Storage-Konfiguration auf ASA r2-Systemen

Enterprise applications

NetApp
January 02, 2026

Inhalt

Storage-Konfiguration auf ASA r2-Systemen . . . 1
- Überblick . . . 1
  - Datenspeicher Design . . . 1
- Datenbankdateien und Dateigruppen . . . 2
- Datensicherung . . . 7
  - SnapCenter . . . 7
  - Datenbanken mit T-SQL-Snapshots werden gesichert . . . 8
- Disaster Recovery . . . 8
  - Disaster Recovery . . . 8
  - SnapMirror . . . 9
  - SnapMirror Active Sync . . . 9

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:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20

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.

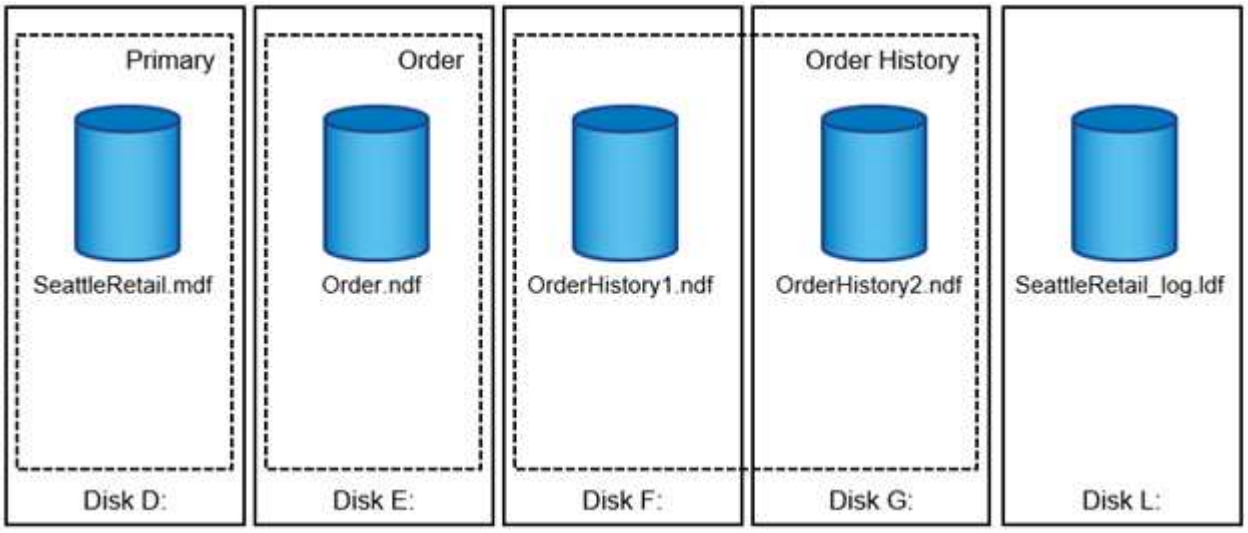
Theoretisch unterstützt SQL Server (64-Bit) 32,767 Datenbanken pro Instanz und 524.272 TB Datenbankgröße, obwohl die typische Installation normalerweise über mehrere Datenbanken verfügt. Die Anzahl der Datenbanken, die SQL Server verarbeiten kann, hängt jedoch von der Last und der Hardware ab. Es ist 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.

