Snapshot-Backup erstellt wurden. Streaming Differential Backups werden auf Wunsch auch unterstützt.

Weitere Informationen finden Sie unter "["Microsoft-Dokumentation zu den T-SQL-Snapshots"](#)".



**NetApp empfiehlt** SnapCenter zum Erstellen von Snapshot Kopien zu verwenden. Die oben beschriebene T-SQL-Methode funktioniert ebenfalls, SnapCenter bietet jedoch eine vollständige Automatisierung für Backup-, Restore- und Klonprozesse. Außerdem wird eine Erkennung durchgeführt, um sicherzustellen, dass die richtigen Snapshots erstellt werden. Es ist keine Vorkonfiguration erforderlich.

### SQL Server-Verfügbarkeitsgruppe mit SnapCenter

SnapCenter unterstützt das Backup der SQL Server Verfügbarkeitsgruppen-Datenbank, die mit Windows Failover Cluster konfiguriert ist.

Das SnapCenter Plug-in für Microsoft SQL Server muss auf allen Knoten des Windows Server Failover Clusters installiert sein. Lesen Sie die Informationen unter "["Dokumentation"](#)" Voraussetzungen und die Schritte zum Einrichten der SnapCenter-Plug-ins.

SnapCenter erkennt alle Datenbanken, Instanzen und Verfügbarkeitsgruppen in Windows-Hosts und Ressourcen werden auf der SnapCenter-Ressourcen-Seite aufgelistet.

## Sicherung von Datenbanken in der Always-on-Verfügbarkeitsgruppe

Datenbanken in Verfügbarkeitsgruppen können auf verschiedene Weise gesichert werden.

- Backup auf Datenbankebene: Wählen Sie die Verfügbarkeitsdatenbank für die Seite der Datenbankressource aus, fügen Sie die Policy hinzu, die aus vollständigen/protokollierten Backups besteht, und planen Sie die Sicherung. SnapCenter übernimmt das Backup unabhängig von der Datenbankrolle, ob es sich um ein primäres oder ein sekundäres Replikat handelt. Der Schutz kann auch durch Hinzufügen von Datenbanken zur Ressourcengruppe konfiguriert werden.
- Backup auf Instanzebene: Wählen Sie die Instanz aus, und alle auf der Instanz ausgeführten Datenbanken werden basierend auf der ausgewählten Richtlinie geschützt. Alle Datenbanken, einschließlich der Verfügbarkeitsdatenbank, die als primäres oder sekundäres Replikat ausgeführt wird, werden mithilfe von SnapCenter gesichert. Der Schutz kann auch konfiguriert werden, indem der Ressourcengruppe eine Instanz hinzugefügt wird.
- Backup auf Verfügbarkeitsgruppenebene: Bei der Konfiguration der Richtlinie bietet SnapCenter eine erweiterte Option für Backups auf Verfügbarkeitsgruppenebene. Mit der Verfügbarkeitsgruppeneinstellung in Policy können Benutzer die Replikatpräferenz für das Backup auswählen. Sie können entweder ein primäres, ein sekundäres Replikat oder alle Replikate auswählen. Die Standardoption basiert auf dem Backup-Replikat, das in der Konfiguration der SQL Server-Verfügbarkeitsgruppe festgelegt wurde.

Die Einstellung für Verfügbarkeitsgruppen in der SnapCenter-Richtlinie gilt nur, wenn Backups auf Verfügbarkeitsgruppenebene zum Schutz von Datenbanken von Verfügbarkeitsgruppen verwendet werden und nicht für Backups auf Datenbank- oder Instanzebene gelten.



**NetApp empfiehlt**, das Backup auf Verfügbarkeitsebene für alle Replikate zu verwenden, die auf NetApp ONTAP Storage ausgeführt werden.

## Konfigurieren von Protokollsicherungen in SnapCenter

Wenn die Verfügbarkeitsgruppe auf einem eigenständigen SQL Server-Setup eingerichtet wird, muss auf jedem Knoten eines Windows Server Failover-Clusters eine dedizierte Festplatte gemountet werden. Zur Konfiguration des Protokollverzeichnisses zum Speichern von Transaktionsprotokollsicherungen sollte ein dedizierter Datenträger verwendet werden.

Wenn die Verfügbarkeitsgruppe auf dem SQL Server Failover Cluster eingerichtet ist, sollte die Clusterfestplatte auf der SQL Server Failover Cluster-Instanz zum Hostprotokollverzeichnis erstellt werden.

## Wiederherstellen der Datenbank in der Verfügbarkeitsgruppen-Einrichtung mit SnapCenter

- SnapCenter bietet die Option für erneutes Seeding, um die Datenbank automatisch von dem letzten Snapshot wiederherzustellen, der auf dem sekundären Replikat verfügbar ist. Der Vorgang für erneutes Seeding wird automatisch wiederhergestellt und wird dem Datenbank-Backup in die Verfügbarkeitsgruppe hinzugefügt.
- Alternativ können Sie die Replikatdatenbank in der Verfügbarkeitsgruppe wiederherstellen, indem Sie die Verfügbarkeitsgruppe unterbrechen und die vollständige vollständige vollständige Wiederherstellung und Protokollwiederherstellung durchführen. Verwenden Sie SnapCenter, um die Datenbank im norecovery-Modus wiederherzustellen, und verwenden Sie dann SQL Server Management Studio oder T-SQL, um der Datenbank wieder zur Verfügbarkeitsgruppe beizutreten.
- Für die Wiederherstellung nur eines Teilbereichs von Daten kann die Klonfunktion von SnapCenter verwendet werden, um eine Klonkopie der Datenbank zu erstellen. Die Datenbankkopie wird innerhalb weniger Minuten mit SnapCenter erstellt und anschließend mit den nativen SQL Server Tools in das primäre Replikat exportiert.

Die Best Practice zum Einrichten des Datenbank-Storage-Layouts, um die RTO- und RPO-Anforderungen zu erfüllen, finden Sie unter "["TR-4714 Best Practices für Microsoft SQL Server mit NetApp SnapCenter"](#)".



SnapCenter unterstützt keine verteilte Verfügbarkeitsgruppe und enthaltene Verfügbarkeitsgruppe.

## Disaster Recovery

### Disaster Recovery

Enterprise-Datenbanken und Applikationsinfrastrukturen erfordern oft Replizierung zum Schutz vor Naturkatastrophen oder unerwarteten Geschäftsunterbrechungen mit minimaler Ausfallzeit.

Die SQL Server Funktion zur Replizierung von Always-on-Verfügbarkeitsgruppen kann sich als hervorragende Option anbieten. NetApp bietet Optionen zur Integration von Datensicherung mit Always-on. In einigen Fällen empfiehlt es sich jedoch, die ONTAP Replizierungstechnologie in Betracht zu ziehen. Es gibt drei grundlegende Optionen.

#### SnapMirror

Die SnapMirror-Technologie bietet eine schnelle und flexible Unternehmenslösung zur Replizierung von Daten über LANs und WANs. Die SnapMirror Technologie überträgt nach Erstellung der ersten Spiegelung nur geänderte Datenblöcke an das Zielsystem, wodurch die Anforderungen an die Netzwerkbandbreite erheblich gesenkt werden. Sie kann im synchronen oder asynchronen Modus konfiguriert werden.

#### NetApp MetroCluster und SnapMirror Active Sync

Für viele Kunden benötigt DR mehr als nur einen Remote-Besitz von Daten, sondern muss in der Lage sein, diese Daten schnell zu nutzen. NetApp bietet zwei Technologien zur Erfüllung dieser Anforderungen: MetroCluster und SnapMirror Active Sync

MetroCluster bezieht sich auf ONTAP in einer Hardwarekonfiguration mit synchron gespiegelten Storage auf niedriger Ebene und zahlreichen zusätzlichen Funktionen. Integrierte Lösungen wie MetroCluster vereinfachen die heutigen komplizierten, horizontal skalierbaren Datenbanken, Applikationen und Virtualisierungsinfrastrukturen. Sie ersetzt mehrere externe Datensicherungsprodukte und -Strategien durch ein einfaches, zentrales Storage-Array. Sie bietet außerdem integriertes Backup, Recovery, Disaster Recovery und Hochverfügbarkeit (HA) in einem einzigen geclusterten Storage-System.

Die aktive SnapMirror Synchronisierung basiert auf SnapMirror Synchronous. Mit MetroCluster ist jeder ONTAP Controller für die Replizierung seiner Laufwerksdaten an einen Remote-Standort verantwortlich. Bei SnapMirror Active Sync haben Sie im Grunde zwei verschiedene ONTAP-Systeme, die unabhängige Kopien Ihrer LUN-Daten führen, aber zusammenarbeiten, um eine einzige Instanz dieser LUN zu präsentieren. Auf Host-Ebene handelt es sich um eine einzelne LUN-Einheit.

#### Vergleich von SM-AS und MCC

SM-AS und MetroCluster sind in der Gesamtfunktionalität ähnlich, es gibt jedoch wichtige Unterschiede in der Art und Weise, wie die RPO=0-Replikation implementiert und gemanagt wird. Die asynchronen und synchronen SnapMirror können auch im Rahmen eines DR-Plans eingesetzt werden, sind aber nicht als Technologien für die HA-Replizierung konzipiert.

- Eine MetroCluster-Konfiguration ähnelt eher einem integrierten Cluster mit über mehrere Standorte

verteilten Nodes. SM-AS verhält sich wie zwei ansonsten unabhängige Cluster, die zusammenarbeiten, um ausgewählte RPO=0 synchron replizierte LUNs bereitzustellen.

- Die Daten in einer MetroCluster-Konfiguration sind zu einem bestimmten Zeitpunkt nur von einem bestimmten Standort aus zugänglich. Eine zweite Kopie der Daten befindet sich am gegenüberliegenden Standort, die Daten sind jedoch passiv. Ohne Failover des Speichersystems ist der Zugriff nicht möglich.
- MetroCluster und SM-As führen die Spiegelung auf verschiedenen Ebenen durch. Die MetroCluster Spiegelung wird auf der RAID-Schicht durchgeführt. Die Low-Level-Daten werden mithilfe von SyncMirror in einem gespiegelten Format gespeichert. Die Verwendung der Spiegelung ist in den LUN-, Volume- und Protokollebenen praktisch unsichtbar.
- Im Gegensatz dazu erfolgt die SM-AS-Spiegelung auf der Protokollebene. Die beiden Cluster sind insgesamt unabhängige Cluster. Sobald die beiden Datenkopien synchron sind, müssen die beiden Cluster nur noch Schreibvorgänge spiegeln. Wenn ein Schreibvorgang auf einem Cluster stattfindet, wird er in das andere Cluster repliziert. Der Schreibvorgang wird dem Host nur dann bestätigt, wenn der Schreibvorgang auf beiden Seiten abgeschlossen ist. Anders als dieses Verhalten bei der Protokollaufteilung sind die beiden Cluster ansonsten normale ONTAP-Cluster.
- Die Hauptrolle bei MetroCluster ist die umfangreiche Replizierung. Sie können ein gesamtes Array mit RPO=0 und RTO von nahezu null replizieren. Dies vereinfacht den Failover-Prozess, da es nur eine „Sache“ für Failover gibt und lässt sich hinsichtlich Kapazität und IOPS extrem gut skalieren.
- Ein wichtiger Anwendungsfall für SM-AS ist die granulare Replizierung. Manchmal möchten Sie nicht alle Daten als eine Einheit replizieren oder bestimmte Workloads selektiv ausfallsicher durchführen.
- Ein weiterer wichtiger Anwendungsfall für SM-As ist der aktiv/aktiv-Betrieb. Dort sollen vollständig nutzbare Datenkopien auf zwei verschiedenen Clustern verfügbar sein, die sich an zwei verschiedenen Standorten mit identischen Performance-Merkmalen befinden und auf Wunsch nicht über Standorte verteilt werden müssen. Sie können Ihre Applikationen bereits auf beiden Standorten ausführen, wodurch sich die RTO während eines Failover verringert.

## SnapMirror

Nachfolgend finden Sie Empfehlungen für SnapMirror für SQL Server:

- Bei Verwendung von SMB muss die Ziel-SVM Mitglied derselben Active Directory-Domäne sein, der die Quell-SVM angehört, damit die in NAS-Dateien gespeicherten Zugriffssteuerungslisten (Access Control Lists, ACLs) während der Wiederherstellung nach einem Notfall nicht beschädigt werden.
- Die Verwendung von Ziel-Volume-Namen, die mit den Namen des Quell-Volume übereinstimmen, ist nicht erforderlich, kann jedoch das Mounten von Ziel-Volumes in das Ziel einfacher gestalten. Wenn SMB verwendet wird, müssen Sie den Ziel-NAS-Namespace in Pfaden und Verzeichnisstruktur mit dem Quell-Namespace identisch machen.
- Aus Konsistenzgründen sollten Sie keine SnapMirror Updates von den Controllern planen. Stattdessen sollten Sie SnapMirror Updates von SnapCenter aktivieren, um SnapMirror zu aktualisieren, nachdem ein vollständiger Backup oder ein Protokoll-Backup abgeschlossen wurde.
- Verteilen Sie Volumes, die SQL Server-Daten enthalten, auf verschiedene Nodes im Cluster, damit alle Clusterknoten SnapMirror-Replikationsaktivitäten gemeinsam nutzen können. Diese Verteilung optimiert die Nutzung von Knotenressourcen.
- Synchrone Replizierung, bei der eine schnelle Datenwiederherstellung erforderlich ist, und asynchrone Lösungen bieten Flexibilität bei RPO.

Weitere Informationen zu SnapMirror finden Sie unter "["TR-4015: SnapMirror Konfigurations- und Best Practices-Leitfaden für ONTAP 9"](#)".

## MetroCluster

### Der Netapp Architektur Sind

Für die Microsoft SQL Server-Bereitstellung mit einer MetroCluster-Umgebung ist eine Erklärung des physischen Designs eines MetroCluster-Systems erforderlich.

MetroCluster spiegelt Daten und Konfiguration synchron zwischen zwei ONTAP Clustern in separaten Speicherorten oder Ausfall-Domains. MetroCluster bietet kontinuierlich verfügbaren Storage für Applikationen, indem zwei Ziele automatisch gemanagt werden:

- Recovery Point Objective (RPO) von null durch synchrones Spiegeln von Daten, die auf das Cluster geschrieben werden.
- Recovery Time Objective (RTO) von nahezu null durch Spiegelung der Konfiguration und Automatisierung des Datenzugriffs am zweiten Standort

MetroCluster sorgt mit automatischer Datenspiegelung und Konfiguration zwischen den beiden unabhängigen Clustern an den beiden Standorten für Einfachheit. Wenn Storage innerhalb eines Clusters bereitgestellt wird, wird dieser automatisch auf das zweite Cluster am zweiten Standort gespiegelt. NetApp SyncMirror® bietet eine vollständige Kopie aller Daten mit einem RPO von null. Das bedeutet, dass Workloads von einem Standort jederzeit auf den gegenüberliegenden Standort umgeschaltet werden können und weiterhin Daten ohne Datenverlust bereitstellen können. MetroCluster managt die Umschaltung von Zugriff auf NAS- und SAN-bereitgestellte Daten am zweiten Standort. Das Design von MetroCluster als validierte Lösung umfasst die Größenanpassung und Konfiguration, die eine Umschaltung innerhalb der Protokollzeitlimits oder früher (in der Regel weniger als 120 Sekunden) ermöglicht. Die RPO ergibt sich so gut wie kein Wert, und Applikationen können ohne Ausfälle auf ihre Daten zugreifen. MetroCluster ist in verschiedenen Variationen über das Back-End Storage Fabric verfügbar.

### MetroCluster ist in 3 verschiedenen Konfigurationen erhältlich

- HA-Paare mit IP-Konnektivität
- HA-Paare mit FC-Konnektivität
- Single Controller mit FC-Konnektivität

 Der Begriff „Konnektivität“ bezieht sich auf die Clusterverbindung, die für die standortübergreifende Replizierung verwendet wird. Er bezieht sich nicht auf die Host-Protokolle. Unabhängig von der Art der Verbindung, die für die Kommunikation zwischen den Clustern verwendet wird, werden alle Host-seitigen Protokolle wie gewohnt in einer MetroCluster-Konfiguration unterstützt.

### MetroCluster IP

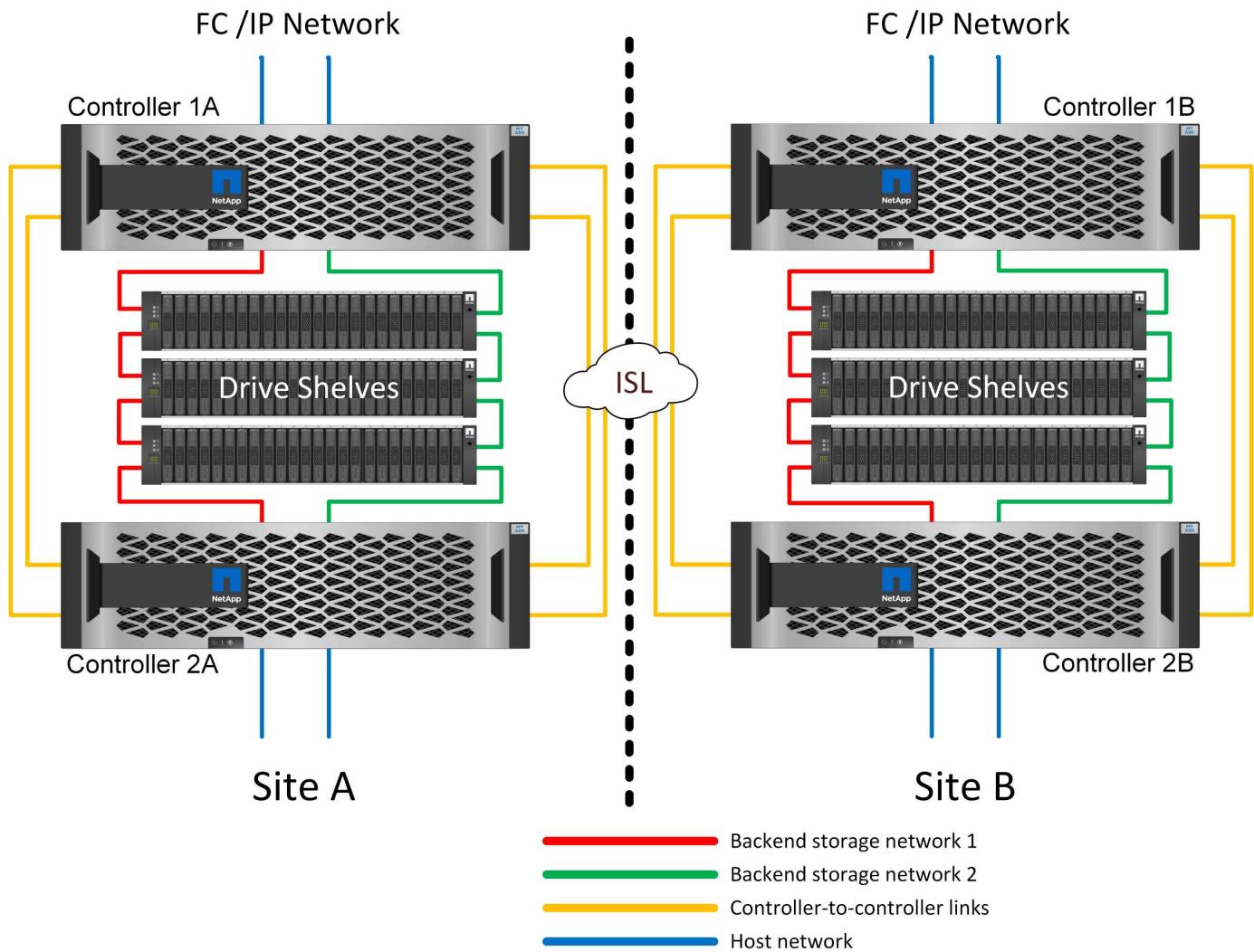
Die HA-Paar-MetroCluster IP-Konfiguration nutzt zwei oder vier Nodes pro Standort. Diese Konfigurationsoption erhöht die Komplexität und die Kosten im Vergleich zur Option mit zwei Nodes, bietet aber einen wichtigen Vorteil: intrasite-Redundanz. Bei einem einfachen Controller-Ausfall ist kein Datenzugriff über das WAN erforderlich. Der Datenzugriff bleibt über den alternativen lokalen Controller lokal.

Die meisten Kunden entscheiden sich für IP-Konnektivität, da die Infrastrukturanforderungen einfacher sind. In der Vergangenheit war die Bereitstellung von ultraschnellen standortübergreifenden Verbindungen über Dark Fibre und FC Switches im Allgemeinen einfacher, heute sind jedoch ultraschnelle IP-Verbindungen mit niedriger Latenz schneller verfügbar.

