



Microsoft SQL Server

Enterprise applications

NetApp
January 02, 2026

Sommario

Microsoft SQL Server	1
Panoramica	1
Workload di Microsoft SQL Server	1
Configurazione del database	2
Configurazione CPU	2
Configurazione della memoria	5
Istanza condivisa contro istanza dedicata	8
File tempdb	9
Configurazione dello storage su sistemi AFF/FAS	10
Panoramica	10
File di database e filegroup	12
Efficienza dello storage	17
Protezione dei dati	22
Disaster recovery	24
Configurazione dello storage sui sistemi ASA R2	45
Panoramica	45
File di database e filegroup	47
Protezione dei dati	51
Disaster recovery	52
Sicurezza dei dati	68
Copie Snapshot	68
Snapshot a prova di manomissione	68
Replica SnapMirror	69
Macchine virtuali di storage	69
RBAC amministrativo	69
Autenticazione multifattore (MFA)	69
RBAC API	70
Verifica multi-admin (MAV)	70

Microsoft SQL Server

Panoramica

ONTAP offre una soluzione per la sicurezza e le prestazioni di livello aziendale per i database Microsoft SQL Server e allo stesso tempo fornisce strumenti di prim'ordine per la gestione dell'ambiente.



Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4590: Best practice guide for Microsoft SQL Server with ONTAP*

NetApp presuppone che il lettore disponga delle seguenti conoscenze operative:

- ONTAP
- Architettura e amministrazione di Microsoft SQL Server
- NetApp SnapCenter come software di backup, che include:
 - Plug-in SnapCenter per Microsoft Windows
 - Plug-in di SnapCenter per SQL Server

L'ambito di questa sezione sulle Best practice è limitato alla progettazione tecnica, basata su principi e standard preferenziali che NetApp consiglia per l'infrastruttura di storage. L'implementazione end-to-end non rientra nell'ambito di applicazione.

Per informazioni sulla compatibilità tra i prodotti NetApp, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Workload di Microsoft SQL Server

Prima di distribuire SQL Server, è necessario comprendere i requisiti dei carichi di lavoro delle applicazioni supportate dalle istanze dei database di SQL Server. Ogni applicazione ha requisiti differenti in termini di capacità, performance e disponibilità, per cui ogni database dovrebbe essere progettato per supportare al meglio tali requisiti. Molte organizzazioni classificano i database in più Tier di gestione, utilizzando i requisiti delle applicazioni per definire gli SLA. I carichi di lavoro di SQL Server sono spesso classificati come descritto di seguito:

- OLTP, che è spesso i database più critici di un'organizzazione. In genere, questi database supportano le applicazioni rivolte ai clienti e sono considerati essenziali per le operazioni chiave dell'azienda. I database OLTP mission-critical e le applicazioni che questi supportano spesso hanno SLA che richiedono performance elevate, sono sensibili al peggioramento delle performance e richiedono la massima disponibilità. Potrebbero anche essere candidati per cluster di failover sempre attivi o gruppi di disponibilità sempre attivi. La combinazione di i/o di questi tipi di database è in genere caratterizzata da una percentuale compresa tra il 75% e il 90% di random Read e tra il 25% e il 10% di scrittura.
- Database DSS (Decision Support System), talvolta denominati data warehouse. Questi database sono mission-critical per molte organizzazioni che si affidano alle analytics per il loro business. Questi database sono sensibili all'utilizzo della CPU e alle operazioni di lettura dal disco quando vengono eseguite query. In molte organizzazioni, i database DSS sono i più critici durante la fine di mese, trimestre e anno. Questo carico di lavoro ha in genere una combinazione di i/o di lettura quasi del 100% e il throughput io è spesso più importante degli IOPS.

Configurazione del database

Configurazione CPU

Le prestazioni di SQL Server dipendono in modo multiplo dalla CPU e dalla configurazione di base.

Hyper-threading

L'Hyper-threading si riferisce all'implementazione simultanea del multithreading (SMT), che migliora la parallelizzazione dei calcoli eseguiti su processori x86. SMT è disponibile sia sui processori Intel che AMD.

L'Hyper-threading produce CPU logiche che appaiono come CPU fisiche nel sistema operativo. SQL Server vede quindi le CPU aggiuntive e le utilizza come se vi fossero più core di quelli fisicamente presenti. Questo può migliorare notevolmente le prestazioni aumentando la parallelizzazione.

Si noti che ogni versione di SQL Server presenta dei limiti specifici sulla potenza di calcolo che può utilizzare. Per ulteriori informazioni, vedere ["Limiti di capacità di calcolo per edizione di SQL Server"](#).

Core e licenze

Esistono due opzioni per la licenza di SQL Server. Il primo è noto come modello server + licenza di accesso client (CAL); il secondo è il modello core per processore. Sebbene sia possibile accedere a tutte le funzioni del prodotto disponibili in SQL Server con la strategia server + CAL, esiste un limite hardware di 20 core CPU per socket. Anche se si dispone di SQL Server Enterprise Edition + CAL per un server con più di 20 core di CPU per socket, l'applicazione non può utilizzare tutti questi core alla volta in tale istanza.

L'immagine seguente mostra il messaggio di registro di SQL Server dopo l'avvio che indica l'imposizione del limite principale.

```

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

```

Pertanto, per utilizzare tutte le CPU, è necessario utilizzare la licenza core per processore. Per informazioni dettagliate sulle licenze di SQL Server, vedere ["SQL Server 2022: La tua moderna piattaforma per i dati"](#).

Affinità della CPU

È improbabile che sia necessario modificare le impostazioni predefinite di affinità del processore a meno che non si verifichino problemi di prestazioni, ma vale ancora la pena capire cosa sono e come funzionano.

SQL Server supporta l'affinità del processore mediante due opzioni:

- Maschera di affinità della CPU
- Maschera i/o di affinità

SQL Server utilizza tutte le CPU disponibili dal sistema operativo (se si sceglie la licenza core per processore). Inoltre, crea degli scheduler for per ogni CPU per utilizzare al meglio le risorse per qualsiasi carico di lavoro. Durante il multitasking, il sistema operativo o altre applicazioni sul server possono passare da un processore all'altro. SQL Server è un'applicazione che richiede molte risorse e in tal caso le prestazioni possono risentirne. Per ridurre al minimo l'impatto, è possibile configurare i processori in modo che tutto il carico di SQL Server venga indirizzato a un gruppo preselezionato di processori. Ciò si ottiene utilizzando la maschera di affinità della CPU.

L'opzione maschera i/o affinità associa l'i/o del disco di SQL Server a un sottoinsieme di CPU. Negli ambienti OLTP di SQL Server, questa estensione può migliorare significativamente le prestazioni dei thread di SQL

Server che emettono operazioni i/O.

Massimo grado di parallelismo (MAXDOP)

Per impostazione predefinita, SQL Server utilizza tutte le CPU disponibili durante l'esecuzione delle query, se si sceglie la licenza core per processore.

Sebbene sia utile per query di grandi dimensioni, può causare problemi di prestazioni e limitare la concorrenza. Un approccio migliore consiste nel limitare il parallelismo al numero di core fisici in un singolo socket CPU. Ad esempio, su un server con due socket CPU fisici con 12 core per socket, indipendentemente dall'Hyper-threading, MAXDOP deve essere impostato su 12. MAXDOP Non è possibile limitare o dettare quale CPU utilizzare. Limita invece il numero di CPU che possono essere utilizzate da una singola query batch.