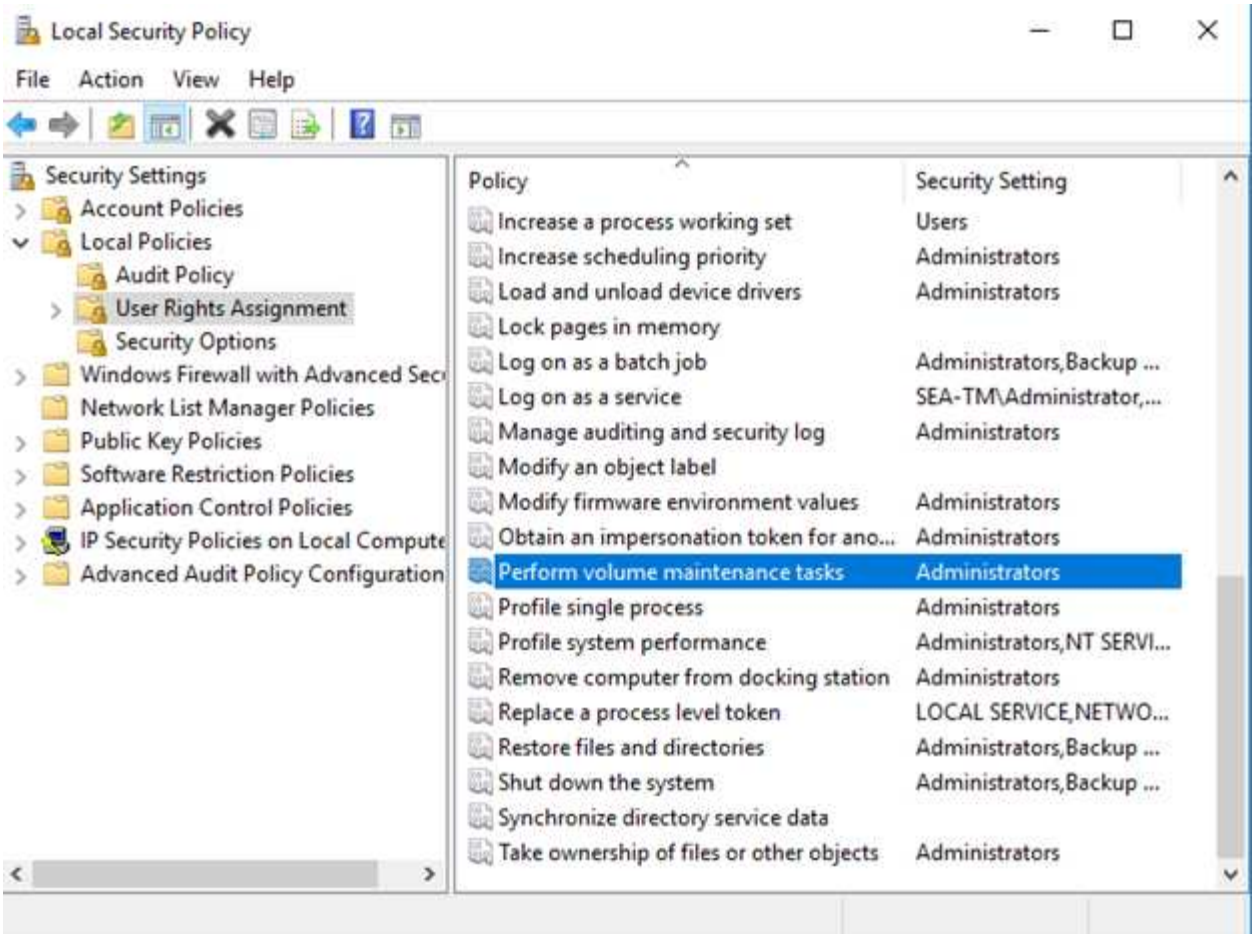
NetApp empfiehlt, dass alle Dateien in der einzelnen Dateigruppe die gleiche Anfangsgröße und die gleichen Autogrowth-Parameter haben, wobei die Grow-Größe in Megabyte und nicht in Prozentsätzen definiert ist. Dies hilft dem proportionalen Füllalgorithmus, Schreibaktivitäten gleichmäßig über Datendateien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