Auch die Architektur ist einfacher, da die einzigen standortübergreifenden Verbindungen für die Controller

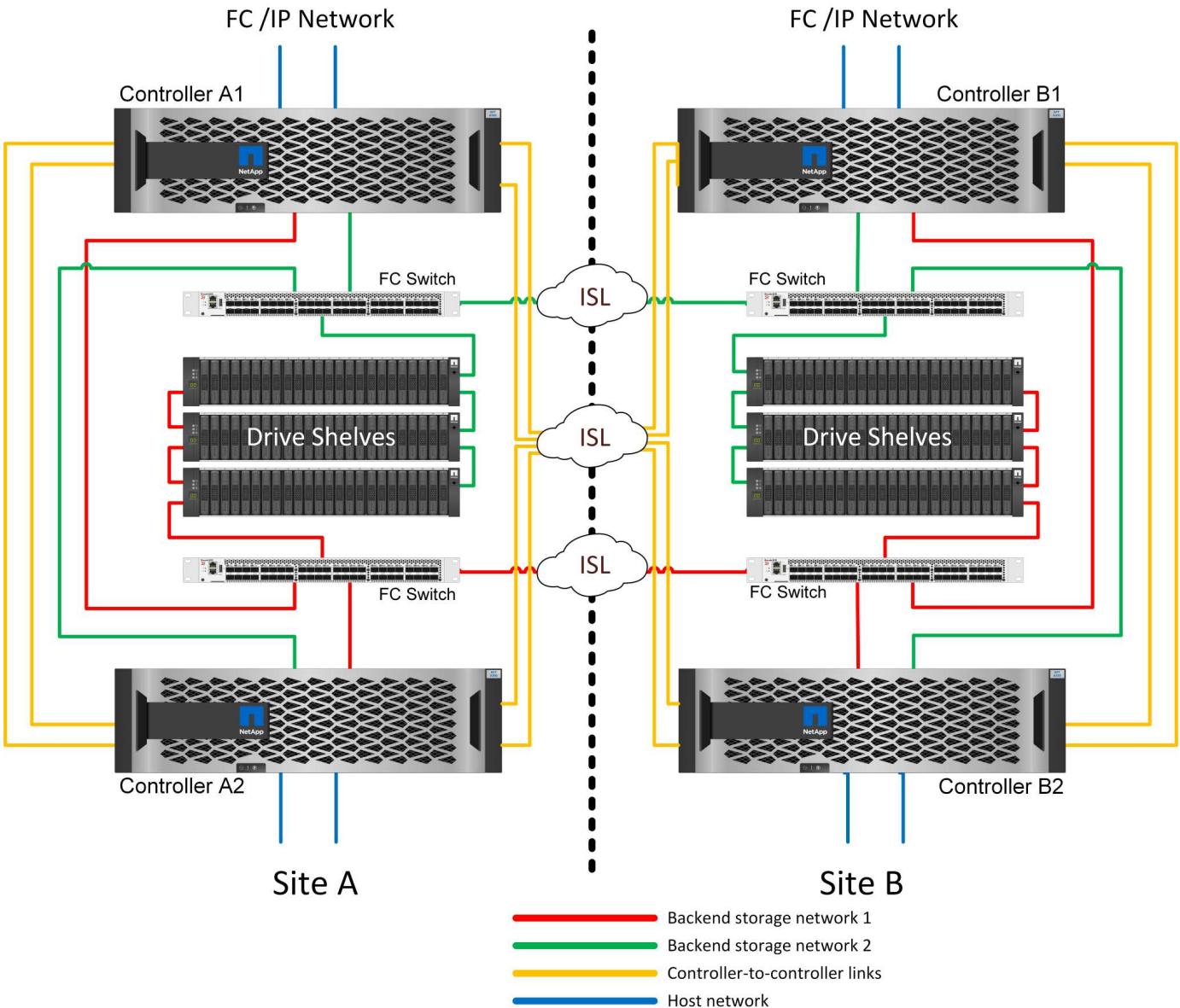
gelten. Bei FC SAN Attached MetroCluster schreibt ein Controller direkt auf die Laufwerke am entgegengesetzten Standort und benötigt somit zusätzliche SAN-Verbindungen, Switches und Bridges. Ein Controller in einer IP-Konfiguration hingegen schreibt über den Controller auf die entgegengesetzten Laufwerke.

Weitere Informationen finden Sie in der offiziellen ONTAP-Dokumentation und "["Architektur und Design der MetroCluster IP-Lösung"](#)".



### HA-Paar FC SAN Attached MetroCluster

Die HA-Paar-Konfiguration von MetroCluster FC nutzt zwei oder vier Nodes pro Standort. Diese Konfigurationsoption erhöht die Komplexität und die Kosten im Vergleich zur Option mit zwei Nodes, bietet aber einen wichtigen Vorteil: intrasite-Redundanz. Bei einem einfachen Controller-Ausfall ist kein Datenzugriff über das WAN erforderlich. Der Datenzugriff bleibt über den alternativen lokalen Controller lokal.



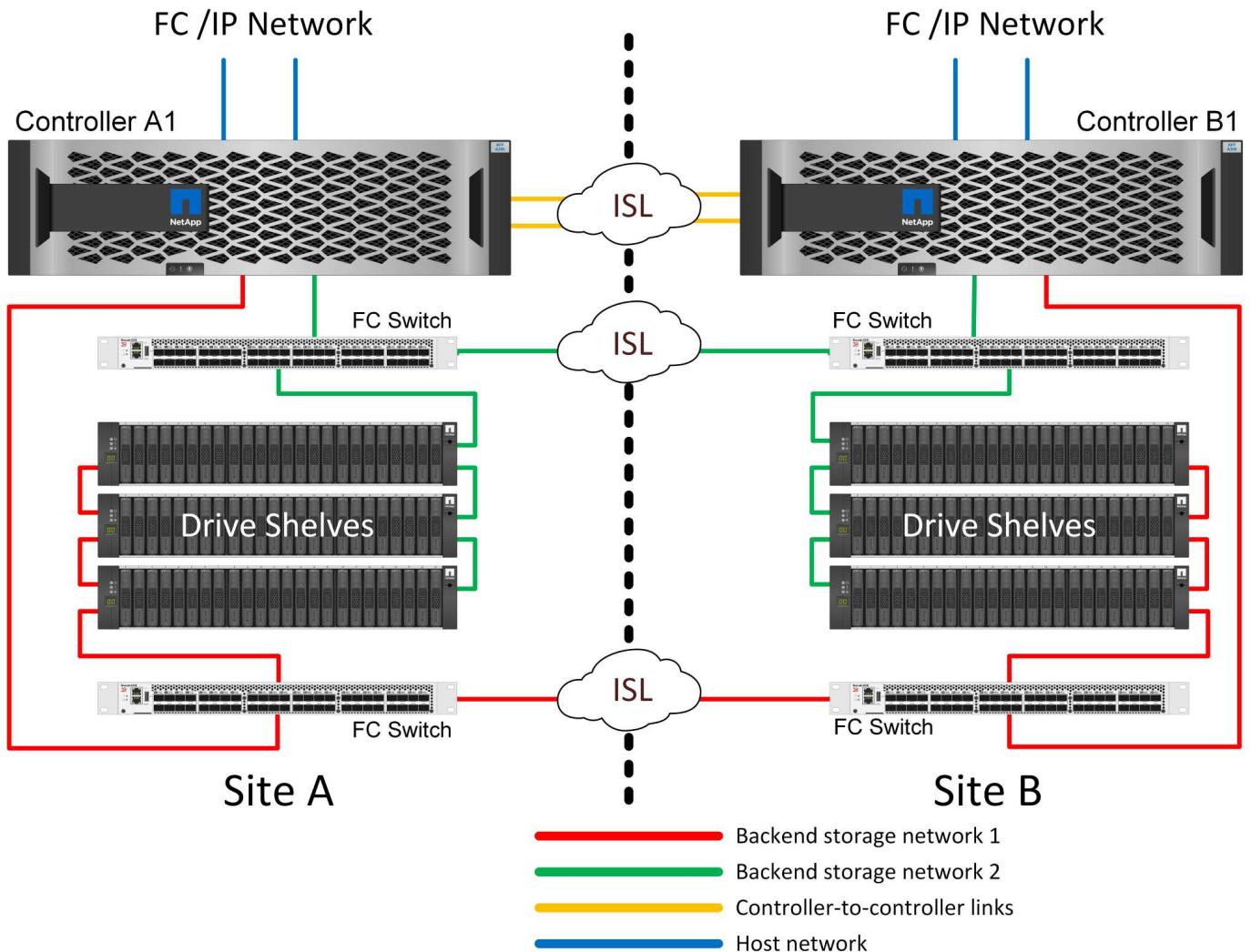
Einige Infrastrukturen mehrerer Standorte sind nicht für den aktiv/aktiv-Betrieb konzipiert, sondern werden eher als primärer Standort und Disaster-Recovery-Standort genutzt. In dieser Situation ist eine MetroCluster-Option für HA-Paare aus den folgenden Gründen im Allgemeinen vorzuziehen:

- Obwohl es sich bei einem MetroCluster Cluster mit zwei Nodes um ein HA-System handelt, müssen für einen unerwarteten Ausfall eines Controllers oder einer geplanten Wartung die Datenservices am anderen Standort online geschaltet werden. Wenn die Netzwerkverbindung zwischen Standorten die erforderliche Bandbreite nicht unterstützen kann, ist die Performance beeinträchtigt. Die einzige Option wäre auch ein Failover der verschiedenen Host-Betriebssysteme und der damit verbundenen Services zum alternativen Standort. Das HA-Paar MetroCluster Cluster eliminiert dieses Problem, da der Verlust eines Controllers zu einfachem Failover innerhalb desselben Standorts führt.
- Einige Netzwerktopologien sind nicht für den standortübergreifenden Zugriff ausgelegt, sondern verwenden stattdessen unterschiedliche Subnetze oder isolierte FC-SANs. In diesen Fällen fungiert der MetroCluster Cluster mit zwei Nodes nicht mehr als HA-System, da der alternative Controller keine Daten für die Server am gegenüberliegenden Standort bereitstellen kann. Um vollständige Redundanz zu gewährleisten, ist die MetroCluster Option für das HA-Paar erforderlich.
- Wird eine Infrastruktur mit zwei Standorten als eine einzelne hochverfügbare Infrastruktur angesehen, eignet sich die MetroCluster Konfiguration mit zwei Nodes. Falls das System jedoch nach einem

Standortausfall über einen längeren Zeitraum hinweg funktionieren muss, ist ein HA-Paar vorzuziehen, da es weiterhin HA innerhalb eines einzelnen Standorts bereitstellen muss.

### FC SAN-Attached MetroCluster mit zwei Nodes

Die MetroCluster Konfiguration mit zwei Nodes verwendet nur einen Node pro Standort. Dieses Design ist einfacher als die Option für HA-Paare, da weniger Komponenten konfiguriert und gewartet werden müssen. Zudem wurden die Infrastrukturanforderungen hinsichtlich Verkabelung und FC-Switching gesenkt. Und schließlich senkt es die Kosten.



Ein solches Design hat ganz offensichtlich zur Folge, dass der Controller-Ausfall an einem einzigen Standort dazu führt, dass die Daten am entgegengesetzten Standort verfügbar sind. Diese Einschränkung ist nicht unbedingt ein Problem. Viele Unternehmen verfügen über standortübergreifende Datacenter-Betriebsabläufe mit verteilten, schnellen Netzwerken mit niedriger Latenz, die im Wesentlichen als eine einzige Infrastruktur fungieren. In diesen Fällen ist die MetroCluster Version mit zwei Nodes die bevorzugte Konfiguration. Systeme mit zwei Nodes werden derzeit im Petabyte-Bereich von mehreren Service-Providern eingesetzt.

### Funktionen zur Ausfallsicherheit von MetroCluster

Es gibt keine Single Points of Failure in einer MetroCluster Lösung:

- Jeder Controller verfügt über zwei unabhängige Pfade zu den Laufwerk-Shelfs am lokalen Standort.

- Jeder Controller verfügt über zwei unabhängige Pfade zu den Laufwerk-Shelfs am Remote-Standort.
- Jeder Controller verfügt über zwei unabhängige Pfade zu den Controllern am gegenüberliegenden Standort.
- In der HA-Paar-Konfiguration besitzt jeder Controller zwei Pfade zu seinem lokalen Partner.

Zusammenfassend lässt sich sagen, dass jede Komponente der Konfiguration entfernt werden kann, ohne dass die Fähigkeit von MetroCluster zur Datenbereitstellung beeinträchtigt wird. Der einzige Unterschied in Bezug auf die Ausfallsicherheit zwischen den beiden Optionen ist, dass die HA-Paar-Version nach einem Standortausfall weiterhin ein insgesamt HA-Storage-System ist.

## **SyncMirror**

Die Sicherung für SQL Server mit MetroCluster basiert auf SyncMirror, die eine synchrone Spiegelungstechnologie zur maximalen Performance-Skalierung bietet.

### **Datensicherung mit SyncMirror**

Auf der einfachsten Ebene bedeutet synchrone Replikation, dass jede Änderung an beiden Seiten des gespiegelten Speichers vorgenommen werden muss, bevor sie bestätigt wird. Wenn beispielsweise eine Datenbank ein Protokoll schreibt oder ein VMware Gast gepatcht wird, darf ein Schreibvorgang nie verloren gehen. Als Protokollebene darf das Storage-System den Schreibvorgang erst dann bestätigen, wenn es auf nichtflüchtigen Medien an beiden Standorten gespeichert wurde. Nur dann ist es sicher, ohne das Risiko eines Datenverlusts zu gehen.

Die Verwendung einer Technologie zur synchronen Replizierung ist der erste Schritt beim Entwurf und Management einer Lösung zur synchronen Replizierung. Die wichtigste Überlegung ist, zu verstehen, was in verschiedenen geplanten und ungeplanten Ausfallszenarien passieren könnte. Nicht alle Lösungen zur synchronen Replizierung bieten dieselben Funktionen. Wenn Sie eine Lösung benötigen, die einen Recovery Point Objective (RPO) von null bietet, d. h. keinen Datenverlust verursacht, müssen alle Ausfallszenarien in Betracht gezogen werden. Welches ist insbesondere das erwartete Ergebnis, wenn die Replikation aufgrund des Verlusts der Verbindung zwischen Standorten nicht möglich ist?

### **SyncMirror Datenverfügbarkeit**

Die MetroCluster-Replizierung basiert auf der NetApp SyncMirror Technologie, mit der effizient in den synchronen Modus bzw. aus dem synchronen Modus gewechselt werden kann. Diese Funktion erfüllt die Anforderungen von Kunden, die synchrone Replizierung benötigen, aber auch Hochverfügbarkeit für ihre Datenservices benötigen. Wenn zum Beispiel die Verbindung zu einem Remote-Standort unterbrochen wird, ist es in der Regel besser, dass das Speichersystem weiterhin in einem nicht replizierten Zustand betrieben wird.

Viele Lösungen zur synchronen Replizierung können nur im synchronen Modus betrieben werden. Diese Art der alles-oder-nichts-Replikation wird manchmal Domino-Modus genannt. Solche Storage-Systeme stellen keine Daten mehr bereit, statt die lokalen und Remote-Kopien der Daten unsynchronisiert zu lassen. Wenn die Replikation gewaltsam unterbrochen wird, kann die Resynchronisierung äußerst zeitaufwendig sein und einen Kunden während der Wiederherstellung der Spiegelung einem vollständigen Datenverlust aussetzen.

SyncMirror kann nicht nur nahtlos aus dem synchronen Modus wechseln, wenn der Remote-Standort nicht erreichbar ist, sondern auch bei der Wiederherstellung der Konnektivität schnell zu einem RPO = 0-Zustand neu synchronisieren. Die veraltete Kopie der Daten am Remote-Standort kann während der Resynchronisierung auch in einem nutzbaren Zustand aufbewahrt werden. Auf diese Weise ist gewährleistet, dass lokale und Remote-Kopien der Daten jederzeit vorhanden sind.

Wo der Domino-Modus erforderlich ist, bietet NetApp SnapMirror Synchronous (SM-S) an. Darüber hinaus gibt es Optionen auf Applikationsebene wie Oracle DataGuard oder SQL Server Always On Availability Groups. Für

die Festplattenspiegelung auf Betriebssystemebene kann eine Option sein. Wenden Sie sich an Ihren NetApp oder Ihr Partner Account Team, um weitere Informationen und Optionen zu erhalten.

### **SQL Server mit MetroCluster**

Eine Option für den Schutz von SQL Server Datenbanken mit einem RPO von null ist MetroCluster. MetroCluster ist eine einfache, hochperformante RPO=0-Replizierungstechnologie, mit der Sie eine gesamte Infrastruktur mühelos über mehrere Standorte hinweg replizieren können.

SQL Server kann auf einem einzigen MetroCluster System bis zu Tausende von Datenbanken skalieren. Es könnten eigenständige SQL Server-Instanzen oder Failover-Cluster-Instanzen geben. Das MetroCluster System führt nicht unbedingt zu oder ändert keine Best Practices für das Management einer Datenbank.

Eine vollständige Erklärung von MetroCluster geht über den Umfang dieses Dokuments hinaus, aber die Prinzipien sind einfach. MetroCluster kann eine Replizierungslösung RPO=0 mit schnellem Failover bereitstellen. Was Sie auf dieser Grundlage aufbauen, hängt von Ihren Anforderungen ab.

Beispielsweise könnte ein grundlegendes schnelles DR-Verfahren nach einem plötzlichen Standortausfall folgende grundlegende Schritte durchführen:

- Erzwingen einer MetroCluster-Umschaltung
- Durchführen der Erkennung von FC/iSCSI-LUNs (nur SAN)
- Mounten Sie File-Systeme
- Starten Sie SQL Services

Die primäre Anforderung dieses Ansatzes ist ein Betriebssystem, das am Remote Standort ausgeführt wird. Es muss mit SQL Server-Setup vorkonfiguriert sein und sollte mit einer gleichwertigen Build-Version aktualisiert werden. SQL Server-Systemdatenbanken können auch am Remote-Standort gespiegelt und gemountet werden, wenn ein Notfall deklariert wird.

Wenn die Volumes, Dateisysteme und der Datastore, die virtualisierte Datenbanken hosten, vor dem Switchover nicht am Disaster-Recovery-Standort verwendet werden, müssen sie nicht auf zugehörigen Volumes festgelegt `dr-force-nvfail` werden.

### **SnapMirror Active Sync**

#### **Überblick**

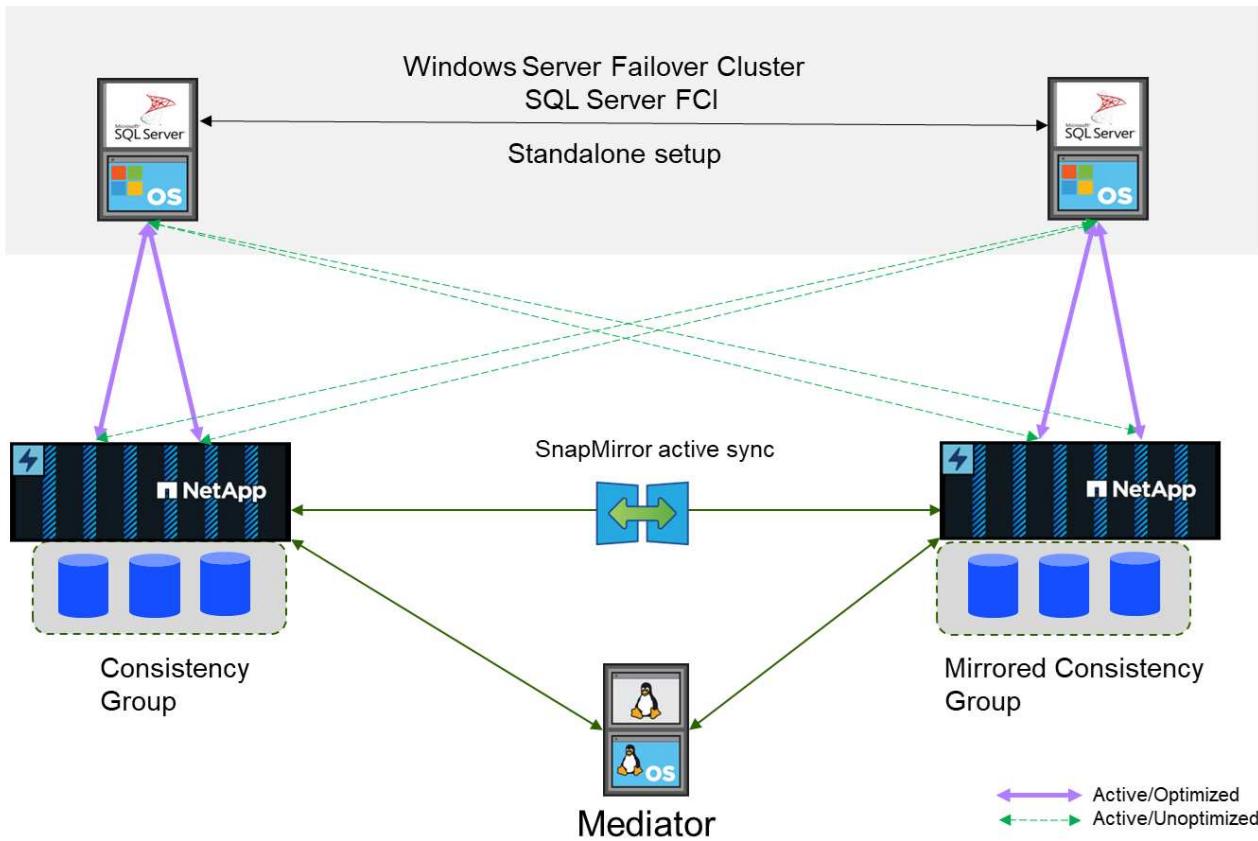
Mit SnapMirror Active Sync können einzelne SQL Server-Datenbanken und -Applikationen bei Storage- und Netzwerkstörungen den Betrieb fortsetzen. Der Storage Failover ist transparent, ohne dass manuelle Eingriffe erforderlich sind.

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync neben der bestehenden asymmetrischen Konfiguration auch die symmetrische aktiv/aktiv-Architektur. Symmetrische aktiv/aktiv-Funktion bietet synchrone bidirektionale Replikation für Business Continuity und Disaster Recovery. Es hilft Ihnen, Ihren Datenzugriff für kritische SAN-Workloads durch gleichzeitigen Lese- und Schreibzugriff auf Daten über mehrere Ausfall-Domains hinweg zu schützen. So wird ein unterbrechungsfreier Betrieb sichergestellt und Ausfallzeiten bei Notfällen oder Systemausfällen werden minimiert.