NetApp consiglia per DSS, ad esempio data warehouse, iniziare con MAXDOP 50 ed esplorare la messa a punto su o giù, se necessario. Assicurarsi di misurare le query critiche nell'applicazione quando si apportano modifiche.

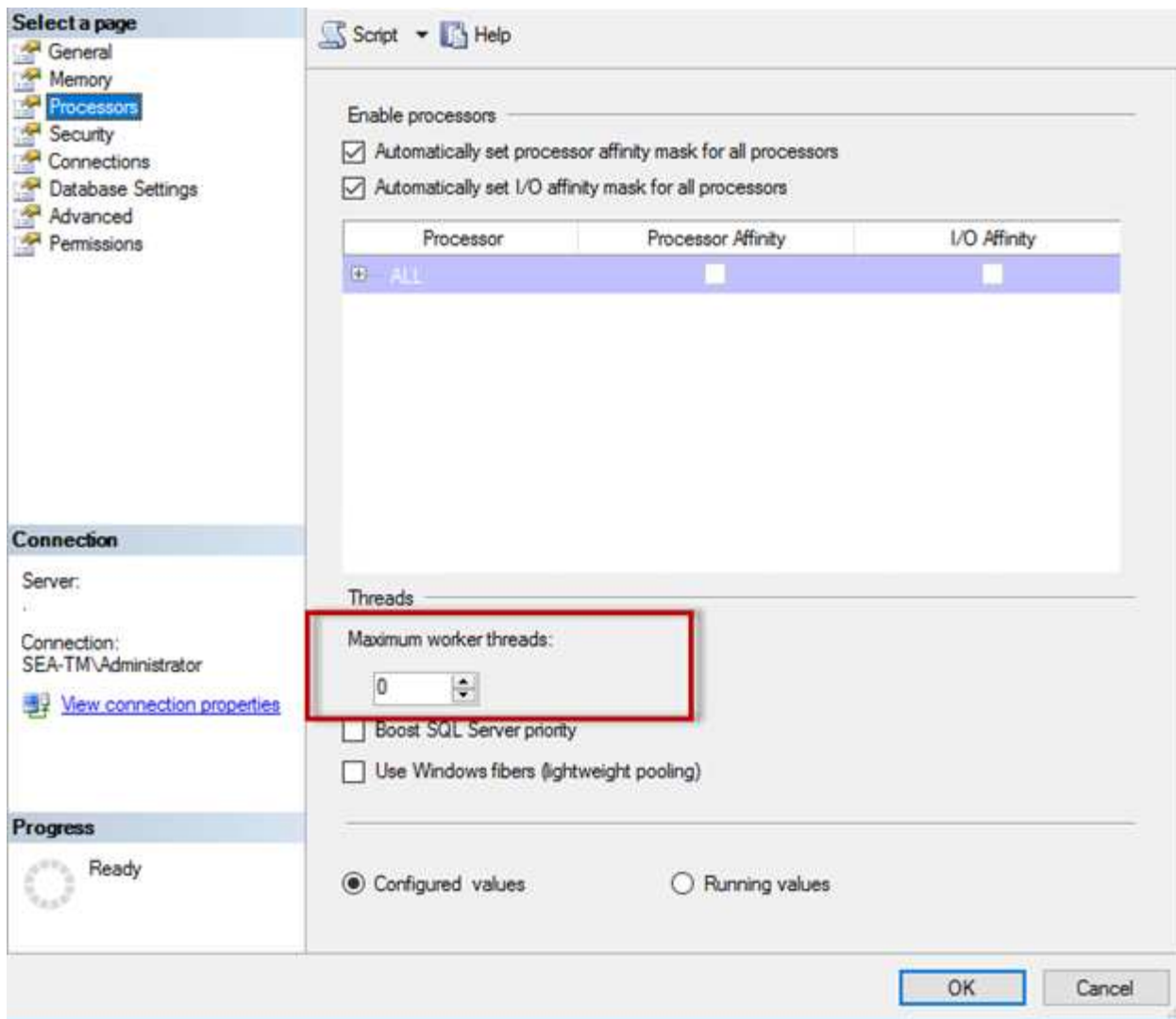
Numero massimo di thread di lavoro

L'opzione numero massimo di thread di lavoro consente di ottimizzare le prestazioni quando un numero elevato di client è connesso a SQL Server.

In genere, per ogni query viene creato un thread del sistema operativo separato. Se vengono effettuate centinaia di connessioni simultanee a SQL Server, la configurazione con un solo thread per query può consumare troppe risorse di sistema. L'`max worker threads` opzione consente di migliorare le prestazioni consentendo a SQL Server di creare un pool di thread di lavoro in grado di gestire collettivamente un maggior numero di richieste di query.

Il valore predefinito è 0, che consente a SQL Server di configurare automaticamente il numero di thread di lavoro all'avvio. Funziona per la maggior parte dei sistemi. Max worker Threads è un'opzione avanzata e non deve essere alterata senza l'assistenza di un amministratore di database esperto (DBA).

Quando è necessario configurare SQL Server per utilizzare più thread di lavoro? Se la lunghezza media della coda di lavoro per ogni pianificatore è superiore a 1, si potrebbe trarre vantaggio dall'aggiunta di più thread al sistema, ma solo se il carico non è legato alla CPU o se si verificano altre attese pesanti. Se si verifica uno di questi due eventi, l'aggiunta di altri thread non aiuta perché sono in attesa di altri colli di bottiglia del sistema. Per ulteriori informazioni sui thread di lavoro max, vedere ["Configurare l'opzione di configurazione del server numero massimo di thread di lavoro"](#).



Configurazione di max worker threads con SQL Server Management Studio.

Nell'esempio seguente viene illustrato come configurare l'opzione numero massimo di thread di lavoro utilizzando T-SQL.

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

Configurazione della memoria

La sezione seguente illustra le impostazioni della memoria di SQL Server necessarie per ottimizzare le prestazioni del database.

Memoria massima del server

L'opzione memoria massima del server imposta la quantità massima di memoria che l'istanza di SQL Server può utilizzare. Viene generalmente utilizzata se più applicazioni vengono eseguite sullo stesso server in cui SQL Server è in esecuzione e si desidera garantire che queste applicazioni dispongano di memoria sufficiente per funzionare correttamente.

Alcune applicazioni utilizzano solo la memoria disponibile all'avvio e non richiedono memoria aggiuntiva, anche se sono sotto pressione della memoria. È qui che entra in gioco l'impostazione della memoria massima del server.

In un cluster SQL Server con diverse istanze SQL Server, ciascuna istanza potrebbe competere per le risorse. L'impostazione di un limite di memoria per ciascuna istanza di SQL Server può contribuire a garantire le migliori prestazioni per ciascuna istanza.



NetApp consiglia di lasciare almeno 4GB o 6GB GB di RAM per il sistema operativo per evitare problemi di prestazioni.

The screenshot displays the 'Server Memory' configuration window in SQL Server Enterprise Manager. The left-hand pane shows a tree view with 'Memory' selected under 'Select a page'. The main area is divided into two sections: 'Server memory options' and 'Other memory options'. The 'Server memory options' section is highlighted with a red rectangle and contains two spinners: 'Minimum server memory (in MB)' set to 0 and 'Maximum server memory (in MB)' set to 120832. The 'Other memory options' section contains two more spinners: 'Index creation memory (in KB, 0 = dynamic memory)' set to 0 and 'Minimum memory per query (in KB)' set to 1024. At the bottom, there are two radio buttons: 'Configured values' (selected) and 'Running values'. The bottom status bar shows 'Ready' under the 'Progress' section. The 'OK' and 'Cancel' buttons are at the bottom right.