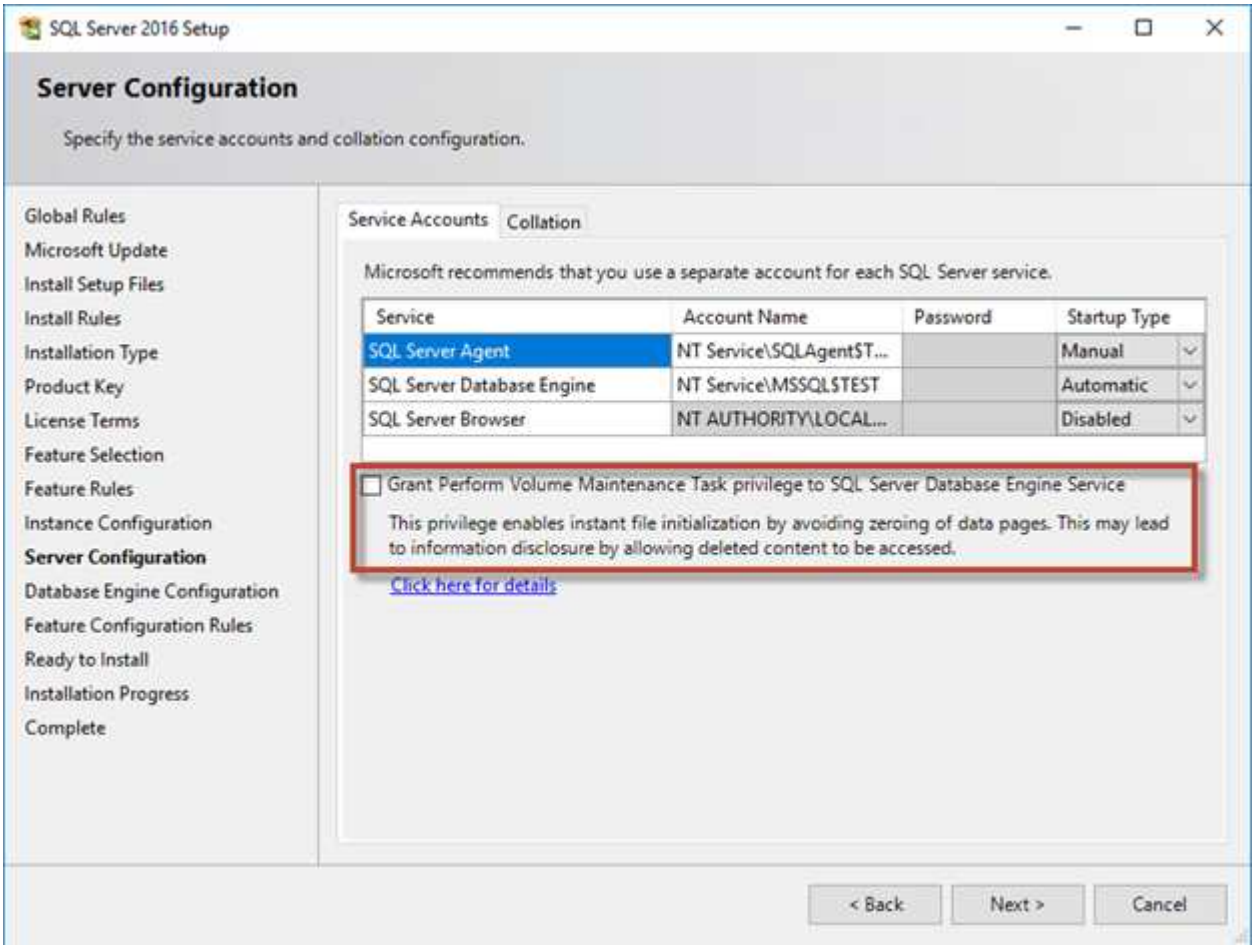
Um zu überprüfen, ob die Berechtigung aktiviert ist, können Sie den Code aus dem folgenden Beispiel verwenden. Dieser Code setzt zwei Trace-Flags, die SQL Server zwingen, zusätzliche Informationen in das Fehlerprotokoll zu schreiben, eine kleine Datenbank zu erstellen und den Inhalt des Protokolls zu 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	FixupLogTail(progress) zeroing C:\Program Files\Micros
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQ
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL
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-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 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 Netzwerkbandbreite 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

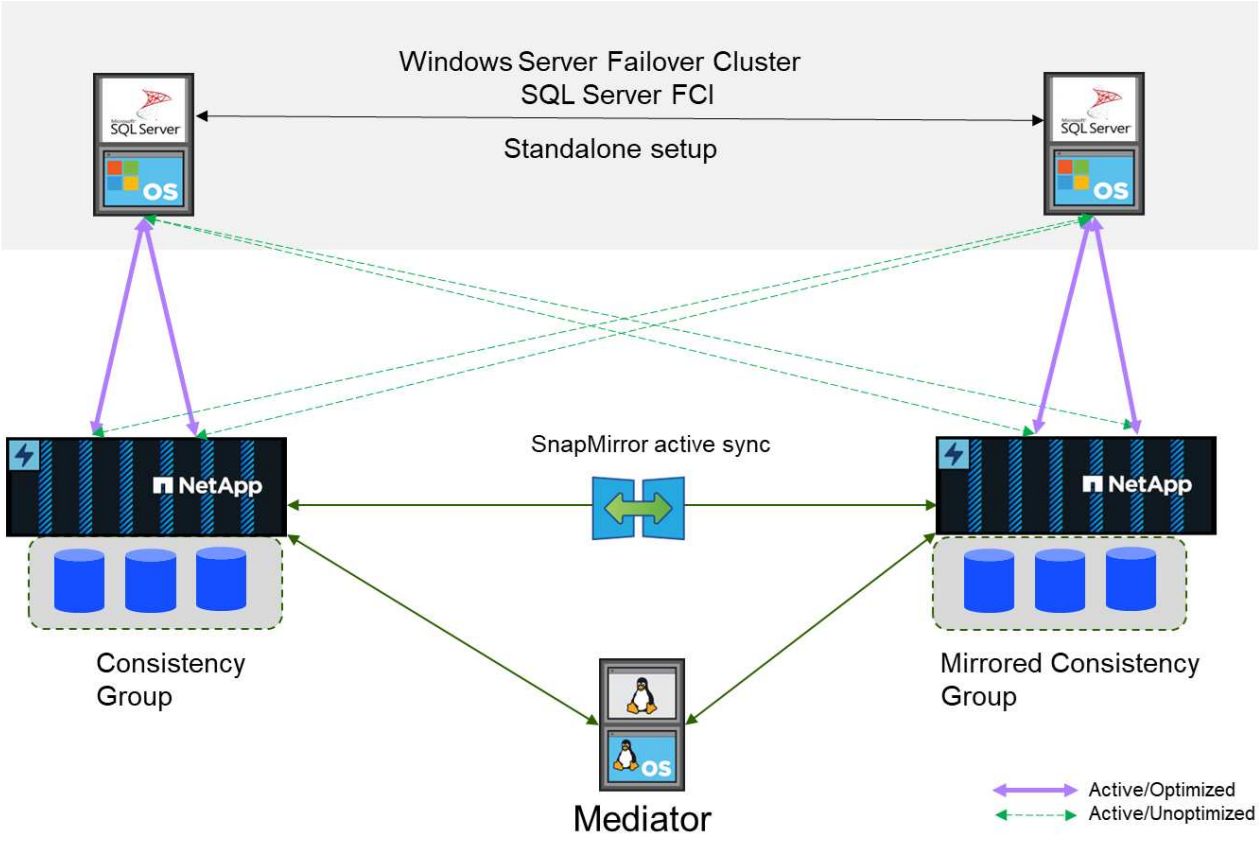
Mit SnapMirror Active Sync können einzelne SQL Server-Datenbanken und -Applikationen bei Storage- und Netzwerkstörungen den Betrieb fortsetzen. Der Storage