SQL-Server-Hosts greifen über Fibre Channel(FC)- oder iSCSI-LUNs auf Speicher zu. Replizierung zwischen jedem Cluster, das eine Kopie der replizierten Daten hostet. Da es sich bei dieser Funktion um die

Replizierung auf Storage-Ebene handelt, können SQL Server-Instanzen auf eigenständigen Host- oder Failover-Cluster-Instanzen Lese-/Schreibvorgänge durchführen. Informationen zu Planungs- und Konfigurationsschritten finden Sie unter "[ONTAP-Dokumentation über SnapMirror Active Sync](#)" .

## Architektur der SnapMirror Active Sync mit symmetrischer aktiv/aktiv-Lösung



## Synchrone Replikation

Im normalen Betrieb ist jede Kopie jederzeit ein synchrones RPO=0-Replikat, mit einer Ausnahme. Wenn Daten nicht repliziert werden können, gibt ONTAP die Notwendigkeit zur Replizierung von Daten frei und stellt die E/A-Bereitstellung an einem Standort wieder her, während die LUNs am anderen Standort offline geschaltet werden.

## Storage Hardware

Im Gegensatz zu anderen Disaster Recovery-Lösungen für Storage bietet SnapMirror Active Sync asymmetrische Plattformflexibilität. Die Hardware an den einzelnen Standorten muss nicht identisch sein. Dank dieser Funktion können Sie die Größe der Hardware anpassen, die zur Unterstützung der SnapMirror Active Sync verwendet wird. Das Remote-Storage-System kann identisch mit dem primären Standort sein, wenn es einen vollständigen Produktions-Workload unterstützen muss. Wenn jedoch ein Ausfall zu einer Verringerung der I/O führt, könnte ein kleineres System am Remote-Standort kostengünstiger sein.

## ONTAP Mediator

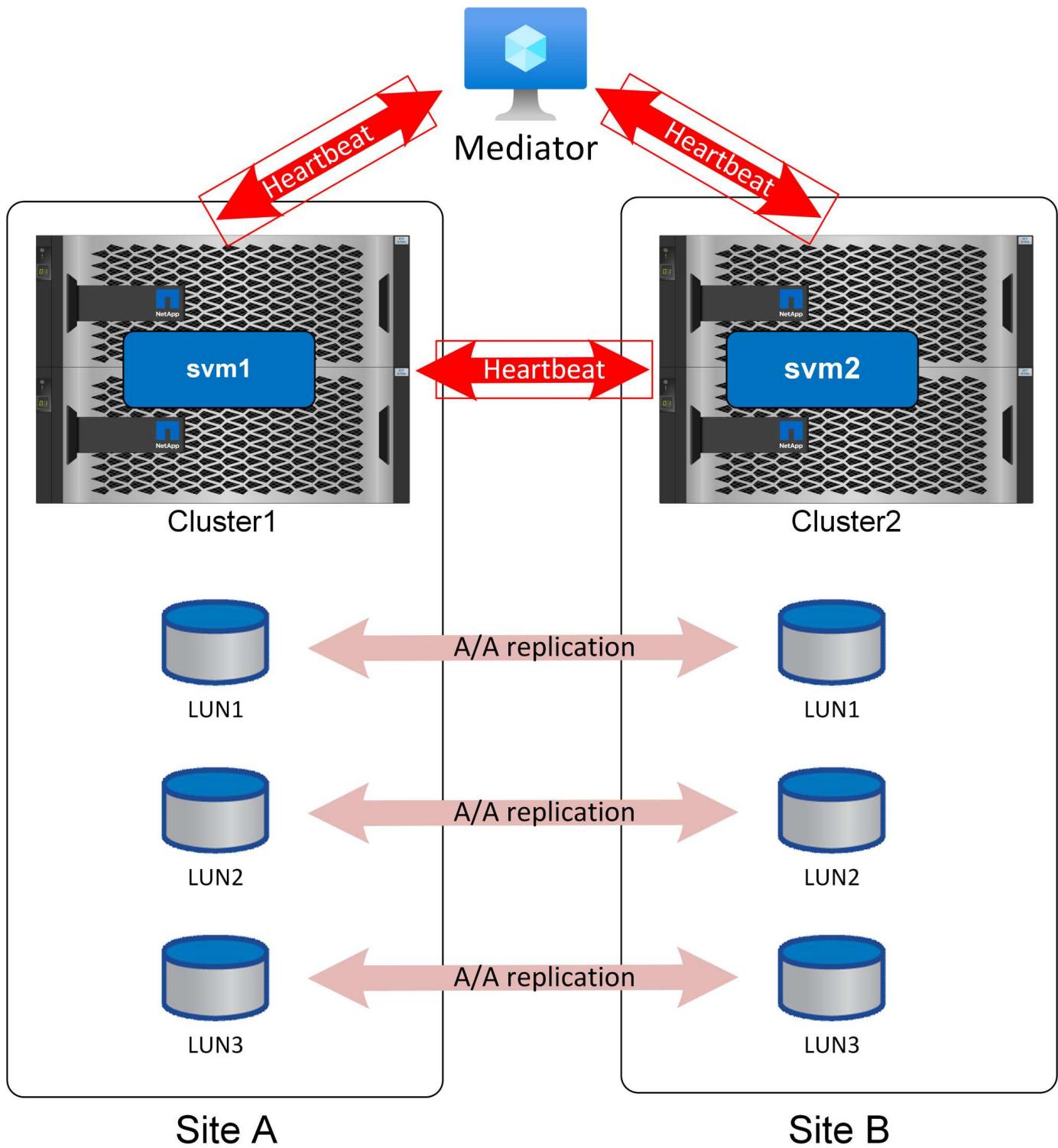
Der ONTAP Mediator ist eine Softwareanwendung, die von der NetApp-Unterstützung heruntergeladen wird und normalerweise auf einer kleinen virtuellen Maschine bereitgestellt wird. Der ONTAP Mediator ist kein Tiebreak. Es handelt sich um einen alternativen Kommunikationskanal für die beiden Cluster, die an der aktiven synchronen SnapMirror-Replikation beteiligt sind. Der automatisierte Betrieb wird durch ONTAP

basierend auf den Antworten gesteuert, die der Partner über direkte Verbindungen und den Mediator erhält.

#### **ONTAP Mediator**

Der Mediator ist für die sichere Automatisierung des Failover erforderlich. Idealerweise würde er an einem unabhängigen dritten Standort platziert werden, kann aber dennoch für die meisten Anforderungen funktionieren, wenn er mit einem der an der Replikation beteiligten Cluster kolokiert wird.

Der Mediator ist eigentlich kein Entscheider bei Stimmengleichständen, obwohl er diese Funktion faktisch übernimmt. Der Mediator hilft dabei, den Zustand der Clusterknoten zu ermitteln und unterstützt den automatischen Umschaltprozess im Falle eines Standortausfalls. Der Mediator übermittelt unter keinen Umständen Daten.



Die #1 Herausforderung mit automatisiertem Failover ist das Split-Brain-Problem, und dieses Problem tritt auf, wenn Ihre zwei Standorte die Verbindung miteinander verlieren. Was soll geschehen? Sie möchten nicht, dass sich zwei verschiedene Standorte als verbleibende Kopien der Daten bezeichnen, aber wie kann ein einzelner Standort den Unterschied zwischen dem tatsächlichen Verlust des anderen Standorts und der Unfähigkeit, mit dem gegenüberliegenden Standort zu kommunizieren, erkennen?

Hier betritt der Mediator das Bild. Wenn jeder Standort an einem dritten Standort platziert wird und über eine separate Netzwerkverbindung zu diesem Standort verfügt, haben Sie für jeden Standort einen zusätzlichen Pfad, um den Zustand des anderen zu überprüfen. Sehen Sie sich das Bild oben noch einmal an und

betrachten Sie die folgenden Szenarien.

- Was passiert, wenn der Mediator ausfällt oder von einem oder beiden Standorten nicht erreichbar ist?
  - Die beiden Cluster können weiterhin über dieselbe Verbindung miteinander kommunizieren, die für Replikationsdienste verwendet wird.
  - Für die Daten wird noch eine RPO=0-Sicherung verwendet
- Was passiert, wenn Standort A ausfällt?
  - An Standort B sehen Sie, dass beide Kommunikationskanäle ausgefallen sind.
  - Standort B übernimmt die Datenservices, jedoch ohne RPO=0-Spiegelung
- Was passiert, wenn Standort B ausfällt?
  - An Standort A sehen Sie, dass beide Kommunikationskanäle ausgefallen sind.
  - Standort A übernimmt die Datenservices, aber ohne RPO=0-Spiegelung

Es gibt ein anderes Szenario zu berücksichtigen: Verlust der Datenreplikationsverbindung. Wenn die Replikationsverbindung zwischen Standorten verloren geht, wird eine RPO=0-Spiegelung offensichtlich unmöglich sein. Was soll dann geschehen?

Dies wird durch den bevorzugten Standortstatus gesteuert. In einer SM-AS-Beziehung ist einer der Standorte zweitrangig zum anderen. Dies hat keine Auswirkungen auf den normalen Betrieb, und der gesamte Datenzugriff ist symmetrisch. Wenn die Replikation jedoch unterbrochen wird, muss die Verbindung unterbrochen werden, um den Betrieb wieder aufzunehmen. Das Ergebnis: Der bevorzugte Standort setzt den Betrieb ohne Spiegelung fort und der sekundäre Standort hält die I/O-Verarbeitung an, bis die Replizierungskommunikation wiederhergestellt ist.

#### **Bevorzugter Standort**

Das aktive Synchronisierungsverhalten von SnapMirror ist symmetrisch, mit einer wichtigen Ausnahme: Konfiguration des bevorzugten Standorts.

SnapMirror Active Sync betrachtet einen Standort als „Quelle“ und den anderen als „Ziel“. Dies impliziert eine One-Way-Replikationsbeziehung, aber dies gilt nicht für das IO-Verhalten. Die Replizierung ist bidirektional und symmetrisch, und die I/O-Reaktionszeiten sind auf beiden Seiten der Spiegelung identisch.

Die `source` Bezeichnung steuert den bevorzugten Standort. Wenn die Replizierungsverbindung verloren geht, stellen die LUN-Pfade auf der Quellkopie weiterhin Daten bereit, während die LUN-Pfade auf der Zielkopie erst dann wieder verfügbar sind, wenn die Replikation wiederhergestellt ist und SnapMirror wieder in den synchronen Zustand wechselt. Die Pfade setzen dann das Bereitstellen von Daten fort.

Die Sourcing/Ziel-Konfiguration kann über Systemmanager angezeigt werden:

## Relationships

The screenshot shows a web-based interface for managing relationships between storage volumes. At the top, there are tabs for 'Local destinations' and 'Local sources'. Below the tabs is a search bar and several action buttons: 'Search', 'Download', 'Show/hide', and 'Filter'. A table lists a single relationship entry:

Source	Destination	Policy type
jfs_as1:/cg/jfsAA	jfs_as2:/cg/jfsAA	Synchronous

Oder über die CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

      Source Path: jfs_as1:/cg/jfsAA
      Destination Path: jfs_as2:/cg/jfsAA
      Relationship Type: XDP
      Relationship Group Type: consistencygroup
      SnapMirror Schedule: -
      SnapMirror Policy Type: automated-failover-duplex
      SnapMirror Policy: AutomatedFailOverDuplex
      Tries Limit: -
      Throttle (KB/sec): -
      Mirror State: Snapmirrored
      Relationship Status: InSync
```

Der Schlüssel ist, dass die Quelle die SVM für Cluster1 ist. Wie oben erwähnt, beschreiben die Begriffe „Quelle“ und „Ziel“ nicht den Fluss replizierter Daten. Beide Standorte können einen Schreibvorgang verarbeiten und am anderen Standort replizieren. Beide Cluster sind Quellen und Ziele. Der Effekt der Festlegung eines Clusters als Quelle steuert einfach, welches Cluster als Lese-/Schreib-Speichersystem überlebt, wenn die Replikationsverbindung verloren geht.

### Netzwerktopologie

#### Einheitlicher Zugriff

Ein einheitliches Netzwerk für den Zugriff bedeutet, dass Hosts auf Pfade auf beiden Seiten (oder auf Ausfall-Domains innerhalb desselben Standorts) zugreifen können.

Eine wichtige Funktion von SM-AS ist die Möglichkeit, die Speichersysteme so zu konfigurieren, dass sie wissen, wo sich die Hosts befinden. Wenn Sie die LUNs einem bestimmten Host zuordnen, können Sie angeben, ob sie einem bestimmten Storage-System proximal sind oder nicht.

#### Annäherungseinstellungen

Proximity bezieht sich auf eine Clusterkonfiguration, die angibt, dass eine bestimmte Host-WWN- oder iSCSI-Initiator-ID zu einem lokalen Host gehört. Dies ist ein zweiter optionaler Schritt für die Konfiguration des LUN-

Zugriffs.

Der erste Schritt ist die übliche igroup-Konfiguration. Jede LUN muss einer Initiatorgruppe zugeordnet werden, die die WWN/iSCSI-IDs der Hosts enthält, die Zugriff auf diese LUN benötigen. Dadurch wird gesteuert, welcher Host Access zu einer LUN hat.

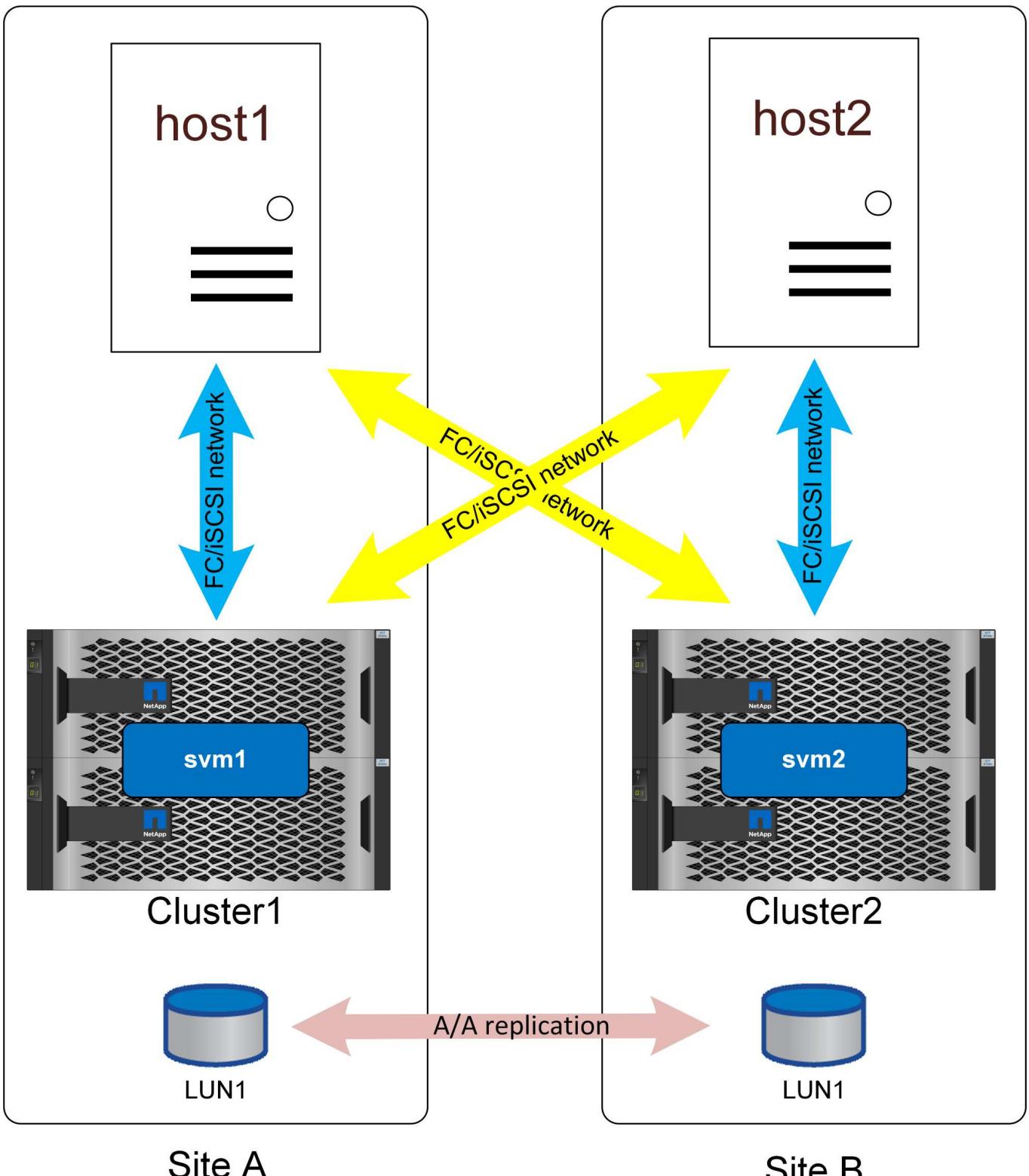
Der zweite, optionale Schritt ist die Konfiguration der Host-Nähe. Dies kontrolliert nicht den Zugriff, es steuert *Priority*.

Beispielsweise kann ein Host an Standort A für den Zugriff auf eine LUN konfiguriert werden, die durch SnapMirror Active Sync geschützt ist. Da das SAN über Standorte erweitert wird, stehen diesem LUN Pfade über Storage an Standort A oder Storage an Standort B zur Verfügung

Ohne Annäherungseinstellungen verwendet der Host beide Speichersysteme gleichmäßig, da beide Speichersysteme aktive/optimierte Pfade anbieten. Wenn die SAN-Latenz und/oder Bandbreite zwischen Standorten begrenzt ist, ist dies möglicherweise nicht erwünscht, und Sie sollten sicherstellen, dass während des normalen Betriebs jeder Host bevorzugt Pfade zum lokalen Speichersystem verwendet. Diese Konfiguration erfolgt durch Hinzufügen der Host-WWN/iSCSI-ID zum lokalen Cluster als proximaler Host. Dies kann unter der CLI oder Systemmanager ausgeführt werden.

## AFF

Bei einem AFF System werden die Pfade nach dem Konfigurieren von Host-Nähe wie unten dargestellt angezeigt.



Active/Optimized Path

Active Path

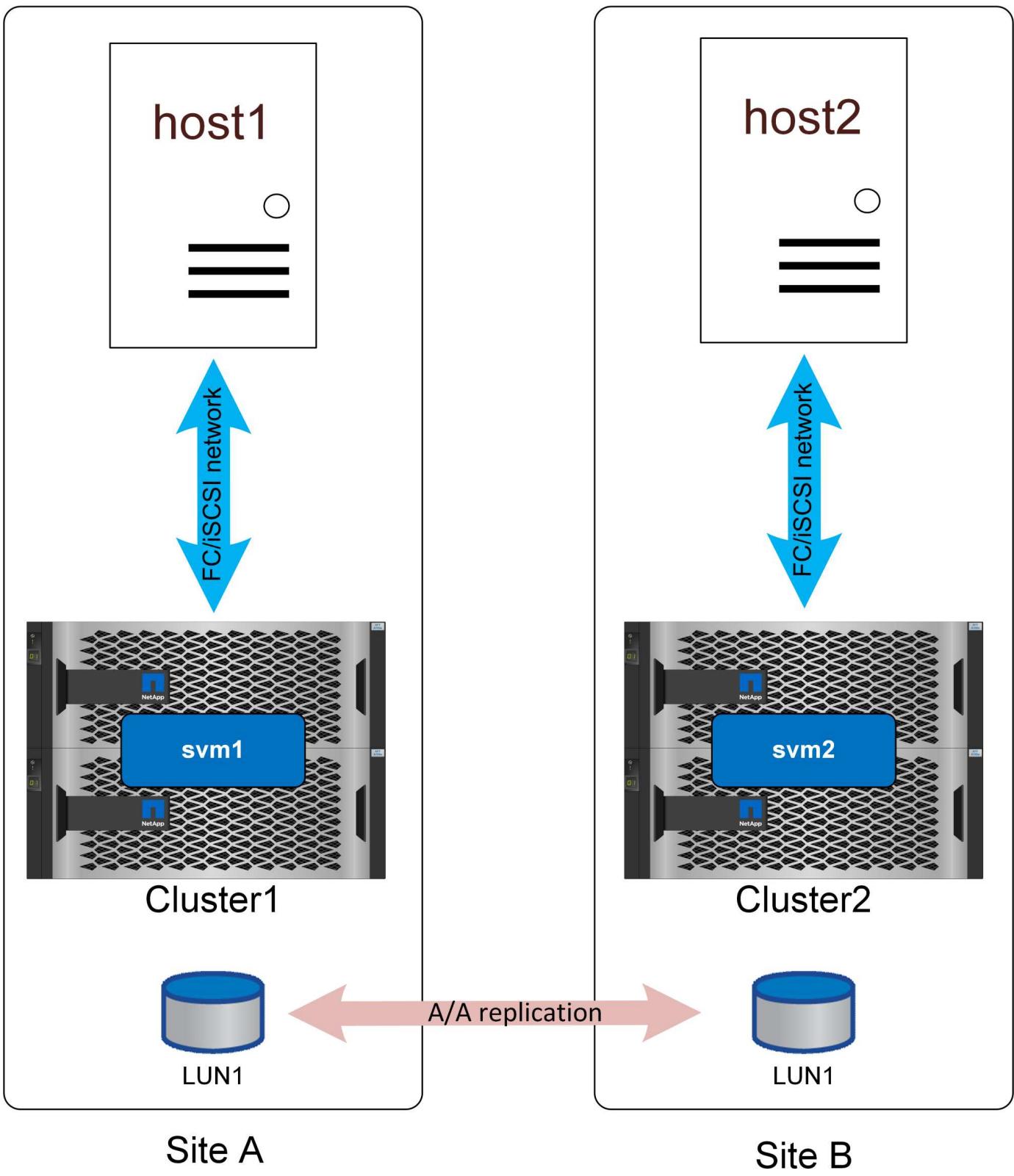
Im normalen Betrieb sind alle E/A-Vorgänge lokal. Lese- und Schreibvorgänge werden vom lokalen Speicher-Array gewartet. Schreib-I/O muss natürlich auch vom lokalen Controller auf das Remote-System repliziert werden, bevor sie bestätigt wird. Alle Lese-I/O-Vorgänge werden jedoch lokal gewartet und es kommt keine zusätzliche Latenz durch das Durchlaufen der SAN-Verbindung zwischen den Standorten zu.

Die nicht optimierten Pfade werden nur dann verwendet, wenn alle aktiven/optimierten Pfade verloren gehen. Wenn beispielsweise das gesamte Array an Standort A Strom verloren hätte, könnten die Hosts an Standort A weiterhin auf Pfade zum Array an Standort B zugreifen und bleiben daher betriebsbereit, obwohl die Latenz höher wäre.

Es gibt redundante Pfade durch den lokalen Cluster, die aus Gründen der Einfachheit nicht auf diesen Diagrammen angezeigt werden. ONTAP Storage-Systeme sind HA selbst, daher sollte ein Controller-Ausfall nicht zu einem Standortausfall führen. Es sollte lediglich zu einer Änderung führen, in der lokale Pfade auf dem betroffenen Standort verwendet werden.

### **Uneinheitlicher Zugriff**

Uneinheitliches Netzwerk durch Zugriff bedeutet, dass jeder Host nur Zugriff auf Ports im lokalen Storage-System hat. Das SAN wird nicht über Standorte (oder Ausfall-Domains am selben Standort) erweitert.



## Active/Optimized Path

Der Hauptvorteil dieses Ansatzes ist die SAN-Einfachheit – Sie müssen kein SAN mehr über das Netzwerk erweitern. Einige Kunden verfügen nicht über eine Konnektivität mit niedriger Latenz zwischen den Standorten

und haben nicht die Infrastruktur, um den FC SAN-Datenverkehr über ein standortverbundes Netzwerk zu Tunneln.

Der Nachteil eines uneinheitlichen Zugriffs besteht darin, dass bestimmte Ausfallszenarien, einschließlich des Verlusts der Replikationsverbindung, dazu führen, dass einige Hosts den Zugriff auf den Speicher verlieren. Applikationen, die als einzelne Instanzen ausgeführt werden, wie z. B. eine Datenbank ohne Cluster, die grundsätzlich nur auf einem einzelnen Host bei einem beliebigen Mount ausgeführt wird, würden ausfallen, wenn die lokale Storage-Konnektivität verloren geht. Die Daten bleiben zwar weiterhin geschützt, aber der Datenbankserver würde nicht mehr darauf zugreifen können. Es müsste an einem Remote-Standort neu gestartet werden, vorzugsweise durch einen automatisierten Prozess. VMware HA kann beispielsweise eine heruntergefahrenen Pfade auf einem Server erkennen und eine VM auf einem anderen Server neu starten, auf dem Pfade verfügbar sind.

Im Gegensatz dazu kann eine Cluster-Anwendung wie Oracle RAC einen Service bereitstellen, der gleichzeitig an zwei verschiedenen Standorten verfügbar ist. Der Verlust eines Standorts bedeutet nicht, dass der Anwendungsdienst als Ganzes verloren geht. Instanzen sind nach wie vor verfügbar und werden am verbleibenden Standort ausgeführt.

In vielen Fällen wäre die zusätzliche Latenz, wenn eine Applikation, die auf den Storage über eine Site-to-Site-Verbindung zugreift, nicht akzeptabel. Dies bedeutet, dass die verbesserte Verfügbarkeit von einheitlichem Netzwerk minimal ist, da der Verlust von Speicher an einem Standort dazu führen würde, dass die Dienste auf diesem ausgesetzten Standort sowieso heruntergefahren werden müssen.

 Es gibt redundante Pfade durch den lokalen Cluster, die aus Gründen der Einfachheit nicht auf diesen Diagrammen angezeigt werden. ONTAP Storage-Systeme sind HA selbst, daher sollte ein Controller-Ausfall nicht zu einem Standortausfall führen. Es sollte lediglich zu einer Änderung führen, in der lokale Pfade auf dem betroffenen Standort verwendet werden.

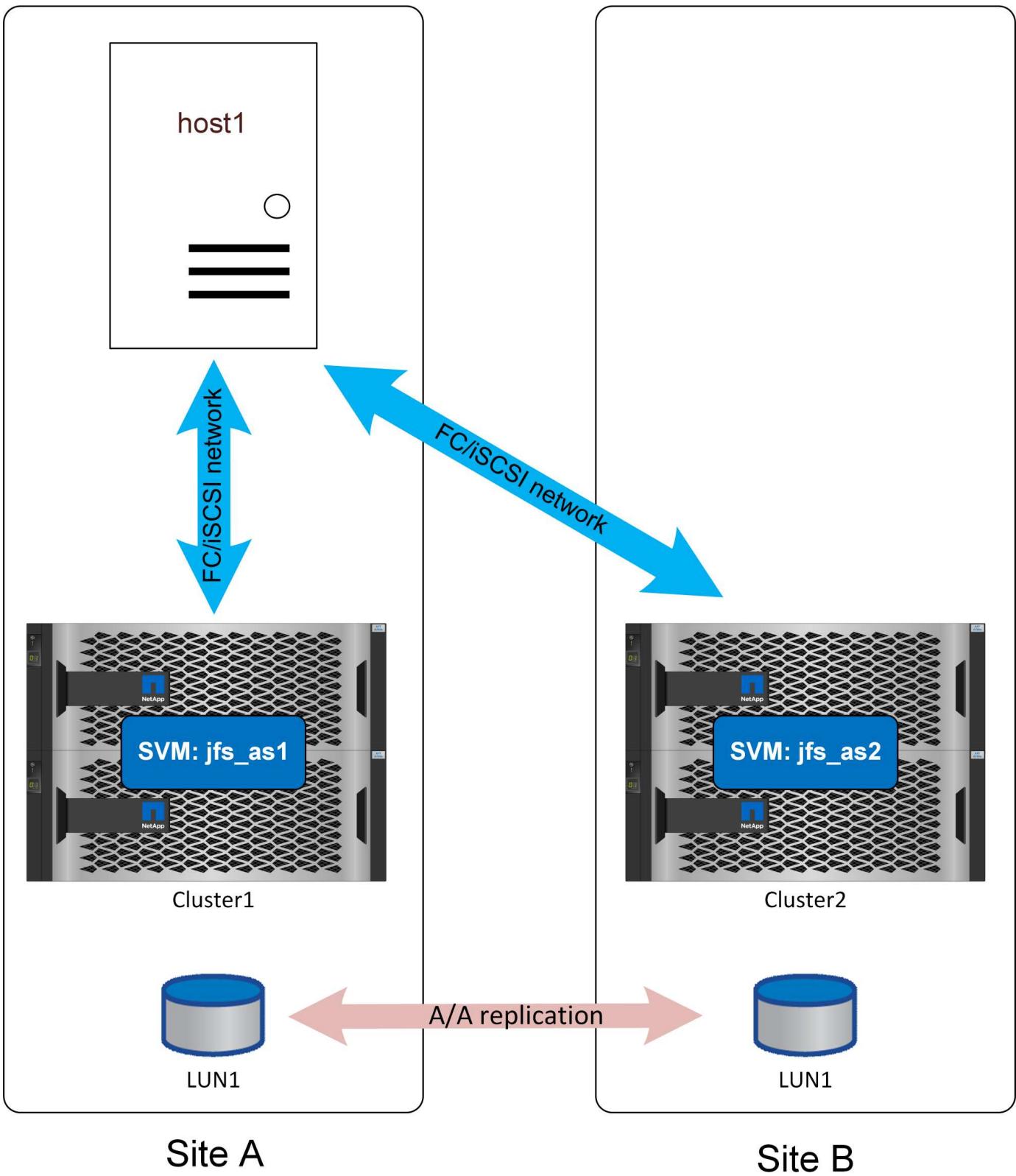
## Überblick

SQL Server kann so konfiguriert werden, dass er auf verschiedene Weise mit SnapMirror Active Sync arbeitet. Die richtige Antwort hängt von der verfügbaren Netzwerkkonnektivität, den RPO-Anforderungen und den Verfügbarkeitsanforderungen ab.

### Eigenständige Instanz von SQL Server

Die Best Practices für das Datei-Layout und die Serverkonfiguration sind dieselben, wie in der Dokumentation empfohlen "[SQL Server auf ONTAP](#)".

Mit einer eigenständigen Einrichtung konnte SQL Server nur an einem Standort ausgeführt werden. Vermutlich "[Einheitlich](#)" würde der Zugriff genutzt werden.



Bei einem einheitlichen Zugriff würde ein Storage-Ausfall an einem der Standorte den Datenbankbetrieb nicht unterbrechen. Ein kompletter Standortausfall am Standort, der den Datenbankserver einschloss, würde natürlich zu einem Ausfall führen.

Einige Kunden konnten ein Betriebssystem konfigurieren, das am Remote-Standort mit einem vorkonfigurierten SQL Server-Setup ausgeführt wird, das mit einer gleichwertigen Build-Version wie die der

Produktionsinstanz aktualisiert wurde. Bei einem Failover müsste die eigenständige Instanz von SQL Server am alternativen Standort aktiviert, die LUNS ermittelt und die Datenbank gestartet werden. Der vollständige Prozess kann mit dem Cmdlet "Windows PowerShell" automatisiert werden, da Storage-seitig kein Betrieb erforderlich ist.

"Uneinheitlich" Zugriff könnte auch verwendet werden, aber das Ergebnis wäre ein Datenbankausfall, wenn das Storage-System, in dem der Datenbankserver lokalisiert war, ausgefallen wäre, da die Datenbank keine Pfade zum Storage hätte. Dies kann in einigen Fällen noch akzeptabel sein. SnapMirror Active Sync bietet weiterhin RPO=0-Datensicherheit. Im Falle eines Standortausfalls wäre die noch verbleibende Kopie aktiv und bereit, den Betrieb mit demselben Verfahren wie oben beschrieben fortzusetzen.

Ein einfacher, automatisierter Failover-Prozess lässt sich mit der Verwendung eines virtuellen Hosts leichter konfigurieren. Wenn beispielsweise SQL Server-Datendateien zusammen mit einer Boot-VMDK synchron auf den sekundären Storage repliziert werden, könnte im Notfall die gesamte Umgebung am alternativen Standort aktiviert werden. Ein Administrator kann den Host am verbleibenden Standort entweder manuell aktivieren oder den Prozess über einen Service wie VMware HA automatisieren.

## **SQL Server Failover-Cluster-Instanz**

SQL Server Failover-Instanzen können auch auf einem Windows Failover Cluster gehostet werden, der auf einem physischen Server oder einem virtuellen Server als Gastbetriebssystem läuft. Diese Architektur mit mehreren Hosts bietet SQL Server Instanzen und Storage Resiliency. Diese Implementierung ist besonders in anspruchsvollen Umgebungen hilfreich, die robuste Failover-Prozesse suchen und gleichzeitig eine verbesserte Performance beibehalten. Wenn bei einem Failover-Cluster-Setup ein Host oder primärer Speicher betroffen ist, erfolgt ein Failover von SQL Services auf den sekundären Host, und gleichzeitig steht der sekundäre Speicher zur Verfügung, um IO bereitzustellen. Es sind kein Automatisierungsskript und keine Eingriffe durch den Administrator erforderlich.

### **Ausfallszenarien**

Die Planung einer vollständigen Applikationsarchitektur für die aktive Synchronisierung von SnapMirror erfordert ein Verständnis dafür, wie SM-AS in verschiedenen geplanten und ungeplanten Failover-Szenarien reagiert.

In den folgenden Beispielen wird davon ausgegangen, dass Standort A als bevorzugter Standort konfiguriert ist.

### **Verlust der Replikationskonnektivität**

Wenn die SM-AS-Replikation unterbrochen wird, kann die Schreib-I/O nicht abgeschlossen werden, da ein Cluster Änderungen nicht auf den anderen Standort replizieren kann.

#### **Standort A (bevorzugte Website)**

Das Ergebnis eines Ausfalls der Replikationsverbindung auf dem bevorzugten Standort ist eine ca. 15-Sekunden-Pause bei der Schreib-I/O-Verarbeitung, da ONTAP erneut replizierte Schreibvorgänge versucht, bevor festgestellt wird, dass die Replikationsverbindung wirklich nicht erreichbar ist. Nach 15 Sekunden wird die I/O-Verarbeitung von Lese- und Schreibzugriffen von Standort A fortgesetzt. Die SAN-Pfade ändern sich nicht, und die LUNs bleiben online.

#### **Standort B**

Da Standort B nicht der bevorzugte Standort für SnapMirror Active Sync ist, sind die LUN-Pfade nach ca. 15 Sekunden nicht mehr verfügbar.

## Ausfall des Storage-Systems

Das Ergebnis eines Storage-Systemausfalls ist nahezu identisch mit dem Ergebnis des Verlusts der Replizierungsverbindung. Am überlebenden Standort sollte eine I/O-Pause von etwa 15 Sekunden stattfinden. Nach Ablauf dieses Zeitraums von 15 Sekunden wird die E/A-Vorgänge wie gewohnt an diesem Standort fortgesetzt.

## Verlust des Mediators

Der Mediator hat keine direkte Kontrolle über Storage-Vorgänge. Er fungiert als alternativer Kontrollpfad zwischen Clustern. Die Lösung bietet insbesondere automatisierte Failover-Prozesse ohne Split-Brain-Szenario. Im normalen Betrieb repliziert jedes Cluster Änderungen an seinem Partner. Daher kann jedes Cluster überprüfen, ob das Partner-Cluster online ist und Daten bereitstellt. Wenn die Replikationsverbindung fehlschlägt, wird die Replikation beendet.

Der Grund für einen sicheren automatisierten Failover ist der Mediator, der darauf zurückzuführen ist, dass ein Storage-Cluster andernfalls nicht feststellen kann, ob der Ausfall einer bidirektionalen Kommunikation auf einen Netzwerkausfall oder einen tatsächlichen Storage-Ausfall zurückzuführen ist.

Der Mediator bietet jedem Cluster einen alternativen Pfad zur Überprüfung des Integrität seines Partners. Die Szenarien sind wie folgt:

- Wenn ein Cluster seinen Partner direkt kontaktieren kann, sind die Replizierungsservices betriebsbereit. Keine Aktion erforderlich.
- Wenn ein bevorzugter Standort nicht direkt mit dem Partner oder über den Mediator in Kontakt treten kann, wird davon ausgegangen, dass der Partner entweder tatsächlich nicht verfügbar ist oder isoliert wurde und seine LUN-Pfade offline geschaltet hat. Der bevorzugte Standort setzt dann den Status RPO=0 frei und setzt die Verarbeitung von Lese- und Schreib-I/O fort.
- Wenn ein nicht bevorzugter Standort seinen Partner nicht direkt kontaktieren kann, ihn aber über den Mediator kontaktieren kann, nimmt er seine Pfade offline und wartet auf die Rückkehr der Replikationsverbindung.
- Wenn ein nicht bevorzugter Standort keine direkte Kontaktaufnahme mit dem Partner oder über einen betrieblichen Mediator bietet, nimmt er an, dass der Partner entweder tatsächlich nicht verfügbar ist oder isoliert war und seine LUN-Pfade offline geschaltet hat. Der nicht bevorzugte Standort setzt dann den Status RPO=0 frei und verarbeitet sowohl Lese- als auch Schreib-I/O weiter. Er übernimmt die Rolle der Replikationsquelle und wird der neue bevorzugte Standort.

Wenn der Mediator vollständig nicht verfügbar ist:

- Wenn keine Replizierungsservices aus irgendeinem Grund verfügbar sind, beispielsweise der Ausfall des nicht bevorzugten Standorts oder des Storage-Systems, wird der bevorzugte Standort den Zustand RPO=0 freigeben und die I/O-Verarbeitung für Lese- und Schreibvorgänge wird wieder aufgenommen. Der nicht bevorzugte Standort nimmt seine Pfade offline.
- Ein Ausfall des bevorzugten Standorts führt zu einem Ausfall, da der nicht bevorzugte Standort nicht verifizieren kann, dass der gegenteilige Standort wirklich offline ist. Daher ist es für den nicht bevorzugten Standort nicht sicher, die Services wieder aufzunehmen.

## Dienste werden wiederhergestellt

Wenn ein Fehler behoben wurde, wie z. B. die Wiederherstellung der Site-to-Site-Verbindung oder das Einschalten eines ausgefallenen Systems, erkennen die SnapMirror Active Sync-Endpunkte automatisch, dass eine fehlerhafte Replikationsbeziehung vorhanden ist, und versetzen sie wieder in den Zustand RPO=0. Sobald die synchrone Replizierung wiederhergestellt ist, werden die fehlerhaften Pfade wieder online