Regolazione della memoria minima e massima del server mediante SQL Server Management Studio.

L'utilizzo di SQL Server Management Studio per regolare la memoria minima o massima del server richiede il riavvio del servizio SQL Server. È inoltre possibile regolare la memoria del server utilizzando Transact SQL (T-

SQL) utilizzando il seguente codice:

```
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
```

Accesso alla memoria non uniforme

L'accesso alla memoria non uniforme (NUMA, non Uniform Memory Access) è una tecnologia di ottimizzazione dell'accesso alla memoria che consente di evitare un carico extra sul bus del processore.

Se NUMA è configurato su un server in cui è installato SQL Server, non è necessaria alcuna configurazione aggiuntiva, in quanto SQL Server è compatibile con NUMA e funziona bene sull'hardware NUMA.

Indice creare memoria

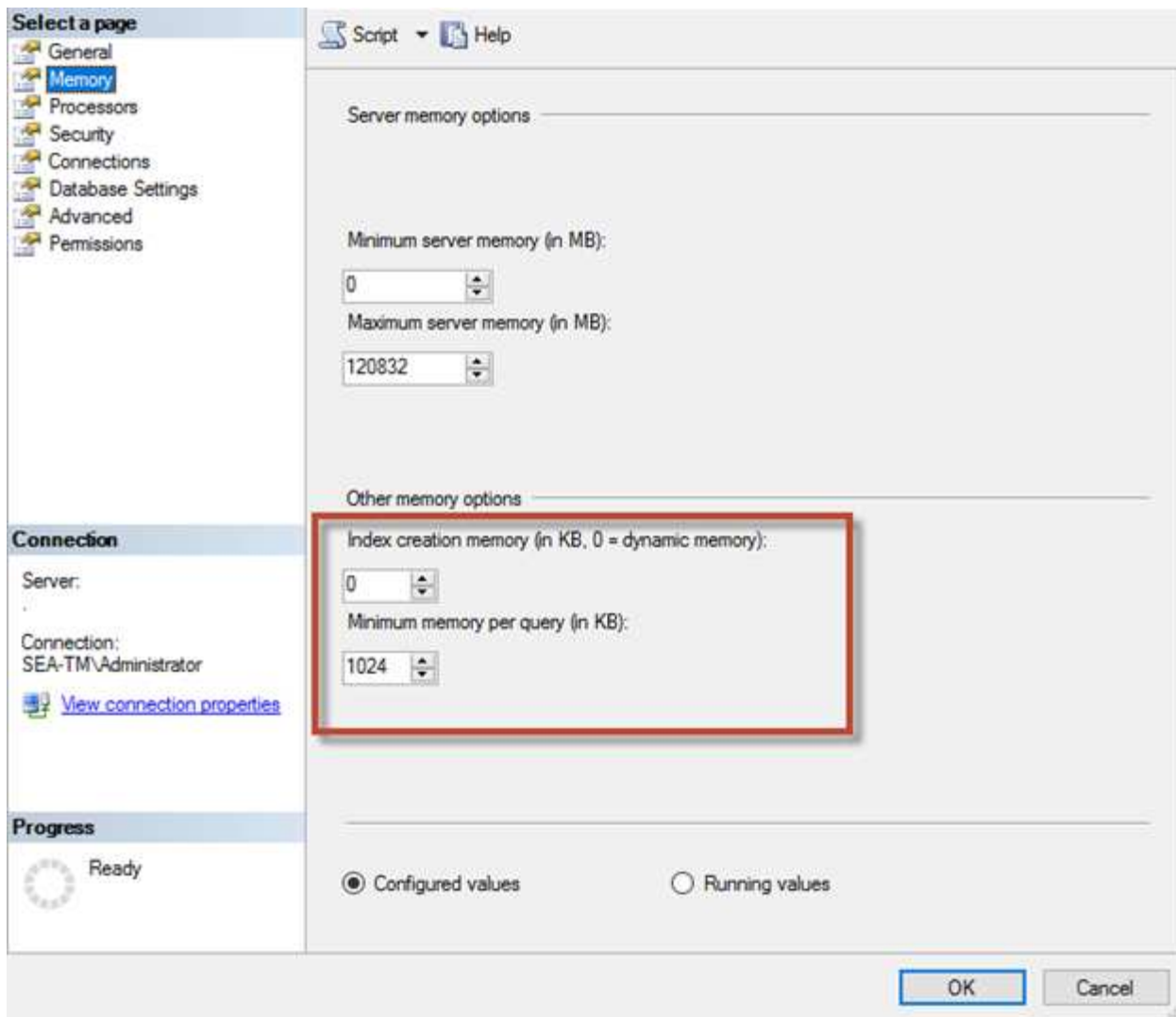
L'opzione di creazione della memoria di indice è un'altra opzione avanzata che non dovrebbe normalmente essere modificata dai valori predefiniti.

Controlla la quantità massima di RAM inizialmente allocata per la creazione degli indici. Il valore predefinito per questa opzione è 0, il che significa che è gestita automaticamente da SQL Server. Tuttavia, se si riscontrano difficoltà nella creazione degli indici, è consigliabile aumentare il valore di questa opzione.

Memoria minima per query

Quando viene eseguita una query, SQL Server tenta di allocare la quantità ottimale di memoria per un'esecuzione efficiente.

Per impostazione predefinita, l'impostazione memoria minima per query assegna \geq a 1024KB per ogni query da eseguire. È consigliabile lasciare questa impostazione al valore predefinito per consentire a SQL Server di gestire dinamicamente la quantità di memoria allocata per le operazioni di creazione dell'indice. Tuttavia, se SQL Server dispone di una quantità di RAM superiore a quella necessaria per un'esecuzione efficiente, le prestazioni di alcune query possono essere migliorate se si aumenta questa impostazione. Pertanto, se sul server non viene utilizzata SQL Server, altre applicazioni o il sistema operativo è disponibile memoria, il miglioramento di questa impostazione può contribuire alle prestazioni complessive di SQL Server. Se non è disponibile memoria libera, l'aumento di questa impostazione potrebbe compromettere le prestazioni complessive.



Istanza condivisa contro istanza dedicata

SQL Server può essere configurato come singola istanza per server o come istanze multiple. La decisione giusta dipende in genere da fattori quali l'utilizzo del server per la produzione o lo sviluppo, indipendentemente dal fatto che l'istanza sia considerata di importanza critica per le operazioni aziendali e gli obiettivi prestazionali.

Le configurazioni delle istanze condivise possono essere inizialmente più semplici da configurare, ma possono causare problemi in cui le risorse vengono divise o bloccate, il che a sua volta causa problemi di prestazioni per altre applicazioni che hanno database ospitati nell'istanza condivisa di SQL Server.

La risoluzione dei problemi di prestazioni può essere complicata, perché è necessario capire quale istanza è la causa principale. Questa domanda è valutata rispetto ai costi delle licenze del sistema operativo e delle licenze di SQL Server. Se le performance applicative sono fondamentali, si consiglia vivamente un'istanza dedicata.