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.

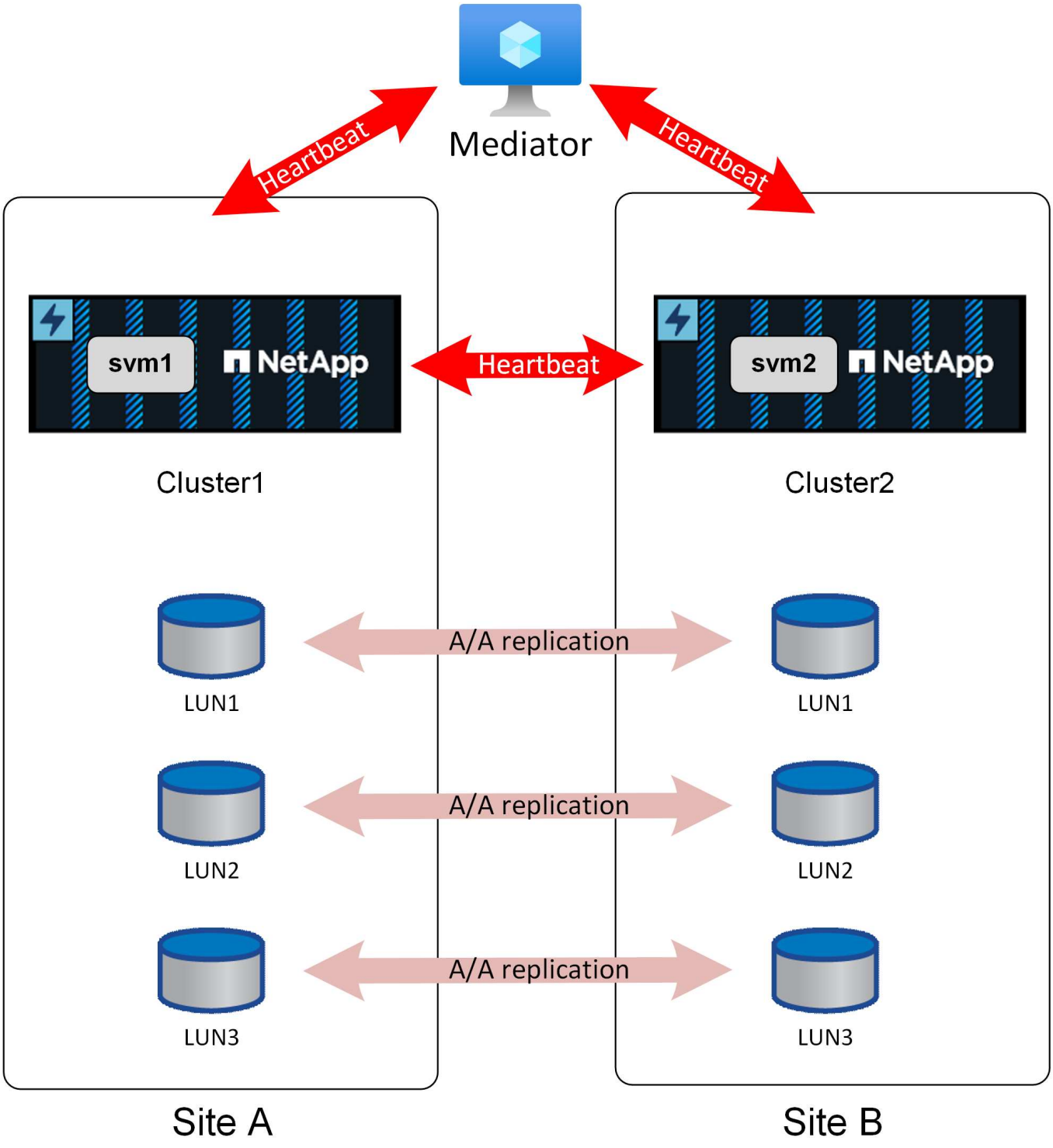
ONTAP Mediator

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.