geschaltet.

In vielen Fällen erkennen Cluster-Applikationen automatisch die Rückgabe ausgefallener Pfade, und diese Applikationen sind ebenfalls wieder online. In anderen Fällen ist möglicherweise ein SAN-Scan auf Host-Ebene erforderlich oder Applikationen müssen manuell wieder online geschaltet werden. Es hängt von der Anwendung und ihrer Konfiguration ab, und im Allgemeinen lassen sich solche Aufgaben leicht automatisieren. ONTAP selbst behebt selbstständig und sollte keinen Benutzereingriff erfordern, um den RPO=0-Storage-Betrieb wiederaufzunehmen.

## Manueller Failover

Das Ändern des bevorzugten Standorts erfordert eine einfache Bedienung. I/O-Vorgänge werden für eine oder zwei Sekunden angehalten, da zwischen den Clustern die Berechtigung für das Replikationsverhalten wechselt, die E/A-Vorgänge sind jedoch ansonsten nicht betroffen.

# Storage-Konfiguration auf ASA r2-Systemen

## Überblick

NetApp ASA r2 ist eine vereinfachte und leistungsstarke Lösung für reine SAN-Kunden, die geschäftskritische Workloads ausführen. Die Kombination der ASA r2 Plattform mit ONTAP Storage-Lösungen und Microsoft SQL Server ermöglicht Datenbank-Storage der Enterprise-Klasse, die auch die anspruchsvollsten Applikationsanforderungen von heute erfüllt.

Folgende ASA Plattformen werden als ASA r2 Systeme klassifiziert, die alle SAN-Protokolle (iSCSI, FC, NVMe/FC, NVMe/TCP) unterstützen. Die Protokolle iSCSI, FC, NVMe/FC und NVMe/TCP unterstützen die symmetrische aktiv/aktiv-Architektur für Multipathing, sodass alle Pfade zwischen Hosts und Storage aktiv/optimiert sind:

- ASAA1K
- ASAA90
- ASAA70
- ASAA50
- ASAA30
- ASAA20

Weitere Informationen finden Sie unter "[NetApp ASA](#)"

Um eine SQL Server auf ONTAP-Lösung zu optimieren, müssen Sie das I/O-Muster und die Merkmale des SQL Servers kennen. Ein gut konzipiertes Storage Layout für eine SQL Server Datenbank muss die Performance-Anforderungen von SQL Server unterstützen und gleichzeitig maximale Management-Fähigkeit der Infrastruktur als Ganzes bieten. Ein gutes Storage-Layout ermöglicht außerdem eine erfolgreiche Erstimplementierung und ein reibungsloses Wachstum der Umgebung im Laufe der Zeit, während das Unternehmen wächst.

## Datenspeicher Design

Microsoft empfiehlt, die Daten- und Protokolldateien auf separaten Laufwerken zu platzieren. Bei Anwendungen, die gleichzeitig Daten aktualisieren und anfordern, ist die Protokolldatei schreibintensiv und die

Datendatei (je nach Anwendung) ist Lese-/schreibintensiv. Für den Datenabruf wird die Protokolldatei nicht benötigt. Daher können Datenanfragen aus der Datendatei auf dem eigenen Laufwerk bearbeitet werden.

Wenn Sie eine neue Datenbank erstellen, empfiehlt Microsoft, getrennte Laufwerke für die Daten und Protokolle anzugeben. Um Dateien nach der Datenbankerstellung zu verschieben, muss die Datenbank offline geschaltet werden. Weitere Empfehlungen von Microsoft finden Sie unter "["Platzieren Sie Daten- und Protokolldateien auf separaten Laufwerken"](#)".

### Überlegungen zu Speichereinheiten

Die Storage-Einheit in ASA bezieht sich auf LUN für SCSI/FC-Hosts oder einen NVMe-Namespace für NVMe-Hosts. Basierend auf dem unterstützten Protokoll werden Sie aufgefordert, LUNs, NVMe Namespace oder beides zu erstellen. Bevor Sie eine Storage-Einheit für die Datenbankimplementierung erstellen, ist es wichtig zu wissen, wie das I/O-Muster und die Merkmale von SQL Server je nach Workload sowie den Backup- und Recovery-Anforderungen variieren. Beachten Sie die folgenden NetApp-Empfehlungen für die Speichereinheit:

- Vermeiden Sie, dieselbe Speichereinheit zwischen mehreren auf demselben Host laufenden SQL Server zu verwenden, um ein kompliziertes Management zu vermeiden. Wenn Sie mehrere SQL Server-Instanzen auf demselben Host ausführen, sollten Sie die Storage-Einheit auf einem Node nicht überschreiten, vermeiden Sie die gemeinsame Nutzung und verfügen stattdessen über eine separate Storage-Einheit pro Instanz pro Host zur Vereinfachung des Datenmanagements.
- Verwenden Sie NTFS-Bereitstellungspunkte anstelle von Laufwerksbuchstaben, um die Beschränkung auf 26 Laufwerksbuchstaben in Windows zu überschreiten.
- Snapshot Zeitpläne und Aufbewahrungsrichtlinien deaktivieren. Verwenden Sie stattdessen SnapCenter, um Snapshot Kopien der SQL Server Daten-Storage-Einheit zu koordinieren.
- Platzieren Sie die SQL Server-Systemdatenbanken auf einer dedizierten Speichereinheit.
- Tempdb ist eine Systemdatenbank, die von SQL Server als temporärer Arbeitsbereich verwendet wird, insbesondere für I/O-intensive DBCC-CHECKDB-Vorgänge. Legen Sie daher diese Datenbank auf eine dedizierte Speichereinheit. In großen Umgebungen, in denen die Anzahl der Speichereinheiten eine Herausforderung darstellt, können Sie tempdb nach sorgfältiger Planung mit Systemdatenbanken in derselben Speichereinheit konsolidieren. Datenschutz für tempdb hat keine hohe Priorität, da diese Datenbank bei jedem Neustart von SQL Server neu erstellt wird.
- Legen Sie Benutzerdatendateien ( .mdf ) auf eine separate Speichereinheit, da es sich um zufällige Lese-/Schreib-Workloads handelt. Es ist üblich, Transaktions-Log-Backups häufiger zu erstellen als Datenbank-Backups. Legen Sie daher Transaktions-Log-Dateien ( .ldf ) auf eine separate Speichereinheit oder VMDK aus den Datendateien, so dass für jede Datei unabhängige Backup-Zeitpläne erstellt werden können. Durch diese Trennung werden auch die I/O-Vorgänge bei sequenziellen Schreibvorgängen aus den I/O-Vorgängen für zufällige Lese-/Schreibzugriffe von Datendateien isoliert und die SQL Server Performance deutlich verbessert.
- Stellen Sie sicher, dass sich die Benutzerdatenbankdateien und das Protokollverzeichnis zum Speichern der Protokollsicherung auf einer separaten Speichereinheit befinden, um zu verhindern, dass die Aufbewahrungsrichtlinie Snapshots überschreibt, wenn diese mit der SnapMirror-Funktion mit der Vault-Richtlinie verwendet werden.
- Mischen Sie keine Datenbank- und nicht-Datenbankdateien, wie z. B. Dateien mit Volltextsuche, auf derselben Speichereinheit.
- Wenn sekundäre Datenbankdateien (als Teil einer Dateigruppe) auf eine separate Speichereinheit platziert werden, wird die Performance der SQL Server-Datenbank verbessert. Diese Trennung ist nur gültig, wenn die Datei der Datenbank .mdf ihre Speichereinheit nicht mit anderen Dateien teilt .mdf.
- Stellen Sie beim Formatieren der Festplatte mithilfe des Datenträgermanagers im Windows-Server sicher, dass die Größe der Zuordnungseinheit für die Partition auf 64K eingestellt ist.

- Legen Sie keine Benutzerdatenbanken oder Systemdatenbanken auf eine Speichereinheit, die Bereitstellungspunkte hostet.
- Siehe "[Microsoft Windows und natives MPIO unter den Best Practices von ONTAP für modernes SAN](#)" So wenden Sie Multipathing-Unterstützung unter Windows auf iSCSI-Geräte in den MPIO-Eigenschaften an.
- Wenn Sie eine Cluster-Instanz mit Always-On-Failover verwenden, müssen Benutzerdatenbanken auf einer Storage-Einheit platziert werden, die von den Failover-Cluster-Knoten des Windows-Servers gemeinsam genutzt wird, und die Cluster-Ressourcen des physischen Laufwerks werden der Cluster-Gruppe zugewiesen, die der SQL Server-Instanz zugeordnet ist.

## Datenbankdateien und Dateigruppen

Die korrekte Platzierung von SQL Server-Datenbankdateien auf ONTAP ist in der ersten Implementierungsphase entscheidend. Dies sorgt für optimale Performance, Speicherplatz-Management, Backup- und Wiederherstellungszeiten, die Ihren geschäftlichen Anforderungen entsprechend konfiguriert werden können.

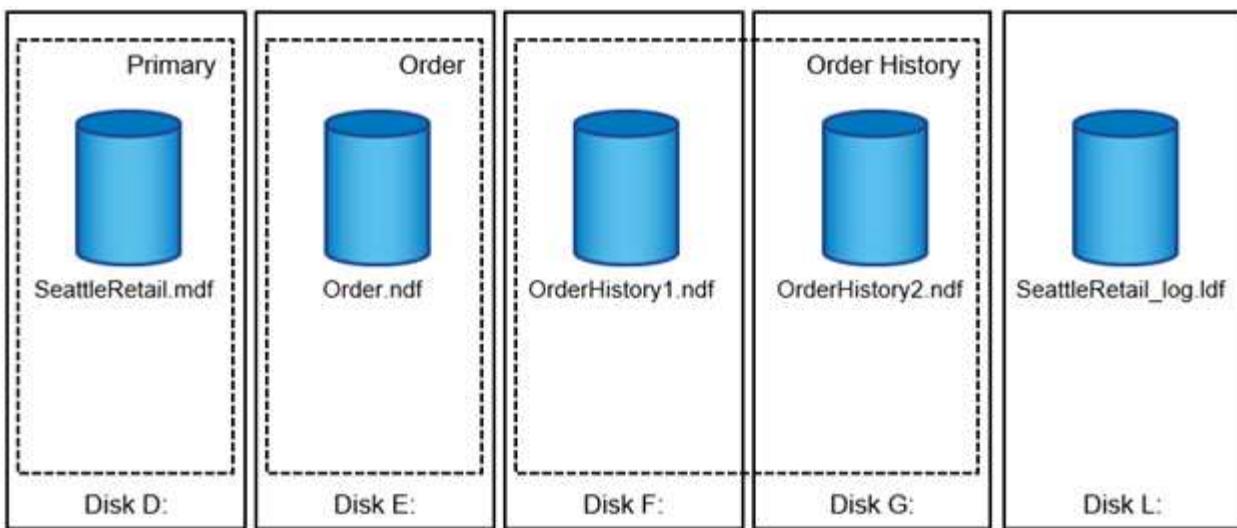
Theoretisch unterstützt SQL Server (64-Bit) 32.767 Datenbanken pro Instanz und 524.272 TB Datenbankgröße, obwohl die typische Installation normalerweise über mehrere Datenbanken verfügt. Die Anzahl der Datenbanken, die SQL Server verarbeiten kann, hängt jedoch von der Last und der Hardware ab. Es ist nicht ungewöhnlich, dass SQL Server Instanzen Dutzende, Hunderte oder sogar Tausende kleine Datenbanken hosten.

### Datenbankdateien & Dateigruppe

Jede Datenbank besteht aus einer oder mehreren Datendateien und einer oder mehreren Transaktions-Log-Dateien. Das Transaktionsprotokoll speichert die Informationen über Datenbanktransaktionen und alle von jeder Sitzung vorgenommenen Datenänderungen. Jedes Mal, wenn die Daten geändert werden, speichert SQL Server genügend Informationen im Transaktionsprotokoll, um die Aktion rückgängig zu machen (Rollback) oder zu wiederholen (Replay). Ein SQL Server-Transaktionsprotokoll ist ein integraler Bestandteil des Rufs von SQL Server für Datenintegrität und Robustheit. Das Transaktionsprotokoll ist für die Atomizität, Konsistenz, Isolation und Strapazierfähigkeit (ACID) von SQL Server von entscheidender Bedeutung. SQL Server schreibt in das Transaktionsprotokoll, sobald eine Änderung an der Datenseite erfolgt. Jede DML-Anweisung (Data Manipulation Language) (z. B. SELECT, Insert, Update oder delete) ist eine vollständige Transaktion, und das Transaktionsprotokoll stellt sicher, dass der gesamte Set-basierte Vorgang durchgeführt wird, um die Atomizität der Transaktion sicherzustellen.

Jede Datenbank verfügt über eine primäre Datendatei, die standardmäßig über die Erweiterung .mdf verfügt. Darüber hinaus kann jede Datenbank sekundäre Datenbankdateien enthalten. Diese Dateien haben standardmäßig .ndf-Erweiterungen.

Alle Datenbankdateien werden in Dateigruppen gruppiert. Eine Dateigruppe ist die logische Einheit, die die Datenbankverwaltung vereinfacht. Sie ermöglichen die Trennung zwischen einer logischen Objektplatzierung und physischen Datenbankdateien. Wenn Sie die Tabellen für Datenbankobjekte erstellen, geben Sie an, in welcher Dateigruppe sie platziert werden sollen, ohne sich um die zugrunde liegende Datendateikonfiguration zu sorgen.



Die Fähigkeit, mehrere Datendateien innerhalb der Dateigruppe zu speichern, ermöglicht es Ihnen, die Last auf verschiedene Speichergeräte zu verteilen, wodurch die I/O-Performance des Systems verbessert wird. Der Kontrast für die Transaktionsprotokollanmeldung profitiert nicht von den mehreren Dateien, da SQL Server in sequenzieller Weise in das Transaktionsprotokoll schreibt.

Die Trennung zwischen der Platzierung logischer Objekte in den Dateigruppen und physischen Datenbankdateien ermöglicht es Ihnen, das Layout von Datenbankdateien zu optimieren und so das Storage-Subsystem optimal zu nutzen. Die Anzahl der Datendateien, die einen mitgebenden Workload unterstützen, kann nach Bedarf variiert werden, um I/O-Anforderungen und erwartete Kapazität ohne Auswirkungen auf die Applikation zu erfüllen. Diese Variationen im Datenbank-Layout sind für Anwendungsentwickler transparent, die die Datenbankobjekte in Dateigruppen statt in Datenbankdateien platzieren.

 **NetApp empfiehlt** die Verwendung der primären Dateigruppe für alles andere als Systemobjekte zu vermeiden. Das Erstellen einer separaten Dateigruppe oder einer Gruppe von Dateigruppen für die Benutzerobjekte vereinfacht die Datenbankverwaltung und Disaster Recovery, insbesondere bei großen Datenbanken.

#### Initialisierung der Datenbankinstanzdatei

Sie können die ursprüngliche Dateigröße und die automatischen Wachstumsparameter angeben, wenn Sie die Datenbank erstellen oder neue Dateien zu einer vorhandenen Datenbank hinzufügen. SQL Server verwendet einen proportionalen Füllalgorithmus bei der Auswahl der Datendatei, in die Daten geschrieben werden sollen. Es schreibt eine Datenmenge proportional zum verfügbaren freien Speicherplatz in den Dateien. Je mehr Speicherplatz in der Datei verfügbar ist, desto mehr Schreibvorgänge werden verarbeitet.

 **NetApp empfiehlt**, dass alle Dateien in der einzelnen Dateigruppe die gleiche Anfangsgröße und die gleichen Autogrowth-Parameter haben, wobei die Grow-Größe in Megabyte und nicht in Prozentsätzen definiert ist. Dies hilft dem proportionalen Füllalgorithmus, Schreibaktivitäten gleichmäßig über Datendateien hinweg auszugleichen.

Jedes Mal, wenn SQL Server Dateien vergrößert, füllt es neu zugewiesenen Speicherplatz mit Nullen. Dieser Prozess blockiert alle Sitzungen, die in die entsprechende Datei geschrieben werden müssen, oder generiert im Falle eines Wachstums des Transaktionsprotokolls Transaktionsprotokolle.

SQL Server löscht das Transaktionsprotokoll immer auf Null, und dieses Verhalten kann nicht geändert werden. Sie können jedoch festlegen, ob Datendateien auf Null gesetzt werden, indem Sie die sofortige Dateiinitialisierung aktivieren oder deaktivieren. Durch die sofortige Dateiinitialisierung wird das Wachstum von

Datendateien beschleunigt und der Zeitaufwand für die Erstellung oder Wiederherstellung der Datenbank verringert.

Mit der sofortigen Dateiinitialisierung ist ein kleines Sicherheitsrisiko verbunden. Wenn diese Option aktiviert ist, können nicht zugewiesene Teile der Datendatei Informationen aus zuvor gelöschten Betriebssystemdateien enthalten. Datenbankadministratoren können solche Daten prüfen.

Sie können die sofortige Dateiinitialisierung aktivieren, indem Sie dem SQL Server-Startkonto die Berechtigung SA\_MANAGE\_VOLUME\_NAME, auch bekannt als „Perform Volume Maintenance Task“, hinzufügen. Sie können dies unter der Anwendung zur Verwaltung lokaler Sicherheitsrichtlinien (secpol.msc) tun, wie in der folgenden Abbildung dargestellt. Öffnen Sie die Eigenschaften für die Berechtigung zum Ausführen von Volume-Wartungsaufgaben und fügen Sie das SQL Server-Startkonto zur Liste der Benutzer dort hinzu.

Policy	Security Setting
Increase a process working set	Users
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Administrators, Backup ...
Log on as a service	SEA-TM\Administrator, ...
Manage auditing and security log	Administrators
Modify an object label	
Modify firmware environment values	Administrators
Obtain an impersonation token for ano...	Administrators
<b>Perform volume maintenance tasks</b>	<b>Administrators</b>
Profile single process	Administrators
Profile system performance	Administrators, NT SERVI...
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE, NETWO...
Restore files and directories	Administrators, Backup ...
Shut down the system	Administrators, Backup ...
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Um zu überprüfen, ob die Berechtigung aktiviert ist, können Sie den Code aus dem folgenden Beispiel verwenden. Dieser Code setzt zwei Trace-Flags, die SQL Server zwingen, zusätzliche Informationen in das Fehlerprotokoll zu schreiben, eine kleine Datenbank zu erstellen und den Inhalt des Protokolls zu lesen.