Microsoft concede in licenza SQL Server per core a livello di server e non per istanza. Per questo motivo, gli amministratori di database sono tentati di installare tutte le istanze di SQL Server che il server è in grado di gestire per risparmiare sui costi di licenza, il che può portare a gravi problemi di performance in un secondo momento.



NetApp consiglia di scegliere istanze dedicate di SQL Server quando possibile per ottenere prestazioni ottimali.

File tempdb

Il database Tempdb può essere utilizzato in modo intensivo. Oltre al posizionamento ottimale dei file di database degli utenti su ONTAP, anche il posizionamento dei file di dati tempdb è fondamentale per ridurre il conflitto di allocazione. Tempdb deve essere posizionato su un disco separato e non condiviso con i file di dati dell'utente.

Il conflitto di pagina può verificarsi nelle pagine GAM (Global allocation map), SGAM (Shared Global allocation map) o PFS (page free space) quando SQL Server deve scrivere in pagine di sistema speciali per allocare nuovi oggetti. I fermi bloccano queste pagine in memoria. In un'istanza SQL Server occupata, può essere necessario molto tempo per ottenere un blocco in una pagina di sistema in tempdb. Ciò si traduce in tempi di esecuzione delle query più lenti ed è noto come conflitto di latch. Per la creazione di file di dati tempdb, vedere le procedure consigliate riportate di seguito:

- Per ≤ 8 core: File di dati tempdb = numero di core
- Per più di 8 core: 8 file di dati tempdb
- Il file dati tempdb deve essere creato con le stesse dimensioni

Lo script di esempio seguente modifica tempdb creando otto file tempdb di pari dimensioni e spostando tempdb sul punto di montaggio C:\MSSQL\tempdb per SQL Server 2012 e versioni successive.

```
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

```

A partire da SQL Server 2016, il numero di core di CPU visibili al sistema operativo viene rilevato automaticamente durante l'installazione e, in base a tale numero, SQL Server calcola e configura il numero di file tempdb necessari per ottenere prestazioni ottimali.

Configurazione dello storage su sistemi AFF/FAS

Panoramica

La combinazione delle soluzioni storage ONTAP e Microsoft SQL Server genera design di storage per database di livello Enterprise in grado di soddisfare le più esigenti esigenze applicative odierne.

L'ottimizzazione di una soluzione SQL Server su ONTAP richiede la comprensione del modello e delle caratteristiche di i/o di SQL Server. Un layout di storage ben progettato per un database SQL Server deve supportare i requisiti relativi alle performance di SQL Server, offrendo al contempo la massima capacità di

gestione dell'infrastruttura nel suo complesso. Un buon layout dello storage permette inoltre di avere successo nell'implementazione iniziale e di far crescere l'ambiente senza problemi nel tempo, con il crescere dell'azienda.

Progettazione dello storage dei dati

Per i database SQL Server che non utilizzano SnapCenter per eseguire i backup, Microsoft consiglia di posizionare i file di dati e di log su dischi separati. Per le applicazioni che aggiornano e richiedono contemporaneamente i dati, il file di log è intensivo in scrittura e il file di dati (a seconda dell'applicazione) è intensivo in lettura/scrittura. Per il recupero dei dati, il file di log non è necessario. Pertanto, le richieste di dati possono essere soddisfatte dal file di dati posto sul proprio disco.

Quando si crea un nuovo database, Microsoft consiglia di specificare unità separate per i dati e i registri. Per spostare i file dopo la creazione del database, il database deve essere portato offline. Per ulteriori consigli Microsoft, vedere ["Posizionare i file di dati e di registro su unità separate"](#).

Aggregati

Gli aggregati sono i container di storage di livello più basso per le configurazioni di storage NetApp. Su Internet esiste una documentazione legacy che consiglia di separare i/o su diversi set di unità sottostanti. Questa operazione non è consigliata con ONTAP. NetApp ha eseguito diverse prove di caratterizzazione dei carichi di lavoro i/o utilizzando aggregati condivisi e dedicati con file di dati e file di log delle transazioni separati. I test dimostrano che un aggregato di grandi dimensioni con più gruppi RAID e dischi ottimizza e migliora le performance dello storage ed è più semplice da gestire per due motivi:

- Un aggregato di grandi dimensioni rende disponibili per tutti i file le funzionalità i/o di tutte le unità.
- Un grande aggregato consente l'utilizzo più efficiente dello spazio su disco.

Per l'high Availability (ha), posiziona la replica sincrona secondaria di SQL Server Always on Availability Group su una Storage Virtual Machine (SVM) separata nell'aggregato. Per scopi di disaster recovery, posizionare la replica asincrona in un aggregato che fa parte di un cluster di storage separato nel sito di disaster recovery, con contenuto replicato utilizzando la tecnologia NetApp SnapMirror. NetApp consiglia di disporre di almeno il 10% di spazio libero in un aggregato per ottenere performance dello storage ottimali.

Volumi

I volumi vengono creati e risiedono all'interno degli aggregati. Questo termine talvolta causa confusione perché un volume ONTAP non è un LUN. Un volume ONTAP è un container di gestione per i dati. Un volume può contenere file, LUN o persino oggetti S3. Un volume non occupa spazio, ma viene utilizzato solo per la gestione dei dati contenuti.

Considerazioni sulla progettazione dei volumi

Prima di creare una progettazione di volumi di database, è importante comprendere in che modo il modello i/o di SQL Server e le relative caratteristiche variano in base al carico di lavoro e ai requisiti di backup e ripristino. Consulta i seguenti consigli NetApp per i volumi flessibili:

- Evitare di condividere i volumi tra gli host. Ad esempio, anche se sarebbe possibile creare 2 LUN in un singolo volume e condividere ogni LUN con un host diverso, questo aspetto dovrebbe essere evitato perché complica la gestione. Se si eseguono più istanze di SQL Server sullo stesso host, a meno che non ci si trovi in prossimità del limite di volume su un nodo, è possibile evitare la condivisione di volumi e utilizzare un volume separato per istanza per host per semplificare la gestione dei dati.
- Utilizzare i punti di montaggio NTFS invece delle lettere dell'unità per superare il limite di 26 lettere di unità in Windows. Quando si utilizzano punti di montaggio del volume, si consiglia di assegnare all'etichetta del

volume lo stesso nome del punto di montaggio.

- Se necessario, configurare un criterio di dimensionamento automatico dei volumi per evitare condizioni di spazio insufficiente.
- Se si installa SQL Server su una condivisione SMB, assicurarsi che Unicode sia attivato sui volumi SMB per la creazione delle cartelle.
- Impostare il valore di riserva snapshot nel volume su zero per semplificare il monitoraggio dal punto di vista operativo.
- Disattivare le pianificazioni delle snapshot e i criteri di conservazione. Utilizzare invece SnapCenter per coordinare le copie Snapshot dei volumi di dati di SQL Server.
- Posizionare i database di sistema di SQL Server su un volume dedicato.
- Tempdb è un database di sistema utilizzato da SQL Server come area di lavoro temporanea, in particolare per operazioni DBCC CHECKDB i/o intensive. Pertanto, collocare questo database su un volume dedicato con un set separato di spindle. In ambienti di grandi dimensioni in cui il numero di volumi rappresenta una sfida, è possibile consolidare il tempdb in un numero inferiore di volumi e memorizzarlo nello stesso volume degli altri database di sistema dopo un'attenta pianificazione. La protezione dei dati per tempdb non è una priorità elevata perché questo database viene ricreato ogni volta che SQL Server viene riavviato.
- Collocare i file di dati utente (.mdf) su volumi separati perché si tratta di carichi di lavoro di lettura/scrittura casuali. È comune creare backup del log delle transazioni con maggiore frequenza rispetto ai backup del database. Per questo motivo, inserire i file di log delle transazioni (.ldf) in un volume separato o VMDK dai file di dati in modo che sia possibile creare pianificazioni di backup indipendenti per ciascuno di essi. Questa separazione isola inoltre l'i/o di scrittura sequenziale dei file di log dall'i/o di lettura/scrittura casuale dei file di dati e migliora significativamente le prestazioni di SQL Server.