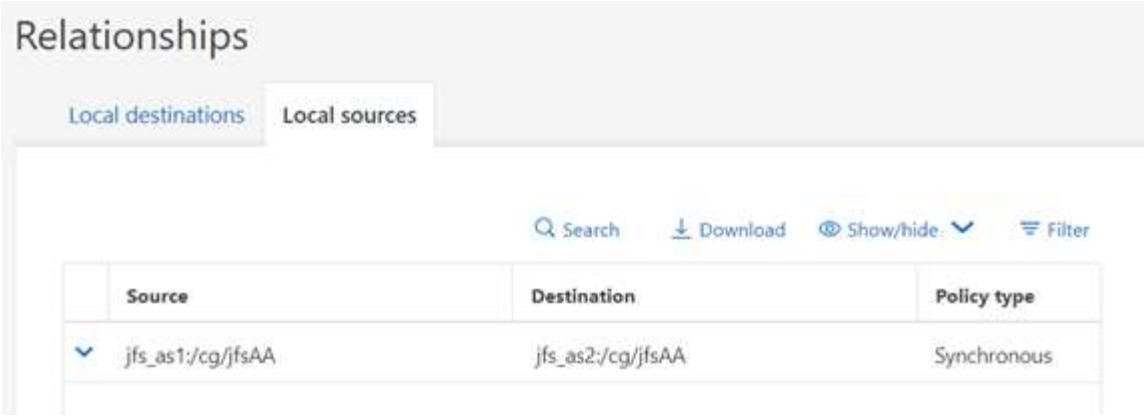
Bevorzugter Standort

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:



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.