```

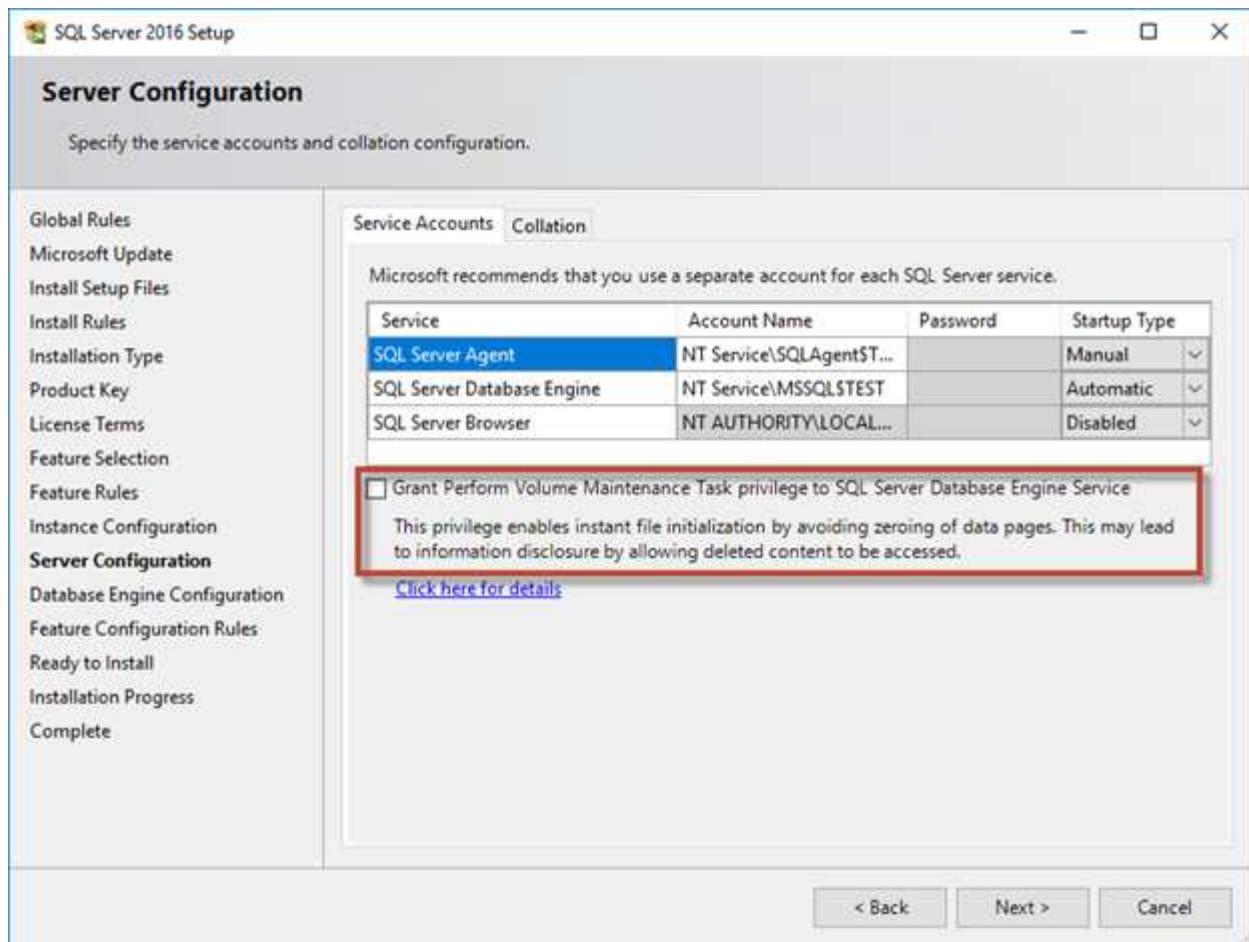
DBCC TRACEON(3004,3605,-1)
GO
CREATE DATABASE DelMe
GO
EXECUTE sp_readerrorlog
GO
DROP DATABASE DelMe
GO
DBCC TRACEOFF(3004,3605,-1)
GO

```

Wenn die sofortige Dateiinitialisierung nicht aktiviert ist, zeigt das SQL Server-Fehlerprotokoll an, dass SQL Server die mdf-Datendatei zusätzlich zum Nullsetzen der ldf-Protokolldatei auf Null setzt, wie im folgenden Beispiel gezeigt. Wenn die sofortige Dateiinitialisierung aktiviert ist, wird nur das Nullsetzen der Protokolldatei angezeigt.

	LogDate	ProcessInfo	Text
365	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 flush delta counts.
366	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 logging active xact info.
367	2017-02-09 08:10:07.750	spid53	Ckpt dbid 3 phase 1 ended (8)
368	2017-02-09 08:10:07.750	spid53	About to log Checkpoint end.
369	2017-02-09 08:10:07.880	spid53	Ckpt dbid 3 complete
370	2017-02-09 08:10:08.130	spid53	Starting up database 'DelMe'.
371	2017-02-09 08:10:08.150	spid53	Fixup Log tail(progress) zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.mdf
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.ldf
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL Server\MSSQL\DATA\DelMe.ldf
374	2017-02-09 08:10:08.710	spid53	Ckpt dbid 6 started
375	2017-02-09 08:10:08.710	spid53	About to log Checkpoint begin.

Die Aufgabe „Volume Maintenance durchführen“ wird in SQL Server 2016 vereinfacht und später während des Installationsprozesses als Option bereitgestellt. In dieser Abbildung wird die Option angezeigt, dem SQL Server-Datenbank-Engine-Service die Berechtigung zum Ausführen der Volume-Wartungsaufgabe zu gewähren.



Eine weitere wichtige Datenbankoption, die die Größe der Datenbankdateien steuert, ist Autoshrink. Wenn diese Option aktiviert ist, verkleinert SQL Server die Datenbankdateien regelmäßig, reduziert deren Größe und gibt Speicherplatz für das Betriebssystem frei. Dieser Vorgang ist ressourcenintensiv und nur selten sinnvoll, da die Datenbankdateien nach einiger Zeit wieder wachsen, wenn neue Daten in das System gelangen. Autoshrink sollte in der Datenbank nicht aktiviert sein.

### Protokollverzeichnis

Das Protokollverzeichnis wird in SQL Server angegeben, um die Backup-Daten des Transaktionsprotokolls auf Hostebene zu speichern. Wenn Sie SnapCenter zum Sichern von Protokolldateien verwenden, muss für jeden von SnapCenter verwendeten SQL Server-Host ein Hostprotokollverzeichnis konfiguriert sein, um Protokollsicherungen durchzuführen.

Platzieren Sie das Protokollverzeichnis auf einer dedizierten Speichereinheit. Die Datenmenge im Host-Log-Verzeichnis hängt von der Größe der Backups und der Anzahl der Tage ab, die Backups aufbewahrt werden. SnapCenter erlaubt nur ein Host-Protokollverzeichnis pro SQL Server-Host. Sie können die Host-Protokollverzeichnisse unter SnapCenter → Host → Configure Plug-in konfigurieren.

## **NetApp empfiehlt** für ein Host-Log-Verzeichnis:

- Stellen Sie sicher, dass das Host-Protokollverzeichnis nicht von anderen Datentypen gemeinsam genutzt wird, die möglicherweise die Backup-Snapshot-Daten beschädigen können.
- Erstellen Sie das Host-Protokollverzeichnis auf einer dedizierten Speichereinheit, auf die SnapCenter Transaktionsprotokolle kopiert.
- Wenn Sie eine Always-On-Failover-Cluster-Instanz verwenden, muss die für das Host-Protokollverzeichnis verwendete Speichereinheit eine Clusterdiskette in derselben Cluster-Gruppe wie die in SnapCenter gesicherte SQL Server-Instanz sein.



## Datensicherung

Strategien für Datenbank-Backups sollten auf den ermittelte geschäftliche Anforderungen basieren, nicht auf theoretischen Möglichkeiten. Durch die Kombination der Snapshot Technologie von ONTAP und der Nutzung der Microsoft SQL Server APIs können Sie schnell applikationskonsistente Backups unabhängig von der Größe der Benutzerdatenbanken erstellen. Für erweiterte oder horizontal skalierbare Datenmanagement-Anforderungen bietet NetApp SnapCenter.

### SnapCenter

SnapCenter ist die NetApp Datensicherungssoftware für Enterprise-Applikationen. Mit dem SnapCenter Plug-in für SQL Server und den vom SnapCenter Plug-in für Microsoft Windows verwalteten Betriebssystemvorgängen können SQL Server Datenbanken schnell und einfach gesichert werden.

Bei der SQL Server-Instanz kann es sich um eine eigenständige Einrichtung oder eine Failover-Cluster-Instanz handeln oder um eine Always-On-Verfügbarkeitsgruppe. Im Ergebnis können Datenbanken über eine zentrale Konsole geschützt, geklont und aus der primären oder sekundären Kopie wiederhergestellt werden. Mit SnapCenter lassen sich SQL Server Datenbanken sowohl vor Ort, in der Cloud als auch in hybriden Konfigurationen managen. Datenbankkopien können für Entwicklungszwecke oder für Berichte in wenigen Minuten auf dem ursprünglichen oder alternativen Host erstellt werden.

SQL Server erfordert außerdem eine Koordination zwischen OS und Storage, um sicherzustellen, dass bei der Erstellung die korrekten Daten in Snapshots vorhanden sind. In den meisten Fällen ist die einzige sichere Methode, dies mit SnapCenter oder T-SQL zu tun. Ohne diese zusätzliche Koordination erstellte Snapshots sind unter Umständen nicht zuverlässig wiederherstellbar.

Weitere Informationen zum SQL Server-Plug-in für SnapCenter finden Sie unter ["TR-4714: Best Practice Guide für SQL Server mit NetApp SnapCenter"](#).

### Datenbanken mit T-SQL-Snapshots werden gesichert

In SQL Server 2022 hat Microsoft T-SQL Snapshots eingeführt, die einen Pfad zu Skripting und Automatisierung von Backup-Vorgängen bieten. Anstatt Kopien in voller Größe zu erstellen, können Sie die Datenbank für Snapshots vorbereiten. Sobald die Datenbank für das Backup bereit ist, können Sie Snapshots mithilfe der ONTAP REST-APIs erstellen.

Im Folgenden finden Sie ein Beispiel für einen Backup-Workflow:

1. Eine Datenbank mit dem Befehl ALTER fixieren. Dadurch wird die Datenbank auf einen konsistenten Snapshot auf dem zugrunde liegenden Speicher vorbereitet. Nach dem Einfrieren können Sie die

- Datenbank auftauen und den Snapshot mit dem BACKUP-Befehl aufzeichnen.
2. Führen Sie Snapshots mehrerer Datenbanken auf den Speichereinheiten gleichzeitig mit den Befehlen der neuen BACKUP-GRUPPE und des BACKUP-SERVERS durch.
  3. Wenn der Datenbank-Workload über mehrere Storage-Einheiten verteilt ist, erstellen Sie Konsistenzgruppen, um Managementaufgaben zu vereinfachen. Die Konsistenzgruppe ist eine Sammlung von Speichereinheiten, die als eine Einheit gemanagt werden.
  4. Führen Sie VOLLSTÄNDIGE Backups oder COPY\_ONLY VOLLSTÄNDIGE Backups durch. Diese Backups werden auch in msdb aufgezeichnet.
  5. Durchführung einer zeitpunktgenauen Recovery mithilfe von Protokoll-Backups, die mit dem normalen Streaming-Ansatz nach dem VOLLSTÄNDIGEN Snapshot-Backup erstellt wurden. Streaming Differential Backups werden auf Wunsch auch unterstützt.

Weitere Informationen finden Sie unter "[Microsoft-Dokumentation zu den T-SQL-Snapshots](#)".

 **NetApp empfiehlt** SnapCenter zum Erstellen von Snapshot Kopien zu verwenden. Die oben beschriebene T-SQL-Methode funktioniert ebenfalls, SnapCenter bietet jedoch eine vollständige Automatisierung für Backup-, Restore- und Klonprozesse. Außerdem wird eine Erkennung durchgeführt, um sicherzustellen, dass die richtigen Snapshots erstellt werden.

## Disaster Recovery

### Disaster Recovery

Enterprise-Datenbanken und Applikationsinfrastrukturen erfordern oft Replizierung zum Schutz vor Naturkatastrophen oder unerwarteten Geschäftsunterbrechungen mit minimaler Ausfallzeit.

Die SQL Server Funktion zur Replizierung von Always-on-Fähigkeitsgruppen kann sich als hervorragende Option anbieten. NetApp bietet Optionen zur Integration von Datensicherung mit Always-on. In einigen Fällen empfiehlt es sich jedoch, die ONTAP Replizierungstechnologie mit den folgenden Optionen in Betracht zu ziehen.

### SnapMirror

Die SnapMirror-Technologie bietet eine schnelle und flexible Unternehmenslösung zur Replizierung von Daten über LANs und WANs. Die SnapMirror Technologie überträgt nach Erstellung der ersten Spiegelung nur geänderte Datenblöcke an das Zielsystem, wodurch die Anforderungen an die Netzwerkbänder erheblich gesenkt werden. Sie kann im synchronen oder asynchronen Modus konfiguriert werden. Die synchrone SnapMirror Replizierung in NetApp ASA wird mit dem SnapMirror Active Sync konfiguriert.

### SnapMirror Active Sync

Für viele Kunden ist für Business Continuity nicht nur ein Remote-Besitz einer Datenkopie erforderlich, sondern es muss die Möglichkeit bestehen, diese Daten schnell zu nutzen, die in NetApp ONTAP mithilfe von SnapMirror Active Sync möglich sind.

Bei SnapMirror Active Sync haben Sie im Grunde zwei verschiedene ONTAP-Systeme, die unabhängige Kopien Ihrer LUN-Daten führen, aber zusammenarbeiten, um eine einzige Instanz dieser LUN zu präsentieren. Auf Host-Ebene handelt es sich um eine einzelne LUN-Einheit. SnapMirror Active Sync wird für iSCSI/FC-basierte LUNs unterstützt.

SnapMirror Active Sync bietet RPO=0-Replizierung und ist einfach zwischen zwei unabhängigen Clustern zu

implementieren. Sind die beiden Datenkopien synchron, müssen die beiden Cluster nur noch Schreibvorgänge spiegeln. Wenn ein Schreibvorgang auf einem Cluster stattfindet, wird er in das andere Cluster repliziert. Der Schreibvorgang wird dem Host nur dann bestätigt, wenn der Schreibvorgang auf beiden Seiten abgeschlossen ist. Anders als dieses Verhalten bei der Protokollaufteilung sind die beiden Cluster ansonsten normale ONTAP-Cluster.

Ein wichtiger Anwendungsfall für SM-AS ist die granulare Replizierung. Manchmal möchten Sie nicht alle Daten als eine Einheit replizieren oder bestimmte Workloads selektiv ausfallsicher durchführen.

Ein weiterer wichtiger Anwendungsfall für SM-As ist der aktiv/aktiv-Betrieb. Dort sollen vollständig nutzbare Datenkopien auf zwei verschiedenen Clustern verfügbar sein, die sich an zwei verschiedenen Standorten mit identischen Performance-Merkmalen befinden und auf Wunsch nicht über Standorte verteilt werden müssen. Sie können Ihre Applikationen, die bereits auf beiden Standorten ausgeführt werden, sofern die Applikation unterstützt wird, wodurch sich die RTO während eines Failover verringert.

## SnapMirror

Nachfolgend finden Sie Empfehlungen für SnapMirror für SQL Server:

- Nutzung der synchronen Replizierung mit SnapMirror Active Sync für höhere Anforderungen an eine schnelle Datenwiederherstellung und asynchrone Lösungen für Flexibilität bei RPO
- Wenn Sie SnapCenter zum Sichern von Datenbanken und zum Replizieren von Snapshots auf Remote-Cluster verwenden, planen Sie aus Konsistenzgründen keine SnapMirror-Updates von den Controllern. Stattdessen sollten Sie SnapMirror Updates von SnapCenter aktivieren, um SnapMirror zu aktualisieren, nachdem ein vollständiger Backup oder ein Protokoll-Backup abgeschlossen wurde.
- Gleichen Sie die Speichereinheiten aus, die SQL Server-Daten enthalten, über verschiedene Knoten im Cluster aus, damit alle Clusterknoten SnapMirror-Replikationsaktivitäten gemeinsam nutzen können. Diese Verteilung optimiert die Nutzung von Knotenressourcen.

Weitere Informationen zu SnapMirror finden Sie unter "["TR-4015: SnapMirror Konfigurations- und Best Practices-Leitfaden für ONTAP 9"](#).

## SnapMirror Active Sync

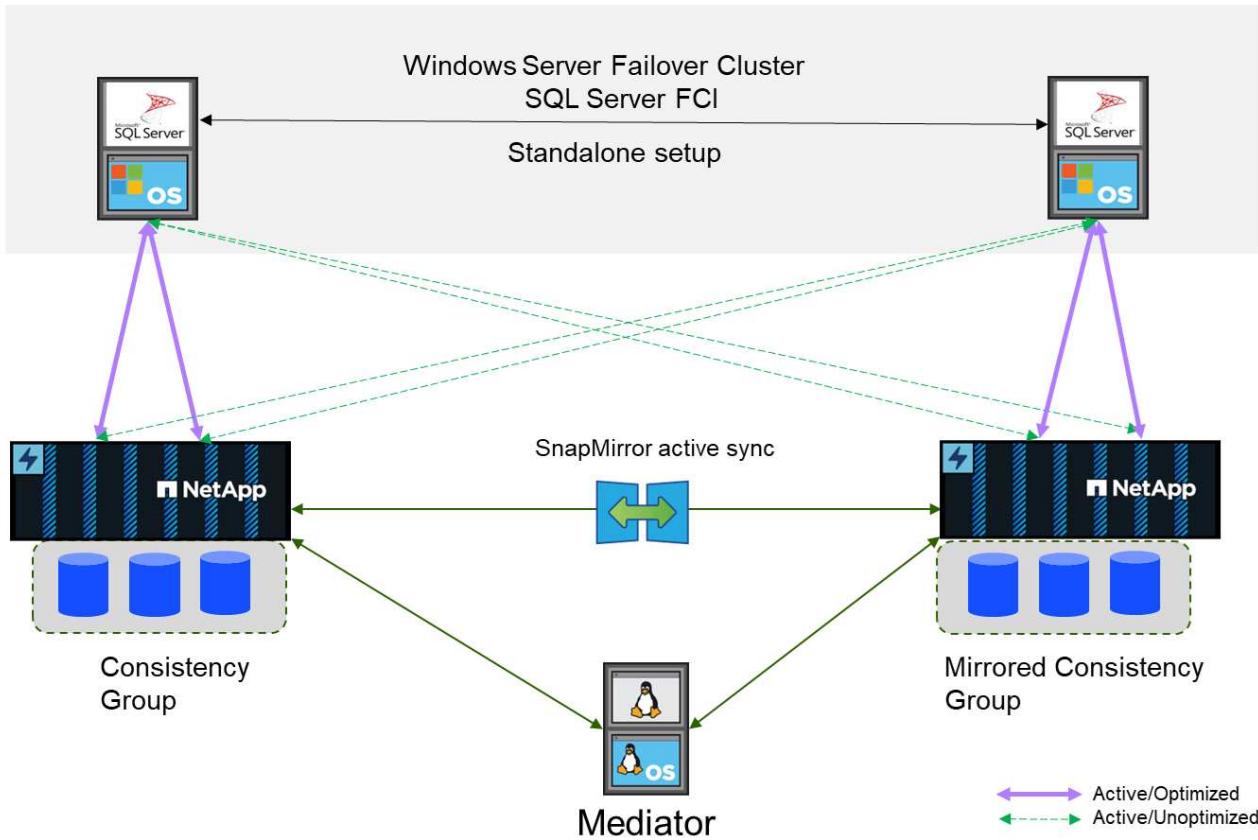
### Überblick

Mit SnapMirror Active Sync können einzelne SQL Server-Datenbanken und -Applikationen bei Storage- und Netzwerkstörungen den Betrieb fortsetzen. Der Storage Failover ist transparent, ohne dass manuelle Eingriffe erforderlich sind.

SnapMirror Active Sync unterstützt die symmetrische aktiv/aktiv-Architektur, die eine synchrone bidirektionale Replizierung für Business Continuity und Disaster Recovery bietet. Es hilft Ihnen, Ihren Datenzugriff für kritische SAN-Workloads durch gleichzeitigen Lese- und Schreibzugriff auf Daten über mehrere Ausfall-Domains hinweg zu schützen. So wird ein unterbrechungsfreier Betrieb sichergestellt und Ausfallzeiten bei Notfällen oder Systemausfällen werden minimiert.

SQL-Server-Hosts greifen über Fibre Channel(FC)- oder iSCSI-LUNs auf Speicher zu. Replizierung zwischen jedem Cluster, das eine Kopie der replizierten Daten hostet. Da es sich bei dieser Funktion um die Replizierung auf Storage-Ebene handelt, können SQL Server-Instanzen auf eigenständigen Host- oder Failover-Cluster-Instanzen Lese-/Schreibvorgänge durchführen. Informationen zu Planungs- und Konfigurationsschritten finden Sie unter "["ONTAP-Dokumentation über SnapMirror Active Sync"](#) .

## Architektur von SnapMirror aktiv mit symmetrischer aktiv/aktiv-Lösung



## Synchrone Replikation

Im normalen Betrieb ist jede Kopie jederzeit ein synchrones RPO=0-Replikat, mit einer Ausnahme. Wenn Daten nicht repliziert werden können, gibt ONTAP die Notwendigkeit zur Replizierung von Daten frei und stellt die E/A-Bereitstellung an einem Standort wieder her, während die LUNs am anderen Standort offline geschaltet werden.

## Storage Hardware

Im Gegensatz zu anderen Disaster Recovery-Lösungen für Storage bietet SnapMirror Active Sync asymmetrische Plattformflexibilität. Die Hardware an den einzelnen Standorten muss nicht identisch sein. Dank dieser Funktion können Sie die Größe der Hardware anpassen, die zur Unterstützung der SnapMirror Active Sync verwendet wird. Das Remote-Storage-System kann identisch mit dem primären Standort sein, wenn es einen vollständigen Produktions-Workload unterstützen muss. Wenn jedoch ein Ausfall zu einer Verringerung der I/O führt, könnte ein kleineres System am Remote-Standort kostengünstiger sein.

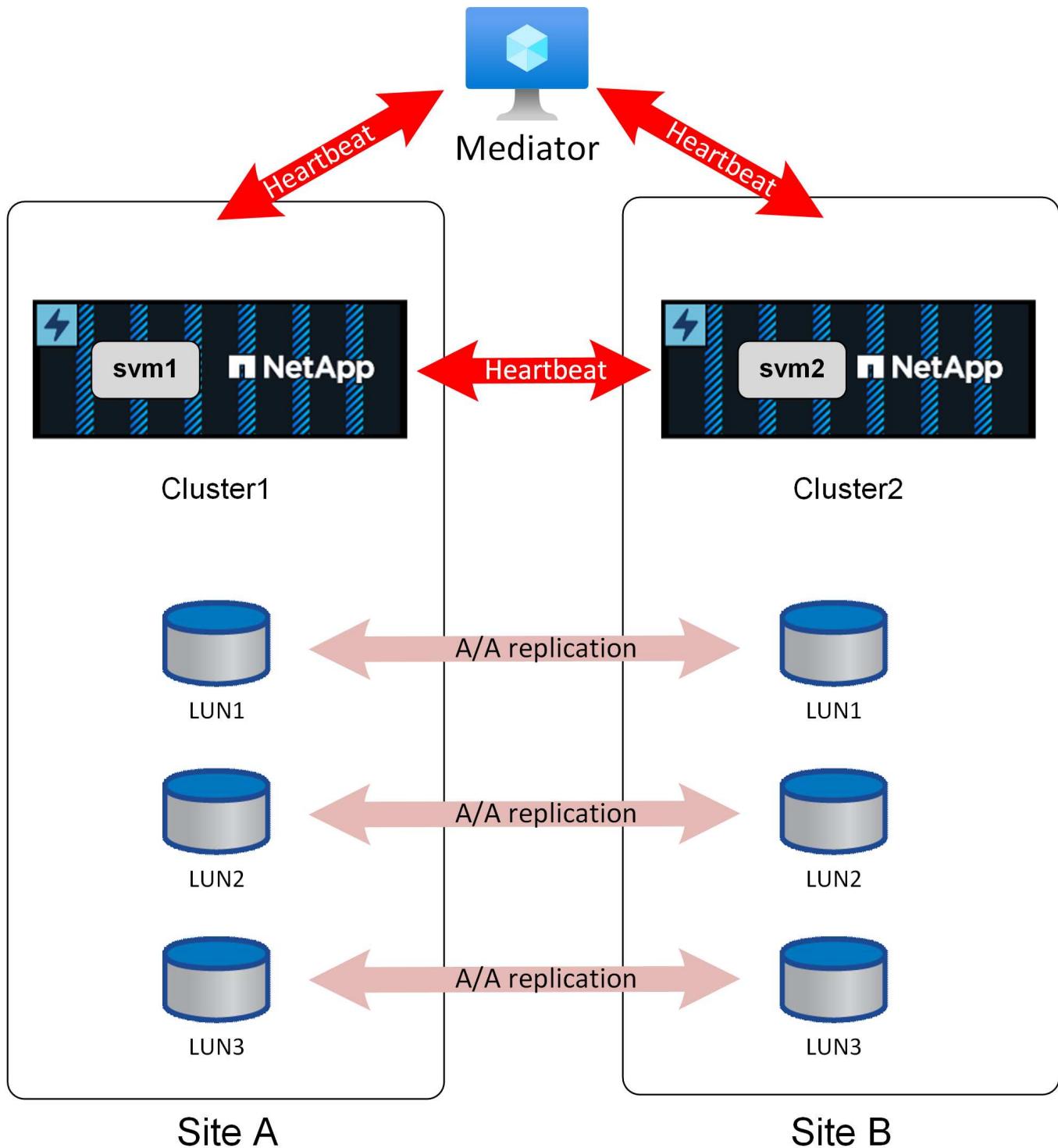
## ONTAP Mediator

Der ONTAP Mediator ist eine Softwareanwendung, die von der NetApp-Unterstützung heruntergeladen wird und normalerweise auf einer kleinen virtuellen Maschine bereitgestellt wird. Der ONTAP Mediator ist kein Tiebreak. Es handelt sich um einen alternativen Kommunikationskanal für die beiden Cluster, die an der aktiven synchronen SnapMirror-Replikation beteiligt sind. Der automatisierte Betrieb wird durch ONTAP basierend auf den Antworten gesteuert, die der Partner über direkte Verbindungen und den Mediator erhält.

## **ONTAP Mediator**

Der Mediator ist für die sichere Automatisierung des Failover erforderlich. Idealerweise würde er an einem unabhängigen dritten Standort platziert werden, kann aber dennoch für die meisten Anforderungen funktionieren, wenn er mit einem der an der Replikation beteiligten Cluster kolokiert wird.

Der Mediator ist nicht wirklich ein Tiebreak, obwohl das ist effektiv die Funktion, die es bietet. Er führt keine Aktionen durch. Stattdessen stellt er einen alternativen Kommunikationskanal für die Kommunikation zwischen Cluster und Cluster bereit.



Die #1 Herausforderung mit automatisiertem Failover ist das Split-Brain-Problem, und dieses Problem tritt auf, wenn Ihre zwei Standorte die Verbindung miteinander verlieren. Was soll geschehen? Sie möchten nicht, dass sich zwei verschiedene Standorte als verbleibende Kopien der Daten bezeichnen, aber wie kann ein einzelner Standort den Unterschied zwischen dem tatsächlichen Verlust des anderen Standorts und der Unfähigkeit, mit dem gegenüberliegenden Standort zu kommunizieren, erkennen?

Hier betritt der Mediator das Bild. Wenn jeder Standort an einem dritten Standort platziert wird und über eine separate Netzwerkverbindung zu diesem Standort verfügt, haben Sie für jeden Standort einen zusätzlichen Pfad, um den Zustand des anderen zu überprüfen. Sehen Sie sich das Bild oben noch einmal an und

betrachten Sie die folgenden Szenarien.

- Was passiert, wenn der Mediator ausfällt oder von einem oder beiden Standorten nicht erreichbar ist?
  - Die beiden Cluster können weiterhin über dieselbe Verbindung miteinander kommunizieren, die für Replikationsdienste verwendet wird.
  - Für die Daten wird noch eine RPO=0-Sicherung verwendet
- Was passiert, wenn Standort A ausfällt?
  - An Standort B sehen Sie, dass beide Kommunikationskanäle ausgefallen sind.
  - Standort B übernimmt die Datenservices, jedoch ohne RPO=0-Spiegelung
- Was passiert, wenn Standort B ausfällt?
  - An Standort A sehen Sie, dass beide Kommunikationskanäle ausgefallen sind.
  - Standort A übernimmt die Datenservices, aber ohne RPO=0-Spiegelung

Es gibt ein anderes Szenario zu berücksichtigen: Verlust der Datenreplikationsverbindung. Wenn die Replikationsverbindung zwischen Standorten verloren geht, wird eine RPO=0-Spiegelung offensichtlich unmöglich sein. Was soll dann geschehen?

Dies wird durch den bevorzugten Standortstatus gesteuert. In einer SM-AS-Beziehung ist einer der Standorte zweitrangig zum anderen. Dies hat keine Auswirkungen auf den normalen Betrieb, und der gesamte Datenzugriff ist symmetrisch. Wenn die Replikation jedoch unterbrochen wird, muss die Verbindung unterbrochen werden, um den Betrieb wieder aufzunehmen. Das Ergebnis: Der bevorzugte Standort setzt den Betrieb ohne Spiegelung fort und der sekundäre Standort hält die I/O-Verarbeitung an, bis die Replizierungskommunikation wiederhergestellt ist.

#### **Bevorzugter Standort**

Das aktive Synchronisierungsverhalten von SnapMirror ist symmetrisch, mit einer wichtigen Ausnahme: Konfiguration des bevorzugten Standorts.

SnapMirror Active Sync betrachtet einen Standort als „Quelle“ und den anderen als „Ziel“. Dies impliziert eine One-Way-Replikationsbeziehung, aber dies gilt nicht für das IO-Verhalten. Die Replizierung ist bidirektional und symmetrisch, und die I/O-Reaktionszeiten sind auf beiden Seiten der Spiegelung identisch.

Die `source` Bezeichnung steuert den bevorzugten Standort. Wenn die Replizierungsverbindung verloren geht, stellen die LUN-Pfade auf der Quellkopie weiterhin Daten bereit, während die LUN-Pfade auf der Zielkopie erst dann wieder verfügbar sind, wenn die Replikation wiederhergestellt ist und SnapMirror wieder in den synchronen Zustand wechselt. Die Pfade setzen dann das Bereitstellen von Daten fort.

Die Sourcing/Ziel-Konfiguration kann über Systemmanager angezeigt werden:

## Relationships

The screenshot shows a 'Relationships' page with tabs for 'Local destinations' and 'Local sources'. The 'Local destinations' tab is selected. At the top, there are search, download, show/hide, and filter buttons. Below is a table with columns: Source, Destination, and Policy type. One row is visible, showing a relationship between 'jfs\_as1:/cg/jfsAA' and 'jfs\_as2:/cg/jfsAA' with a 'Synchronous' policy type.

Source	Destination	Policy type
jfs_as1:/cg/jfsAA	jfs_as2:/cg/jfsAA	Synchronous

Oder über die CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

          Source Path: jfs_as1:/cg/jfsAA
          Destination Path: jfs_as2:/cg/jfsAA
          Relationship Type: XDP
          Relationship Group Type: consistencygroup
          SnapMirror Schedule: -
          SnapMirror Policy Type: automated-failover-duplex
          SnapMirror Policy: AutomatedFailOverDuplex
          Tries Limit: -
          Throttle (KB/sec): -
          Mirror State: Snapmirrored
          Relationship Status: InSync
```