LUN

- Assicurarsi che i file del database utente e la directory di registro per l'archiviazione del backup del registro si trovino su volumi separati per evitare che il criterio di conservazione sovrascriva gli snapshot quando vengono utilizzati con la tecnologia SnapVault.
- Non combinare file di database e non di database, come file di ricerca full-text, sullo stesso LUN.
- L'inserimento di file secondari del database (come parte di un filegroup) in volumi separati migliora le prestazioni del database di SQL Server. Questa separazione è valida solo se il file del database .mdf non condivide il LUN con altri .mdf file.
- Se si creano LUN con DiskManager o altri strumenti, assicurarsi che la dimensione dell'unità di allocazione sia impostata su 64K per le partizioni durante la formattazione dei LUN.
- Vedere ["Microsoft Windows e MPIO nativo nelle Best practice ONTAP per le SAN moderne"](#) Per applicare il supporto multipathing in Windows ai dispositivi iSCSI nelle proprietà MPIO.

File di database e filegroup

Il corretto posizionamento dei file del database SQL Server su ONTAP è fondamentale durante la fase di distribuzione iniziale. Ciò garantisce prestazioni ottimali, gestione dello spazio, tempi di backup e ripristino che possono essere configurati in base alle esigenze aziendali.

In teoria, SQL Server (a 64 bit) supporta 32.767 database per istanza e 524.272TB di dimensioni del database, sebbene l'installazione tipica abbia in genere diversi database. Tuttavia, il numero di database che SQL Server è in grado di gestire dipende dal carico e dall'hardware. Non è insolito vedere le istanze di SQL Server che

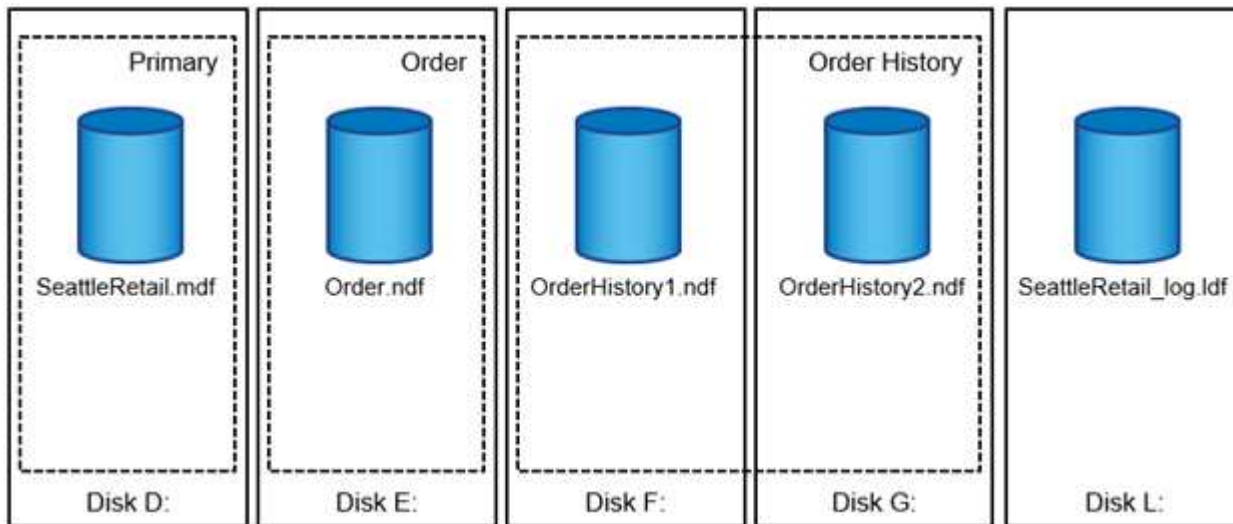
ospitano decine, centinaia o persino migliaia di database di piccole dimensioni.

File di database e filegroup

Ogni database è costituito da uno o più file di dati e da uno o più file di registro delle transazioni. Il registro delle transazioni memorizza le informazioni sulle transazioni del database e tutte le modifiche apportate ai dati da ciascuna sessione. Ogni volta che i dati vengono modificati, SQL Server memorizza informazioni sufficienti nel log delle transazioni per annullare (eseguire il rollback) o ripristinare (riprodurre nuovamente) l'azione. Un log delle transazioni di SQL Server è parte integrante della reputazione di SQL Server in termini di integrità e robustezza dei dati. Il log delle transazioni è fondamentale per le funzionalità di atomicità, coerenza, isolamento e durata (ACID) di SQL Server. SQL Server scrive nel registro delle transazioni non appena si verifica una modifica alla pagina dei dati. Ogni istruzione DML (Data Manipulation Language) (ad esempio, SELECT, INSERT, Update o DELETE) è una transazione completa e il log delle transazioni garantisce che l'intera operazione basata su set abbia luogo, assicurando l'atomicità della transazione.

Ogni database dispone di un file di dati primario che, per impostazione predefinita, ha l'estensione .mdf. Inoltre, ogni database può disporre di file di database secondari. Questi file, per impostazione predefinita, hanno estensioni .ndf.

Tutti i file di database sono raggruppati in filegroup. Un filegroup è l'unità logica, che semplifica l'amministrazione del database. Consentono la separazione tra il posizionamento degli oggetti logici e i file di database fisici. Quando si creano le tabelle degli oggetti del database, si specifica in quale filegroup devono essere posizionati senza preoccuparsi della configurazione del file di dati sottostante.



La possibilità di inserire più file di dati all'interno del filegroup consente di distribuire il carico su diversi dispositivi di archiviazione, migliorando le prestazioni di i/o del sistema. Al contrario, il log delle transazioni non trae vantaggio dai file multipli poiché SQL Server scrive nel log delle transazioni in modo sequenziale.

La separazione tra il posizionamento degli oggetti logici nei filegroup e i file di database fisici consente di ottimizzare il layout dei file di database, ottenendo il massimo dal sottosistema di storage. Il numero di file di dati che supportano un carico di lavoro può essere variato in base alle necessità per supportare i requisiti di i/o e la capacità prevista, senza influire sull'applicazione. Queste variazioni nel layout del database sono trasparenti per gli sviluppatori di applicazioni, che posizionano gli oggetti del database nei filegroup piuttosto che nei file di database.



NetApp recommended evitare l'utilizzo del filegroup primario per oggetti diversi da quelli di sistema. La creazione di un filegroup separato o di un set di filegroup per gli oggetti utente semplifica l'amministrazione del database e il ripristino di emergenza, soprattutto nel caso di database di grandi dimensioni.