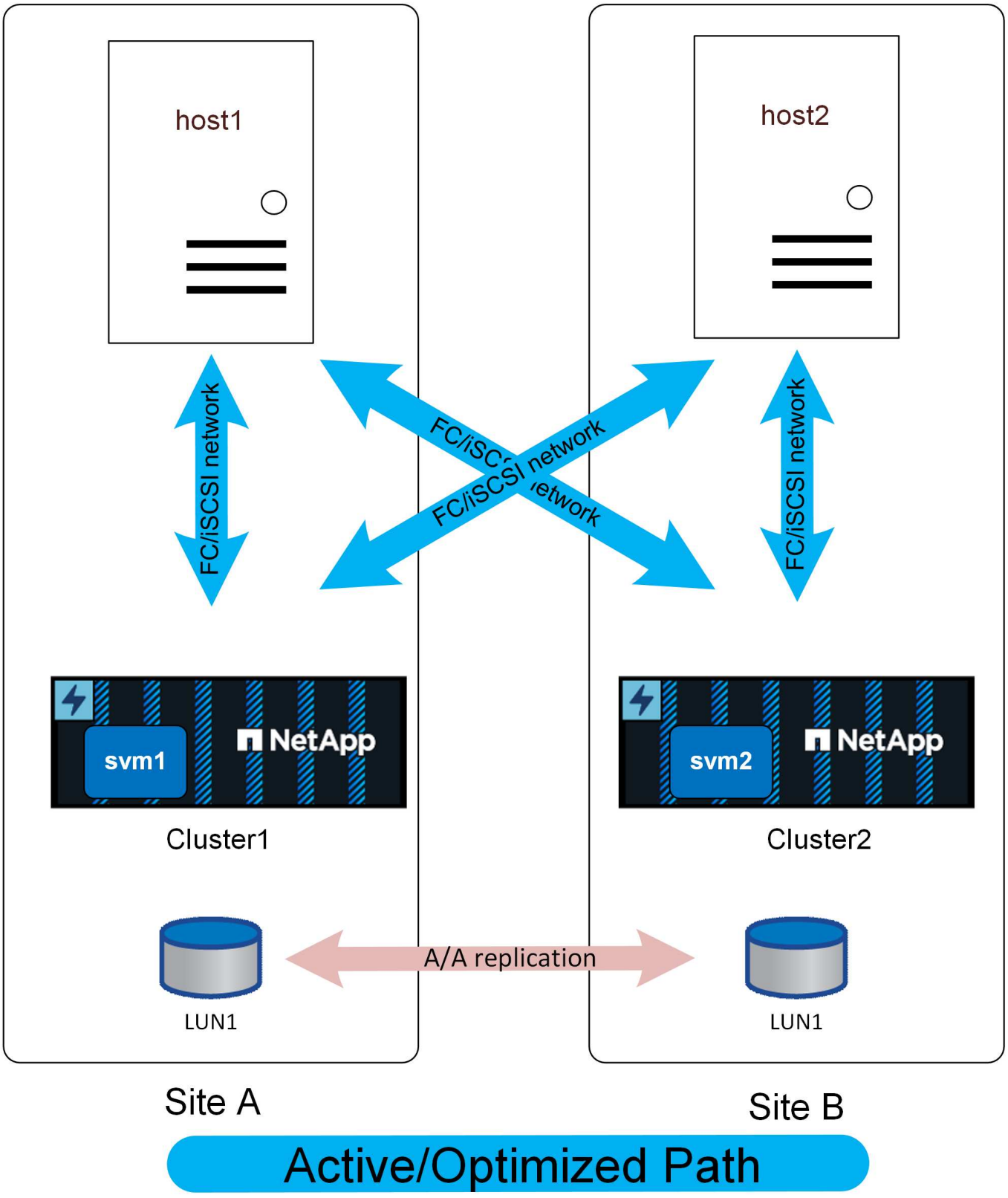
Netzwerktopologie

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.



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.

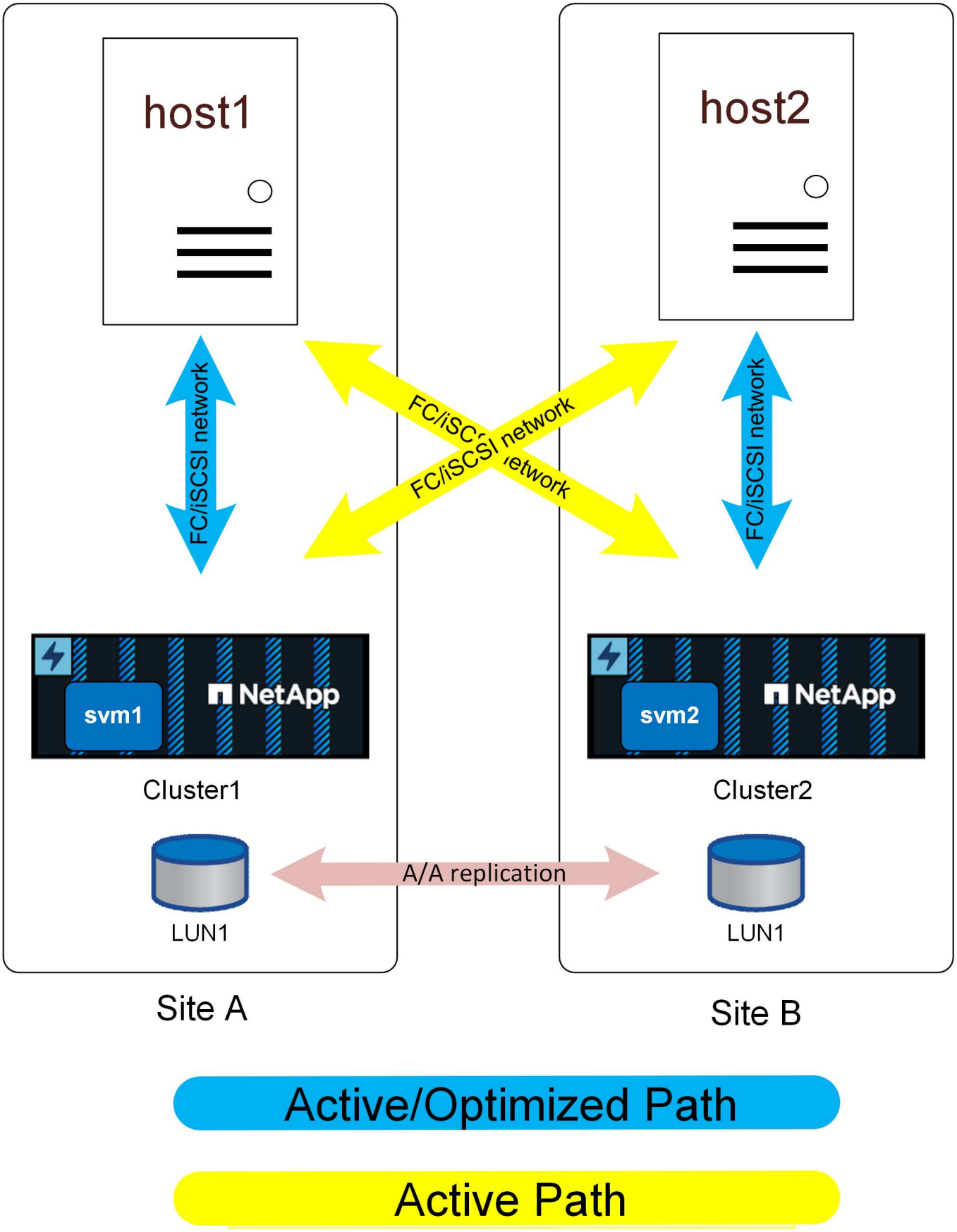
Der erste Schritt ist die übliche igroup-Konfiguration. Jede LUN muss einer Initiatorgruppe zugeordnet werden, die die WWN/iSCSI-IDs der Hosts enthält, die Zugriff auf diese LUN benötigen. Dadurch wird gesteuert, welcher Host *Access* zu einer LUN hat.