Der Schlüssel ist, dass die Quelle die SVM für Cluster1 ist. Wie oben erwähnt, beschreiben die Begriffe „Quelle“ und „Ziel“ nicht den Fluss replizierter Daten. Beide Standorte können einen Schreibvorgang verarbeiten und am anderen Standort replizieren. Beide Cluster sind Quellen und Ziele. Der Effekt der Festlegung eines Clusters als Quelle steuert einfach, welches Cluster als Lese-/Schreib-Speichersystem überlebt, wenn die Replikationsverbindung verloren geht.

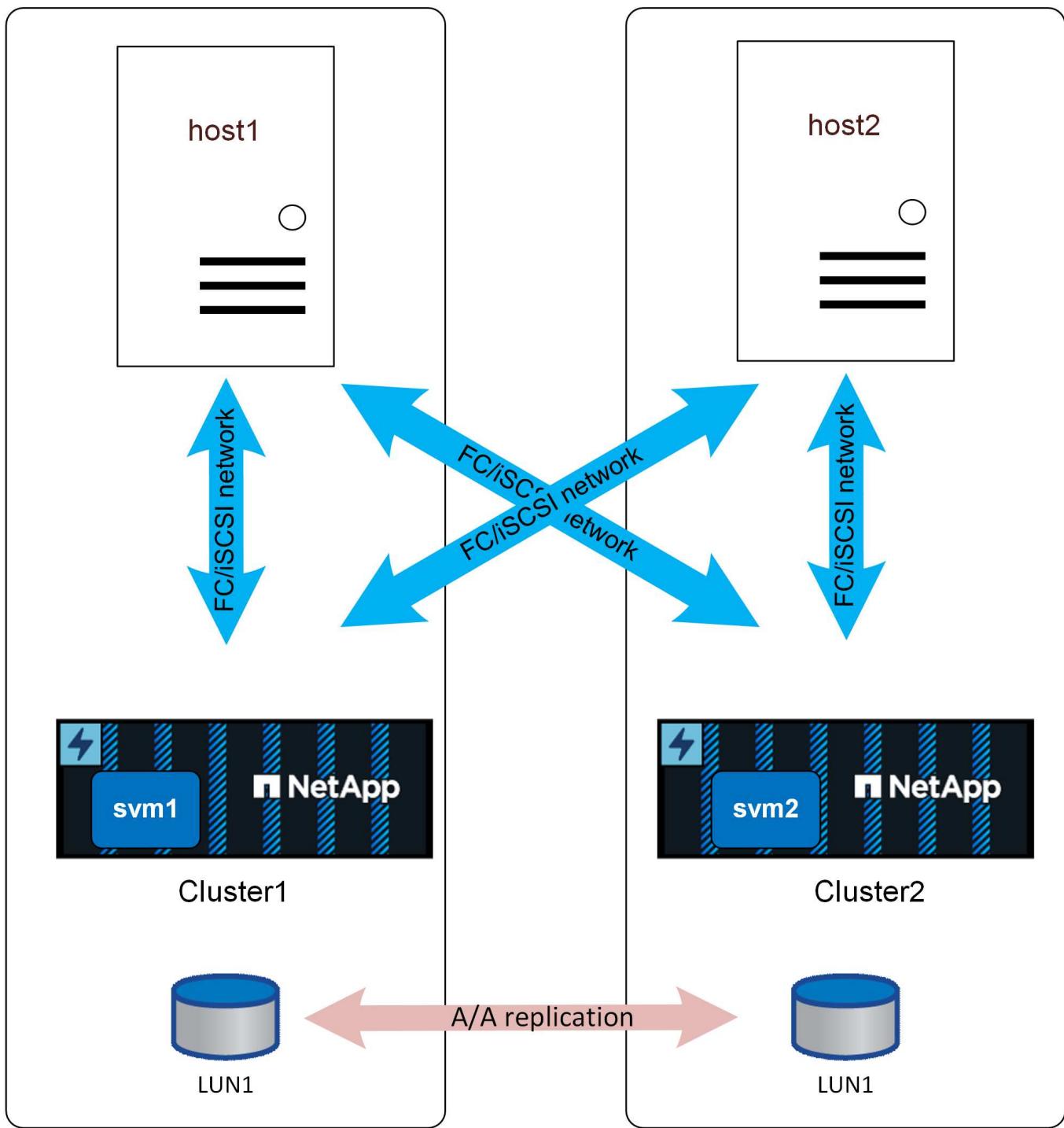
### Netzwerktopologie

#### Einheitlicher Zugriff

Ein einheitliches Netzwerk für den Zugriff bedeutet, dass Hosts auf Pfade auf beiden Seiten (oder auf Ausfall-Domains innerhalb desselben Standorts) zugreifen können.

Eine wichtige Funktion von SM-AS ist die Möglichkeit, die Speichersysteme so zu konfigurieren, dass sie wissen, wo sich die Hosts befinden. Wenn Sie die LUNs einem bestimmten Host zuordnen, können Sie angeben, ob sie einem bestimmten Storage-System proximal sind oder nicht.

NetApp ASA Systeme bieten aktiv/aktiv-Multipathing über alle Pfade eines Clusters hinweg. Dies gilt auch für SM-AS Konfigurationen.



## Active/Optimized Path

Bei einheitlichem Zugriff würde IO das WAN überqueren. Es handelt sich dabei um ein vollständig vernetztes Mesh-Cluster, das für alle Anwendungsfälle wünschenswert sein kann oder auch nicht.

Wenn die beiden Standorte mit Glasfaserverbindung 100 Meter voneinander entfernt wären, sollte keine erkennbare zusätzliche Latenz über das WAN entstehen. Wenn jedoch die Standorte weit voneinander entfernt

wären, würde die Performance beim Lesen an beiden Standorten darunter leiden. ASA mit einem nicht einheitlichen Zugriffsnetzwerk wäre eine Option, um die Kosten- und Funktionsvorteile von ASA ohne Beeinträchtigung des standortübergreifenden Latenzzugriffs zu nutzen oder die Host-Proximity-Funktion zu verwenden, um standortübergreifenden Lese-/Schreibzugriff für beide Standorte zu ermöglichen.

ASA mit SM-AS in einer Konfiguration mit niedriger Latenz bietet zwei interessante Vorteile. Zunächst verdoppelt es die Performance bei jedem einzelnen Host \*, da IO von doppelt so vielen Controllern mit doppelt so vielen Pfaden gewartet werden kann. Zweitens bietet er in einer Umgebung mit einem einzigen Standort eine extreme Verfügbarkeit, da ein komplettes Storage-System ohne Unterbrechung des Host-Zugriffs verloren gehen könnte.

## Annäherungseinstellungen

Proximity bezieht sich auf eine Clusterkonfiguration, die angibt, dass eine bestimmte Host-WWN- oder iSCSI-Initiator-ID zu einem lokalen Host gehört. Dies ist ein zweiter optionaler Schritt für die Konfiguration des LUN-Zugriffs.

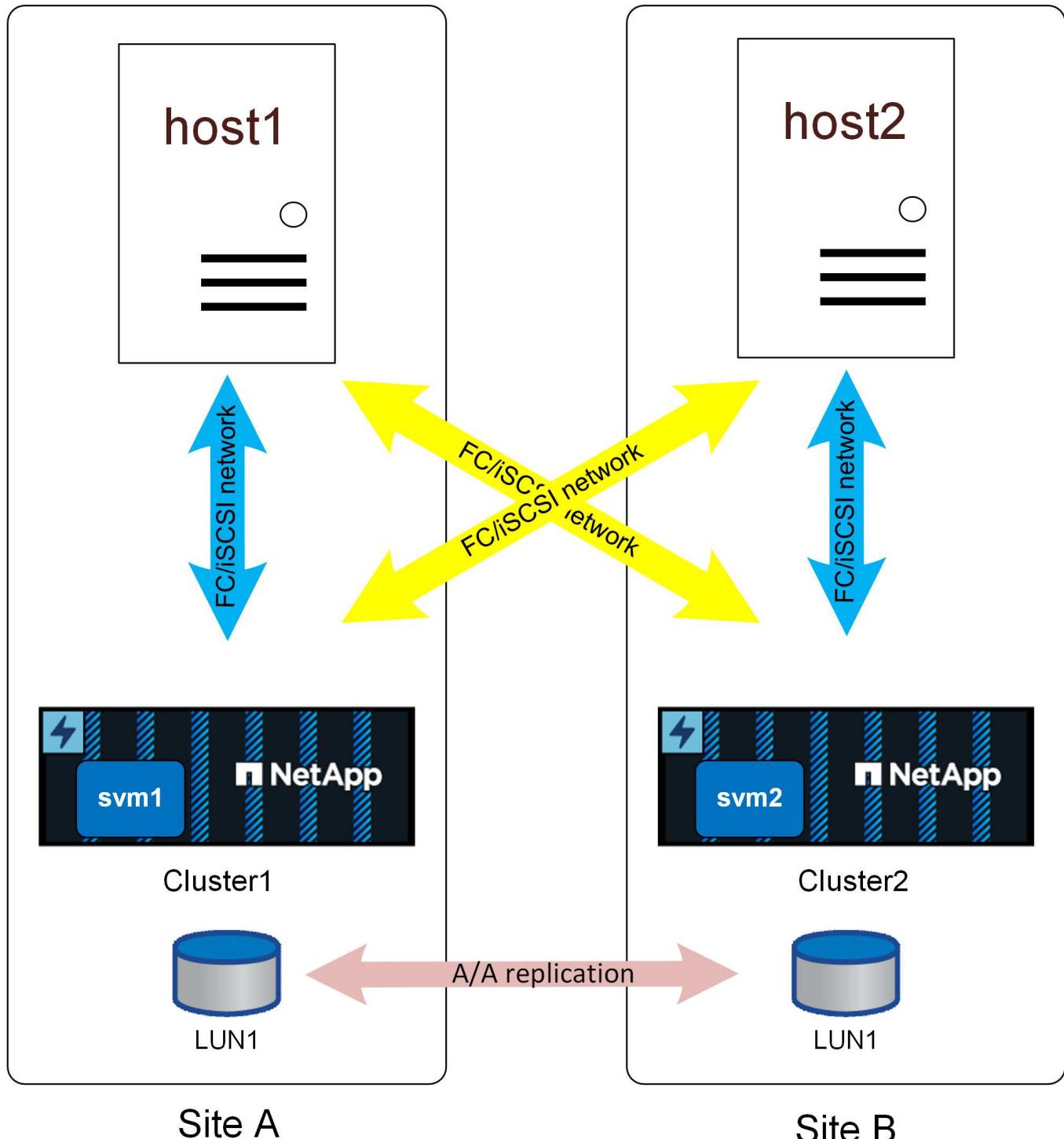
Der erste Schritt ist die übliche igroup-Konfiguration. Jede LUN muss einer Initiatorgruppe zugeordnet werden, die die WWN/iSCSI-IDs der Hosts enthält, die Zugriff auf diese LUN benötigen. Dadurch wird gesteuert, welcher Host Access zu einer LUN hat.

Der zweite, optionale Schritt ist die Konfiguration der Host-Nähe. Dies kontrolliert nicht den Zugriff, es steuert *Priority*.

Beispielsweise kann ein Host an Standort A für den Zugriff auf eine LUN konfiguriert werden, die durch SnapMirror Active Sync geschützt ist. Da das SAN über Standorte erweitert wird, stehen diesem LUN Pfade über Storage an Standort A oder Storage an Standort B zur Verfügung

Ohne Annäherungseinstellungen verwendet der Host beide Speichersysteme gleichmäßig, da beide Speichersysteme aktive/optimierte Pfade anbieten. Wenn die SAN-Latenz und/oder Bandbreite zwischen Standorten begrenzt ist, ist dies möglicherweise nicht erwünscht, und Sie sollten sicherstellen, dass während des normalen Betriebs jeder Host bevorzugt Pfade zum lokalen Speichersystem verwendet. Diese Konfiguration erfolgt durch Hinzufügen der Host-WWN/iSCSI-ID zum lokalen Cluster als proximaler Host. Dies kann unter der CLI oder Systemmanager ausgeführt werden.

Wenn die Host-Nähe konfiguriert wurde, werden die Pfade wie unten dargestellt angezeigt.

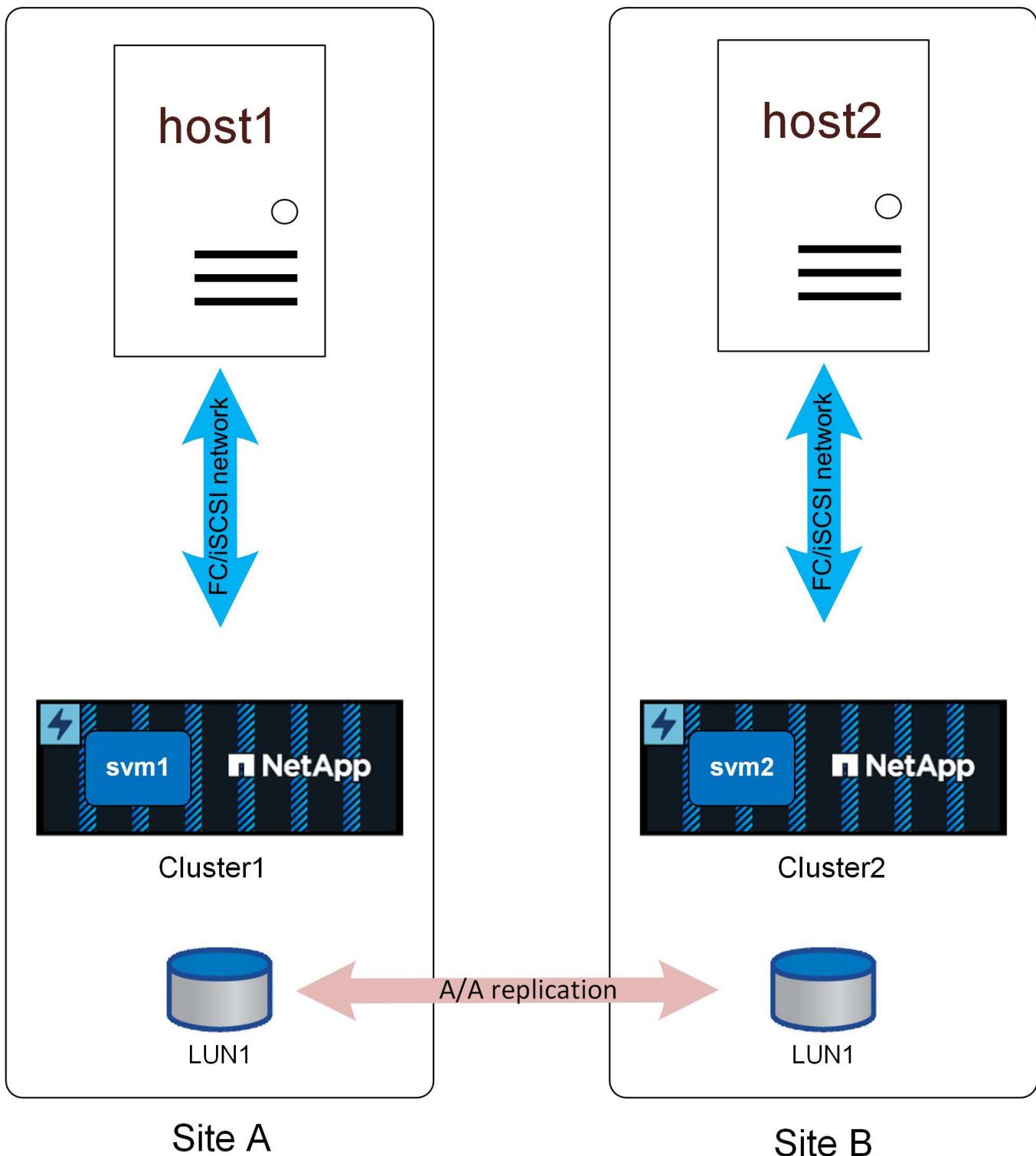


Active/Optimized Path

Active Path

### **Uneinheitlicher Zugriff**

Uneinheitliches Netzwerk durch Zugriff bedeutet, dass jeder Host nur Zugriff auf Ports im lokalen Storage-System hat. Das SAN wird nicht über Standorte (oder Ausfall-Domains am selben Standort) erweitert.



## Active/Optimized Path

Der Hauptvorteil dieses Ansatzes ist die SAN-Einfachheit – Sie müssen kein SAN mehr über das Netzwerk erweitern. Einige Kunden verfügen nicht über eine Konnektivität mit niedriger Latenz zwischen den Standorten und haben nicht die Infrastruktur, um den FC SAN-Datenverkehr über ein standortverbundenes Netzwerk zu Tunneln.

Der Nachteil eines uneinheitlichen Zugriffs besteht darin, dass bestimmte Ausfallszenarien, einschließlich des Verlusts der Replikationsverbindung, dazu führen, dass einige Hosts den Zugriff auf den Speicher verlieren. Applikationen, die als einzelne Instanzen ausgeführt werden, wie z. B. eine Datenbank ohne Cluster, die grundsätzlich nur auf einem einzelnen Host bei einem beliebigen Mount ausgeführt wird, würden ausfallen, wenn die lokale Storage-Konnektivität verloren geht. Die Daten bleiben zwar weiterhin geschützt, aber der Datenbankserver würde nicht mehr darauf zugreifen können. Es müsste an einem Remote-Standort neu gestartet werden, vorzugsweise durch einen automatisierten Prozess. VMware HA kann beispielsweise eine heruntergefahrenen Pfade auf einem Server erkennen und eine VM auf einem anderen Server neu starten, auf dem Pfade verfügbar sind.

Im Gegensatz dazu kann eine Cluster-Anwendung wie Oracle RAC einen Service bereitstellen, der gleichzeitig an zwei verschiedenen Standorten verfügbar ist. Der Verlust einer Website bedeutet nicht, dass der Anwendungsdienst als Ganzes verloren geht. Instanzen sind nach wie vor verfügbar und werden am verbleibenden Standort ausgeführt.

In vielen Fällen wäre die zusätzliche Latenz, wenn eine Applikation, die auf den Storage über eine Site-to-Site-Verbindung zugreift, nicht akzeptabel. Dies bedeutet, dass die verbesserte Verfügbarkeit von einheitlichem Netzwerk minimal ist, da der Verlust von Speicher an einem Standort dazu führen würde, dass die Dienste auf diesem ausgesetzten Standort sowieso heruntergefahren werden müssen.

Es gibt redundante Pfade durch den lokalen Cluster, die aus Gründen der Einfachheit nicht auf diesen Diagrammen angezeigt werden. ONTAP Storage-Systeme sind HA selbst, daher sollte ein Controller-Ausfall nicht zu einem Standortausfall führen. Es sollte lediglich zu einer Änderung führen, in der lokale Pfade auf dem betroffenen Standort verwendet werden.