Inizializzazione del file di istanza del database

È possibile specificare le dimensioni iniziali del file e i parametri di crescita automatica al momento della creazione del database o dell'aggiunta di nuovi file a un database esistente. SQL Server utilizza un algoritmo di riempimento proporzionale quando sceglie in quale file di dati scrivere i dati. Scrive una quantità di dati proporzionalmente allo spazio libero disponibile nei file. Maggiore è lo spazio libero nel file, maggiore è il numero di scritture gestite.



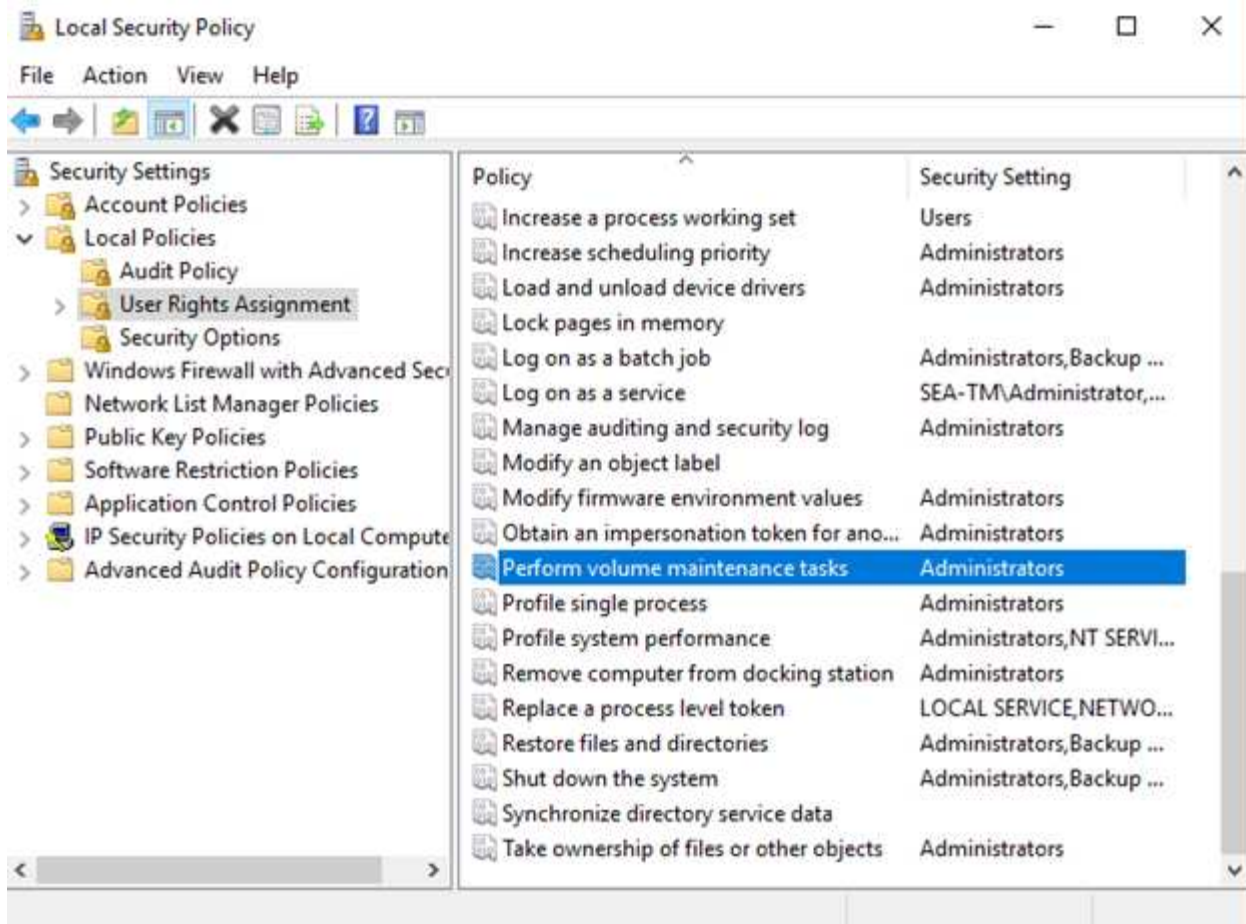
NetApp consiglia che tutti i file nel singolo filegroup abbiano le stesse dimensioni iniziali e parametri di crescita automatica, con la dimensione di crescita definita in megabyte piuttosto che in percentuali. Questo aiuta l'algoritmo di riempimento proporzionale a bilanciare uniformemente le attività di scrittura nei file di dati.

Ogni volta che SQL Server espande i file, riempie di zero lo spazio appena allocato. Questo processo blocca tutte le sessioni che devono scrivere nel file corrispondente o, in caso di crescita del log delle transazioni, genera record di log delle transazioni.

SQL Server azzerà sempre il log delle transazioni e questo comportamento non può essere modificato. Tuttavia, è possibile controllare se i file di dati vengono azzerati attivando o disattivando l'inizializzazione istantanea dei file. L'attivazione dell'inizializzazione immediata dei file consente di velocizzare la crescita dei file di dati e di ridurre il tempo necessario per creare o ripristinare il database.

Un piccolo rischio per la sicurezza è associato all'inizializzazione immediata dei file. Quando questa opzione è attivata, le parti non allocate del file di dati possono contenere informazioni provenienti da file del sistema operativo eliminati in precedenza. Gli amministratori di database possono esaminare tali dati.

È possibile attivare l'inizializzazione immediata dei file aggiungendo l'autorizzazione SA_MANAGE_VOLUME_NAME, nota anche come "Esegui attività di manutenzione del volume" all'account di avvio di SQL Server. È possibile eseguire questa operazione nell'applicazione di gestione dei criteri di protezione locale (secpol.msc), come illustrato nella figura seguente. Aprire le proprietà per l'autorizzazione "Esegui attività di manutenzione del volume" e aggiungere l'account di avvio di SQL Server all'elenco degli utenti.