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

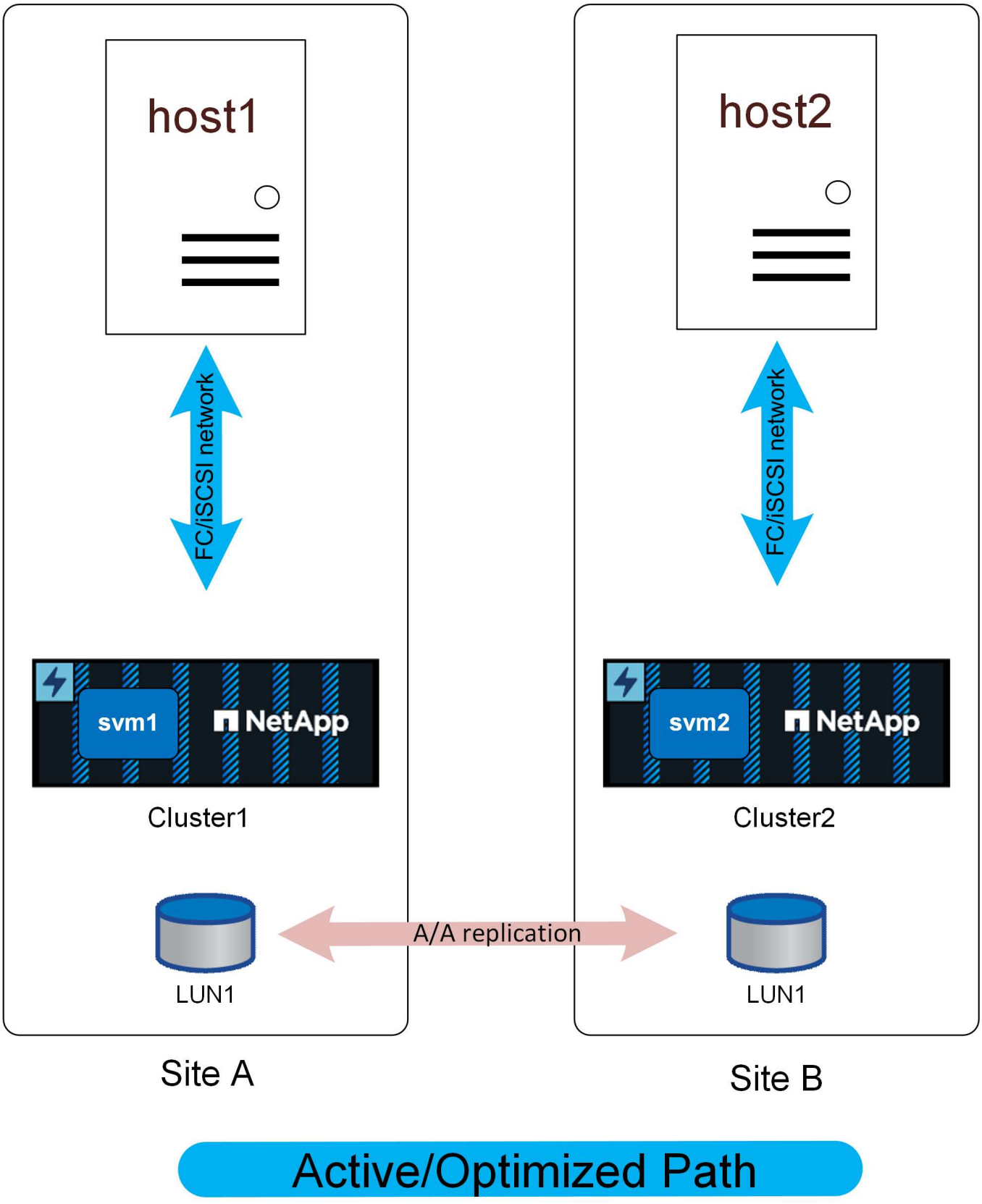
Ohne Annäherungseinstellungen verwendet der Host beide Speichersysteme gleichmäßig, da beide Speichersysteme aktive/optimierte Pfade anbieten. Wenn die SAN-Latenz und/oder Bandbreite zwischen Standorten begrenzt ist, ist dies möglicherweise nicht erwünscht, und Sie sollten sicherstellen, dass während 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.