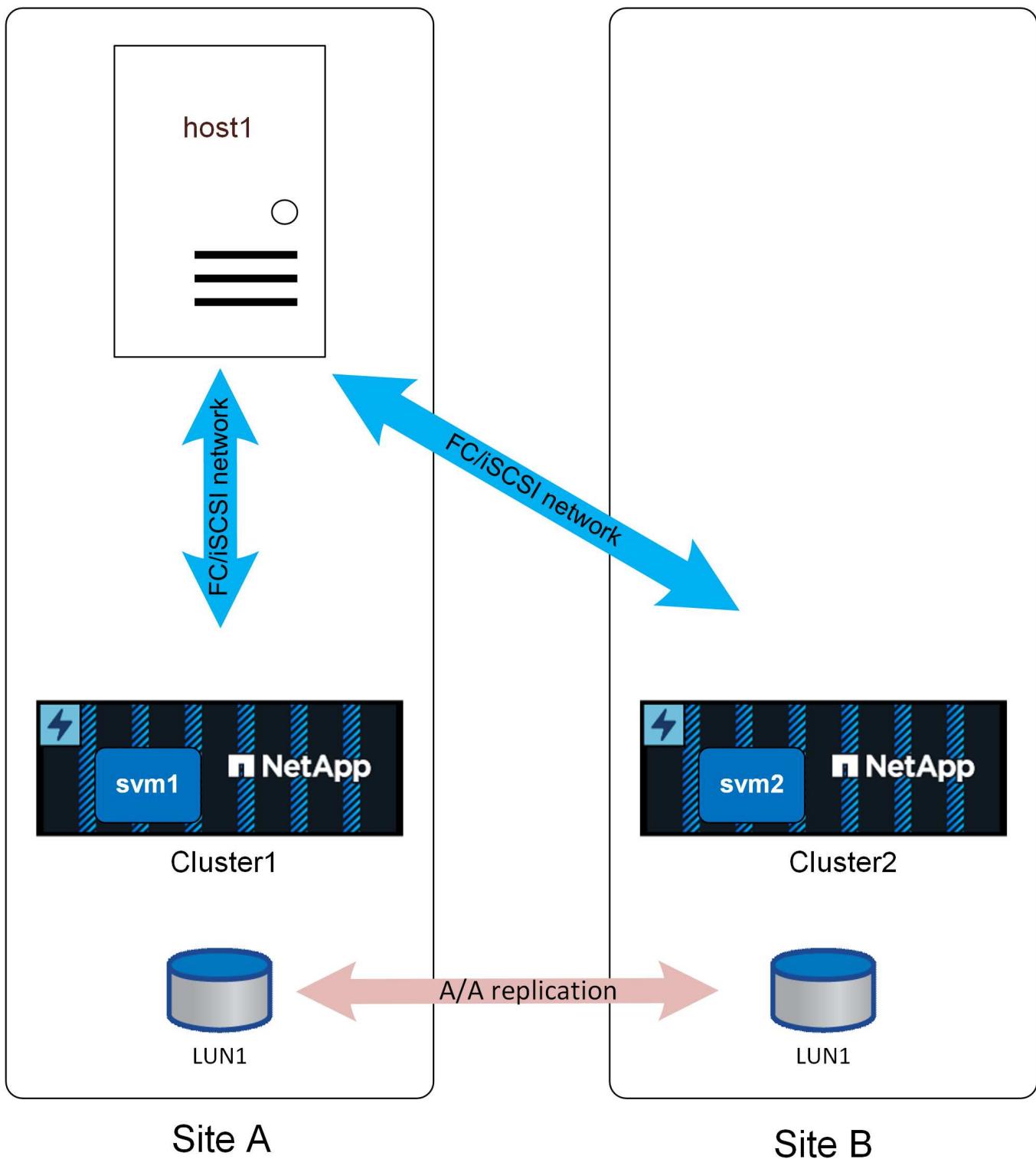
## Überblick

SQL Server kann so konfiguriert werden, dass er auf verschiedene Weise mit SnapMirror Active Sync arbeitet. Die richtige Antwort hängt von der verfügbaren Netzwerkkonnectivität, den RPO-Anforderungen und den Verfügbarkeitsanforderungen ab.

### Eigenständige Instanz von SQL Server

Die Best Practices für das Datei-Layout und die Serverkonfiguration sind dieselben, wie in der Dokumentation empfohlen "[SQL Server auf ONTAP](#)".

Mit einer eigenständigen Einrichtung konnte SQL Server nur an einem Standort ausgeführt werden. Vermutlich "[Einheitlich](#)" würde der Zugriff genutzt werden.



Bei einem einheitlichen Zugriff würde ein Storage-Ausfall an einem der Standorte den Datenbankbetrieb nicht unterbrechen. Ein kompletter Standortausfall am Standort, der den Datenbankserver einschloss, würde natürlich zu einem Ausfall führen.

Einige Kunden konnten ein Betriebssystem konfigurieren, das am Remote-Standort mit einem vorkonfigurierten SQL Server-Setup ausgeführt wird, das mit einer gleichwertigen Build-Version wie die der Produktionsinstanz aktualisiert wurde. Bei einem Failover müsste die eigenständige Instanz von SQL Server am alternativen Standort aktiviert, die LUNS ermittelt und die Datenbank gestartet werden. Der vollständige

Prozess kann mit dem Cmdlet "Windows PowerShell" automatisiert werden, da Storage-seitig kein Betrieb erforderlich ist.

"Uneinheitlich" Zugriff könnte auch verwendet werden, aber das Ergebnis wäre ein Datenbankausfall, wenn das Storage-System, in dem der Datenbankserver lokalisiert war, ausgefallen wäre, da die Datenbank keine Pfade zum Storage hätte. Dies kann in einigen Fällen noch akzeptabel sein. SnapMirror Active Sync bietet weiterhin RPO=0-Datensicherheit. Im Falle eines Standortausfalls wäre die noch verbleibende Kopie aktiv und bereit, den Betrieb mit demselben Verfahren wie oben beschrieben fortzusetzen.

Ein einfacher, automatisierter Failover-Prozess lässt sich mit der Verwendung eines virtuellen Hosts leichter konfigurieren. Wenn beispielsweise SQL Server-Datendateien zusammen mit einer Boot-VMDK synchron auf den sekundären Storage repliziert werden, könnte im Notfall die gesamte Umgebung am alternativen Standort aktiviert werden. Ein Administrator kann den Host am verbleibenden Standort entweder manuell aktivieren oder den Prozess über einen Service wie VMware HA automatisieren.

## **SQL Server Failover-Cluster-Instanz**

SQL Server Failover-Instanzen können auch auf einem Windows Failover Cluster gehostet werden, der auf einem physischen Server oder einem virtuellen Server als Gastbetriebssystem läuft. Diese Architektur mit mehreren Hosts bietet SQL Server Instanzen und Storage Resiliency. Diese Implementierung ist besonders in anspruchsvollen Umgebungen hilfreich, die robuste Failover-Prozesse suchen und gleichzeitig eine verbesserte Performance beibehalten. Wenn bei einem Failover-Cluster-Setup ein Host oder primärer Speicher betroffen ist, erfolgt ein Failover von SQL Services auf den sekundären Host, und gleichzeitig steht der sekundäre Speicher zur Verfügung, um IO bereitzustellen. Es sind kein Automatisierungsskript und keine Eingriffe durch den Administrator erforderlich.

### **Ausfallszenarien**

Die Planung einer vollständigen Applikationsarchitektur für die aktive Synchronisierung von SnapMirror erfordert ein Verständnis dafür, wie SM-AS in verschiedenen geplanten und ungeplanten Failover-Szenarien reagiert.

In den folgenden Beispielen wird davon ausgegangen, dass Standort A als bevorzugter Standort konfiguriert ist.

### **Verlust der Replikationskonnektivität**

Wenn die SM-AS-Replikation unterbrochen wird, kann die Schreib-I/O nicht abgeschlossen werden, da ein Cluster Änderungen nicht auf den anderen Standort replizieren kann.

### **Standort A (bevorzugte Website)**

Das Ergebnis eines Ausfalls der Replikationsverbindung auf dem bevorzugten Standort ist eine ca. 15-Sekunden-Pause bei der Schreib-I/O-Verarbeitung, da ONTAP erneut replizierte Schreibvorgänge versucht, bevor festgestellt wird, dass die Replikationsverbindung wirklich nicht erreichbar ist. Nach 15 Sekunden wird die I/O-Verarbeitung von Lese- und Schreibzugriffen von Standort A fortgesetzt. Die SAN-Pfade ändern sich nicht, und die LUNs bleiben online.

### **Standort B**

Da Standort B nicht der bevorzugte Standort für SnapMirror Active Sync ist, sind die LUN-Pfade nach ca. 15 Sekunden nicht mehr verfügbar.

## Ausfall des Storage-Systems

Das Ergebnis eines Storage-Systemausfalls ist nahezu identisch mit dem Ergebnis des Verlusts der Replizierungsverbindung. Am überlebenden Standort sollte eine I/O-Pause von etwa 15 Sekunden stattfinden. Nach Ablauf dieses Zeitraums von 15 Sekunden wird die E/A-Vorgänge wie gewohnt an diesem Standort fortgesetzt.

## Verlust des Mediators

Der Mediator hat keine direkte Kontrolle über Storage-Vorgänge. Er fungiert als alternativer Kontrollpfad zwischen Clustern. Die Lösung bietet insbesondere automatisierte Failover-Prozesse ohne Split-Brain-Szenario. Im normalen Betrieb repliziert jedes Cluster Änderungen an seinem Partner. Daher kann jedes Cluster überprüfen, ob das Partner-Cluster online ist und Daten bereitstellt. Wenn die Replikationsverbindung fehlschlägt, wird die Replikation beendet.

Der Grund für einen sicheren automatisierten Failover ist der Mediator, der darauf zurückzuführen ist, dass ein Storage-Cluster andernfalls nicht feststellen kann, ob der Ausfall einer bidirektionalen Kommunikation auf einen Netzwerkausfall oder einen tatsächlichen Storage-Ausfall zurückzuführen ist.

Der Mediator bietet jedem Cluster einen alternativen Pfad zur Überprüfung des Integrität seines Partners. Die Szenarien sind wie folgt:

- Wenn ein Cluster seinen Partner direkt kontaktieren kann, sind die Replizierungsservices betriebsbereit. Keine Aktion erforderlich.
- Wenn ein bevorzugter Standort nicht direkt mit dem Partner oder über den Mediator in Kontakt treten kann, wird davon ausgegangen, dass der Partner entweder tatsächlich nicht verfügbar ist oder isoliert wurde und seine LUN-Pfade offline geschaltet hat. Der bevorzugte Standort setzt dann den Status RPO=0 frei und setzt die Verarbeitung von Lese- und Schreib-I/O fort.
- Wenn ein nicht bevorzugter Standort seinen Partner nicht direkt kontaktieren kann, ihn aber über den Mediator kontaktieren kann, nimmt er seine Pfade offline und wartet auf die Rückkehr der Replikationsverbindung.
- Wenn ein nicht bevorzugter Standort keine direkte Kontaktaufnahme mit dem Partner oder über einen betrieblichen Mediator bietet, nimmt er an, dass der Partner entweder tatsächlich nicht verfügbar ist oder isoliert war und seine LUN-Pfade offline geschaltet hat. Der nicht bevorzugte Standort setzt dann den Status RPO=0 frei und verarbeitet sowohl Lese- als auch Schreib-I/O weiter. Er übernimmt die Rolle der Replikationsquelle und wird der neue bevorzugte Standort.

Wenn der Mediator vollständig nicht verfügbar ist:

- Wenn keine Replizierungsservices aus irgendeinem Grund verfügbar sind, beispielsweise der Ausfall des nicht bevorzugten Standorts oder des Storage-Systems, wird der bevorzugte Standort den Zustand RPO=0 freigeben und die I/O-Verarbeitung für Lese- und Schreibvorgänge wird wieder aufgenommen. Der nicht bevorzugte Standort nimmt seine Pfade offline.
- Ein Ausfall des bevorzugten Standorts führt zu einem Ausfall, da der nicht bevorzugte Standort nicht verifizieren kann, dass der gegenteilige Standort wirklich offline ist. Daher ist es für den nicht bevorzugten Standort nicht sicher, die Services wieder aufzunehmen.

## Dienste werden wiederhergestellt

Wenn ein Fehler behoben wurde, wie z. B. die Wiederherstellung der Site-to-Site-Verbindung oder das Einschalten eines ausgefallenen Systems, erkennen die SnapMirror Active Sync-Endpunkte automatisch, dass eine fehlerhafte Replikationsbeziehung vorhanden ist, und versetzen sie wieder in den Zustand RPO=0. Sobald die synchrone Replizierung wiederhergestellt ist, werden die fehlerhaften Pfade wieder online

geschaltet.

In vielen Fällen erkennen Cluster-Applikationen automatisch die Rückgabe ausgefallener Pfade, und diese Applikationen sind ebenfalls wieder online. In anderen Fällen ist möglicherweise ein SAN-Scan auf Host-Ebene erforderlich oder Applikationen müssen manuell wieder online geschaltet werden. Es hängt von der Anwendung und ihrer Konfiguration ab, und im Allgemeinen lassen sich solche Aufgaben leicht automatisieren. ONTAP selbst behebt selbstständig und sollte keinen Benutzereingriff erfordern, um den RPO=0-Storage-Betrieb wiederaufzunehmen.

## Manueller Failover

Das Ändern des bevorzugten Standorts erfordert eine einfache Bedienung. I/O-Vorgänge werden für eine oder zwei Sekunden angehalten, da zwischen den Clustern die Berechtigung für das Replikationsverhalten wechselt, die E/A-Vorgänge sind jedoch ansonsten nicht betroffen.

# Datensicherheit

Die Sicherung einer SQL Server Datenbankumgebung ist ein mehrdimensionaler Prozess, der über das Management der Datenbank selbst hinausgeht. ONTAP bietet verschiedene einzigartige Funktionen, die den Storage-Aspekt Ihrer Datenbankinfrastruktur sichern sollen.

## Snapshots

Speicher-Snapshots sind Point-in-Time-Replikate der Zieldaten. Die Implementierung von ONTAP umfasst die Möglichkeiten, verschiedene Richtlinien festzulegen und bis zu 1024 Snapshots pro Volume zu speichern. Snapshots in ONTAP sind platzsparend. Speicherplatz wird nur dann verbraucht, wenn sich der ursprüngliche Datensatz ändert. Sie sind auch schreibgeschützt. Ein Snapshot kann gelöscht, jedoch nicht geändert werden.

In einigen Fällen können Snapshots direkt auf ONTAP geplant werden. In anderen Fällen muss Software wie SnapCenter vor der Erstellung von Snapshots Applikations- oder Betriebssystemvorgänge orchestrieren. Ganz gleich, welcher Ansatz für Ihren Workload am besten geeignet ist: Eine aggressive Snapshot-Strategie bietet Datensicherheit durch häufigen, leicht zugänglichen Zugriff auf Backups aller Komponenten, von Boot-LUNs bis hin zu geschäftskritischen Datenbanken.



Ein flexibles ONTAP Volume oder ganz einfach ein Volume ist nicht gleichbedeutend mit einer LUN. Volumes sind Management-Container für Daten wie Dateien oder LUNs. Eine Datenbank kann beispielsweise auf einen Stripe-Satz mit 8 LUNs platziert werden, wobei alle LUNs in einem einzelnen Volume enthalten sind.

Weitere Informationen zu Snapshots finden Sie im "[ONTAP Dokumentation](#)."

## Manipulationssichere Snapshots

Ab ONTAP 9.12.1 sind Snapshots nicht nur schreibgeschützt, sondern können auch vor versehentlichem oder absichtlichem Löschen geschützt werden. Diese Funktion wird als manipulationssichere Snapshots bezeichnet. Über die Snapshot-Richtlinie kann eine Aufbewahrungsfrist festgelegt und durchgesetzt werden. Die resultierenden Snapshots können erst gelöscht werden, wenn sie ihr Ablaufdatum erreicht haben. Es gibt keine administrativen oder Support Center-Überschreibungen.

So wird sichergestellt, dass ein Eindringling, ein böswilliger Insider oder sogar ein Ransomware-Angriff die Backups nicht kompromittieren kann, selbst wenn er zum Zugriff auf das ONTAP-System selbst geführt hat. In

Verbindung mit häufigen Snapshot-Zeitplänen ist das Ergebnis eine äußerst leistungsstarke Datensicherheit mit einem sehr niedrigen RPO.



Manipulationssichere Snapshots können nicht mithilfe eines Fabric Pools gestaffelt werden.

Weitere Informationen zu manipulationssicheren Snapshots finden Sie im "[ONTAP Dokumentation](#)."



Replizieren Sie Snapshots in einer neuen ASA Plattform mithilfe der *Vault*-Richtlinie in einen Remote-Cluster und sperren Sie dann das Ziel, um Snapshots manipulationssicher zu machen.

## SnapMirror Replizierung

Snapshots können auch auf ein Remote-System repliziert werden. Dazu gehören manipulationssichere Snapshots, bei denen der Aufbewahrungszeitraum auf dem Remote-System angewendet und durchgesetzt wird. Dies führt zu denselben Vorteilen in Bezug auf die Datensicherung wie bei lokalen Snapshots, aber die Daten befinden sich auf einem zweiten Storage-Array. Dadurch wird sichergestellt, dass die Backups durch die Zerstörung des ursprünglichen Arrays nicht beeinträchtigt werden.

Ein zweites System eröffnet auch neue Optionen für die administrative Sicherheit. Beispielsweise trennen einige NetApp Kunden die Authentifizierungsdaten für die primären und sekundären Storage-Systeme. Kein administrativer Benutzer hat Zugriff auf beide Systeme. Das bedeutet, dass ein böswilliger Administrator nicht alle Datenkopien löschen kann.

Weitere Informationen zu SnapMirror finden Sie im "[ONTAP Dokumentation](#)."

## Storage Virtual Machines

Ein neu konfiguriertes ONTAP Storage-System ähnelt einem neu bereitgestellten VMware ESX Server, da keiner von ihnen bis zum Erstellen einer Virtual Machine Benutzer unterstützen kann. Mit ONTAP erstellen Sie eine Storage Virtual Machine (SVM), die die grundlegende Storage-Managementeinheit darstellt. Jede SVM verfügt über eigene Storage-Ressourcen, Protokollkonfigurationen, IP-Adressen und FCP-WWNs. Dies ist die Grundlage der Mandantenfähigkeit von ONTAP.

Beispielsweise können Sie eine SVM für kritische Produktions-Workloads und eine zweite SVM in einem anderen Netzwerksegment für Entwicklungsaktivitäten konfigurieren. Anschließend könnten Sie den Zugriff auf die Produktions-SVM auf bestimmte Administratoren beschränken und Entwicklern eine umfassendere Kontrolle über die Storage-Ressourcen in der Entwicklungs-SVM gewähren. Möglicherweise müssen Sie Ihren Finanz- und HR-Teams auch eine dritte SVM bereitstellen, damit sie besonders wichtige „eyed-only“-Daten speichern können.

Weitere Informationen zu SVMs finden Sie im "[ONTAP Dokumentation](#)."

## Administrative RBAC

ONTAP bietet eine leistungsstarke rollenbasierte Zugriffssteuerung (RBAC) für administrative Anmeldungen. Einige Administratoren benötigen unter Umständen vollständigen Cluster-Zugriff, während andere unter Umständen nur Zugriff auf bestimmte SVMs benötigen. Erfahrene Helpdesk-Mitarbeiter müssen möglicherweise die Volumegröße erhöhen können. Das Ergebnis ist, dass Sie administrativen Benutzern den Zugriff gewähren können, der für die Ausführung ihrer Aufgaben erforderlich ist, und nicht mehr. Darüber hinaus können Sie diese Anmeldungen mit PKI von verschiedenen Anbietern sichern, den Zugriff auf SSH-Schlüssel beschränken und Sperrungen bei fehlgeschlagenen Anmeldeversuchen erzwingen.

Weitere Informationen zur administrativen Zugriffssteuerung finden Sie im "[ONTAP Dokumentation](#)."

## **Multi-Faktor-Authentifizierung (MFA)**

ONTAP und einige andere NetApp Produkte unterstützen jetzt Multi-Faktor-Authentifizierung (MFA) anhand verschiedener Methoden. Das Ergebnis ist, dass ein kompromittierter Benutzername/Passwort allein kein Sicherheitsthreat ohne die Daten des zweiten Faktors, wie z. B. eine FOB oder eine Smartphone-App, ist.

Weitere Informationen zur Multifaktor-Authentifizierung (MFA) finden Sie im "[ONTAP Dokumentation](#)."

## **API RBAC**

Für die Automatisierung sind API-Aufrufe erforderlich, aber nicht alle Tools benötigen vollständigen administrativen Zugriff. Um Automatisierungssysteme zu sichern, ist RBAC auch auf API-Ebene verfügbar. Sie können die Benutzerkonten für die Automatisierung auf die erforderlichen API-Aufrufe beschränken. Die Überwachungssoftware benötigt beispielsweise keinen Änderungszugriff, sondern nur Lesezugriff. Workflows, die Storage bereitstellen, müssen Storage nicht löschen können.

Weitere Informationen zu API-RBAC finden Sie im "[ONTAP Dokumentation](#)."

## **Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)**

Die Multi-Faktor-Authentifizierung kann noch weiter ausgebaut werden, indem zwei verschiedene Administratoren mit jeweils eigenen Anmeldeinformationen bestimmte Aktivitäten genehmigen müssen. Dazu gehören das Ändern von Anmeldeberechtigungen, das Ausführen von Diagnosebefehlen und das Löschen von Daten.

Weitere Informationen zur Multi-Admin-Verifizierung (MAV) finden Sie im "[ONTAP Dokumentation](#)."

## **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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 IRGENDERWEINER 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.