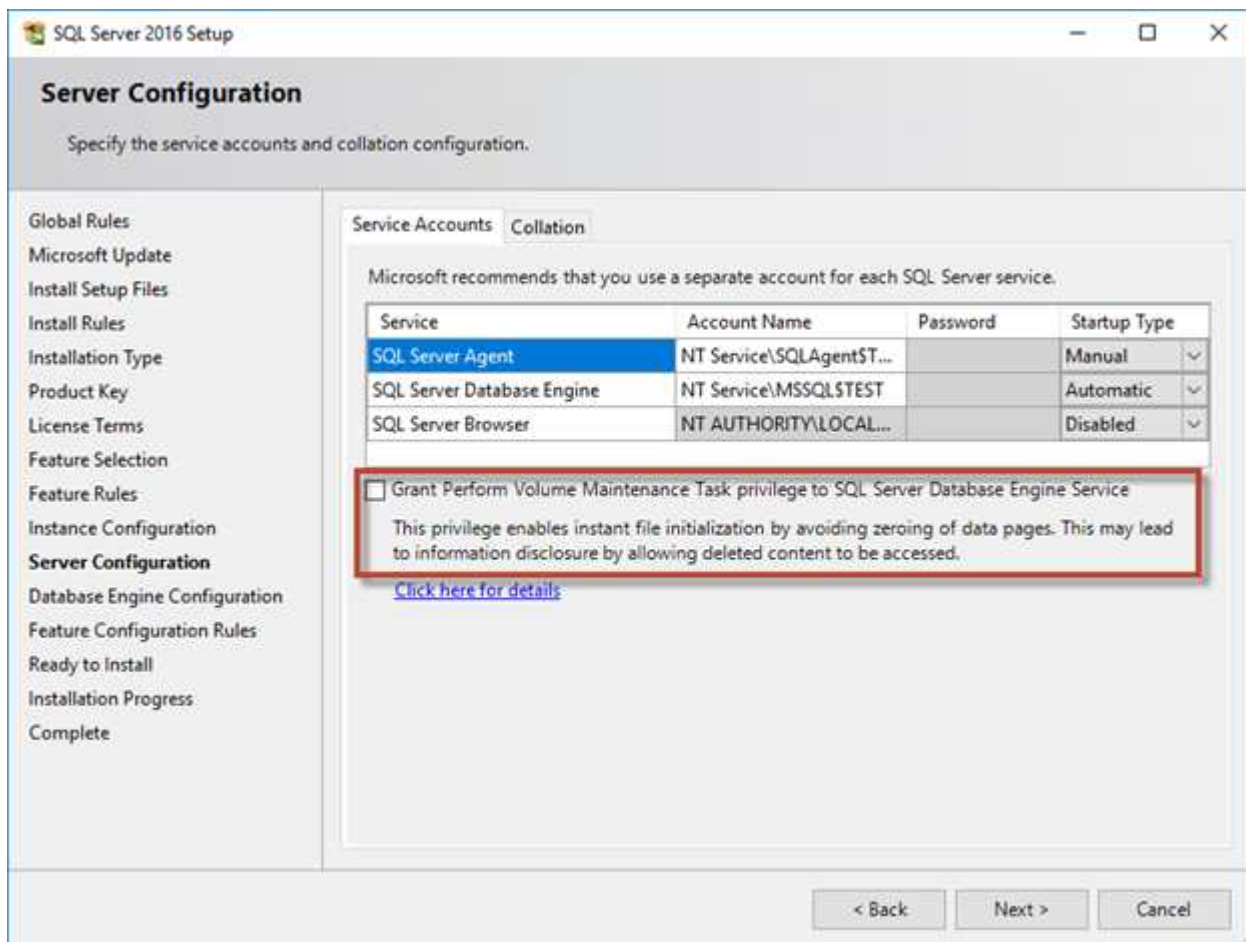
Per verificare se l'autorizzazione è attivata, è possibile utilizzare il codice riportato nell'esempio seguente. Questo codice imposta due flag di traccia che obbligano SQL Server a scrivere informazioni aggiuntive nel registro degli errori, a creare un database di piccole dimensioni e a leggere il contenuto del registro.

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

Quando l'inizializzazione immediata del file non è attivata, il registro degli errori di SQL Server mostra che SQL Server sta azzerando il file di dati mdf oltre a azzerare il file di registro ldf, come illustrato nell'esempio seguente. Quando l'inizializzazione immediata del file è attivata, viene visualizzato solo l'azzeramento del file di registro.

	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\Microsoft SQL Server\90\Shared\
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL Server\MSSQL\DATA\
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.

L'attività Esegui manutenzione volume è semplificata in SQL Server 2016 e viene fornita come opzione durante il processo di installazione. In questa figura viene visualizzata l'opzione per concedere al servizio del motore di database di SQL Server il privilegio di eseguire l'attività di manutenzione del volume.



Un'altra importante opzione del database che controlla le dimensioni dei file di database è l'autohrink. Quando questa opzione è attivata, SQL Server riduce regolarmente i file di database, ne riduce le dimensioni e rilascia spazio al sistema operativo. Questa operazione richiede molte risorse ed è raramente utile perché i file di database crescono di nuovo dopo un certo periodo di tempo quando nuovi dati entrano nel sistema. Il collegamento automatico non deve essere attivato nel database.

Directory di log

La directory di registro è specificata in SQL Server per memorizzare i dati di backup del registro delle transazioni a livello di host. Se si utilizza SnapCenter per eseguire il backup dei file di registro, ciascun host SQL Server utilizzato da SnapCenter deve disporre di una directory di registro host configurata per eseguire i backup dei registri. SnapCenter dispone di un repository di database, pertanto i metadati relativi alle operazioni di backup, ripristino o clonazione vengono memorizzati in un repository di database centrale.

Le dimensioni della directory del registro host vengono calcolate come segue:

Dimensione della directory del log host = ((dimensione massima LDF DB x velocità di modifica giornaliera del log %) x (conservazione snapshot) ÷ (1 - spazio di overhead LUN %))

La formula di dimensionamento della directory del registro host presuppone uno spazio di overhead LUN del 10%

Posizionare la directory di registro su un volume o LUN dedicato. La quantità di dati nella directory del registro host dipende dalle dimensioni dei backup e dal numero di giorni in cui i backup vengono conservati. SnapCenter consente una sola directory di registro host per host SQL Server. È possibile configurare le directory del registro host in SnapCenter → host → Configura plug-in.

NetApp consiglia quanto segue per una directory del registro host:

- Assicurarsi che la directory del registro host non sia condivisa da altri tipi di dati che potrebbero danneggiare i dati dello snapshot di backup.
- Non posizionare database utente o database di sistema su un LUN che ospita punti di montaggio.
- Creare la directory di registro dell'host su un volume dedicato in cui SnapCenter copia i registri delle transazioni.
- Utilizzare le procedure guidate SnapCenter per migrare i database nello storage NetApp in modo che i database vengano memorizzati in posizioni valide, consentendo operazioni di backup e ripristino SnapCenter corrette. Tenere presente che il processo di migrazione causa interruzioni e può causare la disconnessione dei database mentre è in corso la migrazione.
- Per le istanze di cluster di failover (FCI) di SQL Server devono essere presenti le seguenti condizioni:
 - Se si utilizza un'istanza del cluster di failover, il LUN della directory del log host deve essere una risorsa del disco del cluster nello stesso gruppo di cluster dell'istanza di SQL Server di cui viene eseguito il backup in SnapCenter.
 - Se si utilizza un'istanza cluster di failover, i database utente devono essere collocati su LUN condivisi che sono risorse cluster di dischi fisici assegnate al gruppo di cluster associato all'istanza di SQL Server.



Efficienza dello storage

L'efficienza dello storage di ONTAP è ottimizzata per memorizzare e gestire i dati di SQL Server in modo che utilizzino la minore quantità di spazio di storage senza impatti sulle performance.

Le funzionalità di efficienza in termini di spazio, come compressione, compaction e deduplica, sono progettate per aumentare la quantità di dati logici applicabili a una determinata quantità di storage fisico. Il risultato è una riduzione dei costi e dell'overhead di gestione.

Ad un livello elevato, la compressione è un processo matematico in cui gli schemi nei dati vengono rilevati e codificati in modo da ridurre i requisiti di spazio. La deduplica, invece, rileva i blocchi di dati effettivi e ripetuti e rimuove le copie estranee. La tecnologia di compaction consente a più blocchi logici di dati di condividere lo stesso blocco fisico sui supporti.



Per una spiegazione dell'interazione tra efficienza dello storage e prenotazione frazionata, vedere le sezioni seguenti sul thin provisioning.