host1
host2
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
svm1
NetApp
svm2
NetApp
Cluster1
Cluster2
A/A replication
LUN1
LUN1
Site A
Site B
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.



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 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 ausgefallenen 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.

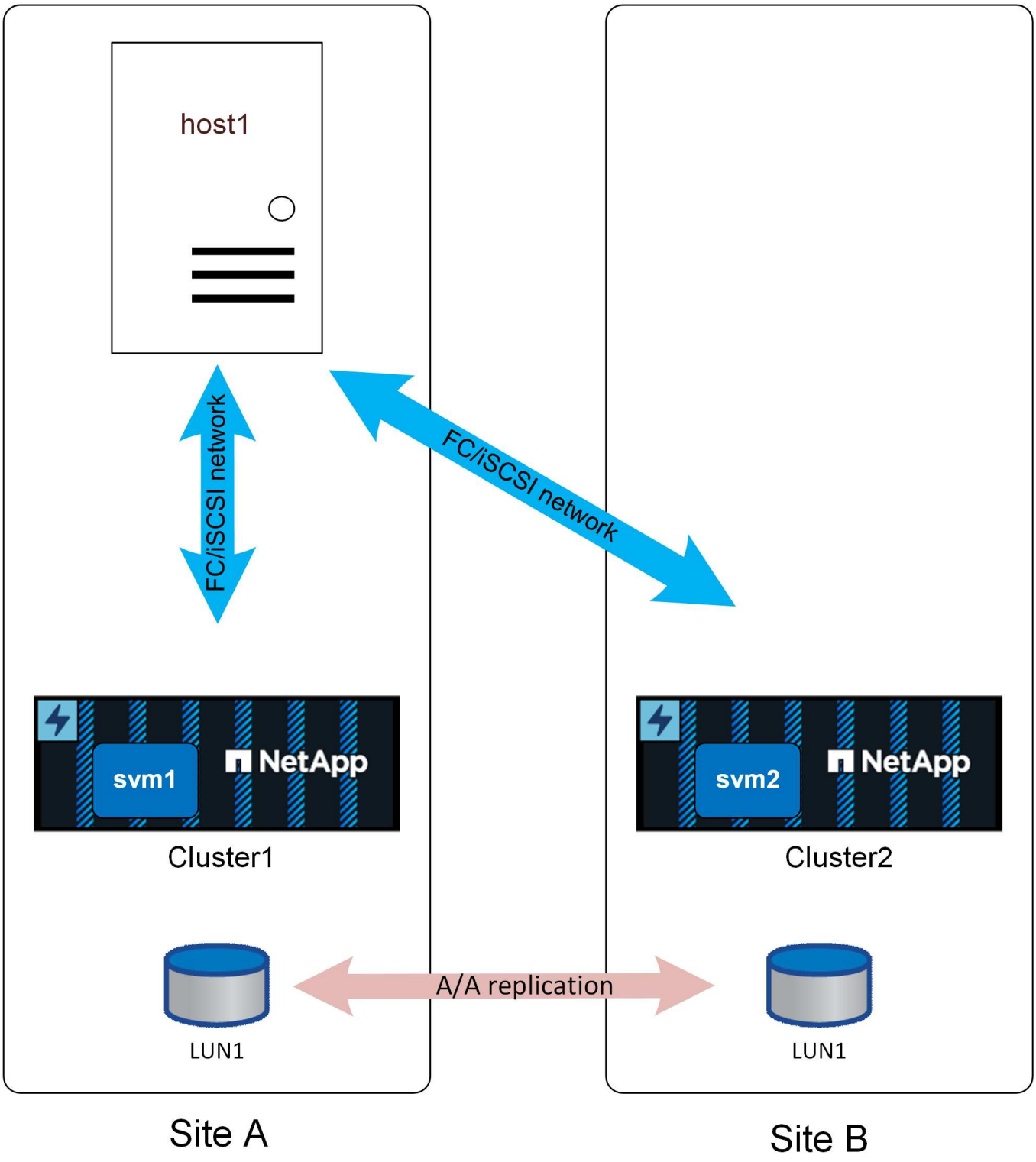
Überblick

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.