Compressione

Prima della disponibilità dei sistemi storage all-flash, la compressione basata su array aveva un valore limitato, perché la maggior parte dei carichi di lavoro con i/o-intensive richiedeva un numero molto elevato di spindle per fornire performance accettabili. I sistemi storage contenevano invariabilmente una capacità superiore rispetto a quella richiesta come effetto collaterale dell'elevato numero di dischi. La situazione è cambiata con l'ascesa dello storage a stato solido. Non è più necessario effettuare un provisioning in eccesso significativo dei dischi solo per ottenere buone prestazioni. Lo spazio su disco di un sistema di storage può essere adattato alle effettive esigenze di capacità.

L'aumento della capacità degli IOPS dei dischi a stato solido (SSD) offre quasi sempre risparmi sui costi rispetto ai dischi rotanti, ma la compressione può ottenere ulteriori risparmi aumentando la capacità effettiva dei supporti a stato solido.

Esistono diversi modi per comprimere i dati. Molti database includono proprie funzionalità di compressione, sebbene raramente queste vengano osservate negli ambienti dei clienti. Il motivo è solitamente la penalizzazione delle prestazioni per una **modifica** dei dati compressi, mentre con alcune applicazioni vi sono elevati costi di licenza per la compressione a livello di database. Infine, ci sono le conseguenze globali delle performance sulle operazioni di database. Ha poco senso pagare un costo elevato di licenza per CPU per una CPU che esegue la compressione e la decompressione dei dati piuttosto che un vero lavoro di database. Un'opzione migliore è trasferire il lavoro di compressione sul sistema storage.

Compressione adattiva

La compressione adattiva è stata testata accuratamente con carichi di lavoro Enterprise senza effetti osservati sulle performance, anche in un ambiente all-flash in cui la latenza viene misurata in microsecondi. Alcuni clienti hanno anche segnalato un aumento delle performance con l'utilizzo della compressione, perché i dati rimangono compressi nella cache, aumentando di fatto la quantità di cache disponibile in un controller.

ONTAP gestisce i blocchi fisici in 4KB unità. La compressione adattiva utilizza dimensioni predefinite dei blocchi di compressione di 8KB KB, il che significa che i dati sono compressi in unità da 8KB KB. Corrisponde alle dimensioni dei blocchi di 8KB KB utilizzate più spesso dai database relazionali. Gli algoritmi di compressione diventano più efficienti con la compressione di un numero maggiore di dati come una singola unità. Una dimensione dei blocchi di compressione da 32KB KB sarebbe più efficiente in termini di spazio rispetto a un'unità dei blocchi di compressione da 8KB KB. Ciò significa che la compressione adattiva che utilizza le dimensioni predefinite dei blocchi di 8KB KB produce tassi di efficienza leggermente inferiori, ma esiste anche un vantaggio significativo nell'utilizzo di dimensioni inferiori dei blocchi di compressione. I carichi di lavoro dei database includono un'elevata attività di sovrascrittura. La sovrascrittura di un 8KB di un blocco di dati 32KB compresso richiede la lettura dell'intero 32KB di dati logici, la decompressione, l'aggiornamento della regione 8KB richiesta, la ricompressione e quindi la riscrittura dell'intero 32KB sui dischi. Si tratta di un'operazione molto costosa per un sistema storage ed è il motivo per cui alcuni storage array concorrenti basati su dimensioni dei blocchi di compressione più grandi implicano anche una significativa penalizzazione delle performance con i carichi di lavoro dei database.



Le dimensioni dei blocchi utilizzate dalla compressione adattiva possono essere aumentate fino a 32KB KB. Questo può migliorare l'efficienza di archiviazione e dovrebbe essere considerato per i file inattivi come i log delle transazioni e i file di backup quando una quantità sostanziale di tali dati è memorizzata nell'array. In alcune situazioni, i database attivi che utilizzano dimensioni blocco 16KB KB o 32KB KB possono anche trarre vantaggio dall'aumento delle dimensioni blocco della compressione adattiva per adeguarsi. Consulta un NetApp o un rappresentante del partner per ottenere indicazioni relative all'adeguatezza del tuo carico di lavoro.



Le dimensioni dei blocchi di compressione superiori a 8KB KB non devono essere utilizzate insieme alla deduplica nelle destinazioni di backup in streaming. Il motivo è che piccole modifiche ai dati di backup influiscono sulla finestra di compressione 32KB. Se la finestra si sposta, i dati compressi risultanti differiscono per l'intero file. La deduplica si verifica dopo la compressione, il che significa che il motore di deduplica vede ogni backup compresso in modo diverso. Se è richiesta la deduplica dei backup in streaming, è consigliabile utilizzare solo la compressione adattiva per blocchi da 8KB KB. La compressione adattiva è preferibile, perché funziona a blocchi di dimensioni inferiori e non interrompe l'efficienza di deduplica. Per motivi simili, la compressione lato host interferisce anche con l'efficienza della deduplica.

Allineamento delle compressioni

La compressione adattiva in un ambiente di database richiede alcune considerazioni sull'allineamento dei blocchi di compressione. Ciò rappresenta solo una preoccupazione per i dati che sono soggetti a sovrascritture casuali di blocchi molto specifici. Questo approccio è simile in teoria all'allineamento complessivo del file system, dove l'inizio di un file system deve essere allineato al limite di un dispositivo 4K e la dimensione di blocco di un file system deve essere un multiplo di 4K.

Ad esempio, una scrittura 8KB in un file viene compressa solo se si allinea con un limite 8KB all'interno del file system stesso. Questo punto significa che deve rientrare nel primo 8KB del file, nel secondo 8KB del file e così via. Il modo più semplice per garantire un corretto allineamento è utilizzare il tipo di LUN corretto, ogni partizione creata dovrebbe avere un offset dall'inizio del dispositivo che è un multiplo di 8K, e utilizzare una dimensione del blocco del file system che è un multiplo della dimensione del blocco del database.

Dati come backup o log delle transazioni sono operazioni scritte in sequenza che coprono più blocchi, tutti compressi. Pertanto, non è necessario considerare l'allineamento. L'unico modello di i/o che desta preoccupazione sono le sovrascritture casuali dei file.

Compaction dei dati

La data compaction è una tecnologia che migliora l'efficienza di compressione. Come indicato in precedenza, la sola compressione adattiva può garantire risparmi 2:1:1 al meglio, perché è limitata alla memorizzazione di un i/o da 8KB KB in un blocco WAFL da 4KB KB. I metodi di compressione con dimensioni dei blocchi maggiori garantiscono una maggiore efficienza. Tuttavia, non sono adatte per i dati che sono soggetti a piccole sovrascritture dei blocchi. La decompressione di 32KB unità di dati, l'aggiornamento di una porzione 8KB, la ricomprensione e la riscrittura sui dischi crea overhead.

La data compaction opera consentendo di memorizzare più blocchi logici all'interno dei blocchi fisici. Ad esempio, un database con dati altamente comprimibili come testo o blocchi parzialmente completi può comprimere da 8KB a 1KB. Senza la compaction, quei 1KB PB di dati continuerebbero ad occupare un intero blocco da 4KB KB. Inline data compaction per memorizzare 1KB TB di dati compressi in sole 1KB:1 di spazio fisico insieme ad altri dati compressi. Non si tratta di una tecnologia di compressione, ma semplicemente di un metodo più efficiente per allocare spazio sulle unità e quindi non dovrebbe creare alcun effetto rilevabile sulle prestazioni.

Il grado di risparmio ottenuto varia. I dati già compressi o crittografati non possono in genere essere

ulteriormente compressi, e pertanto tali set di dati non traggono vantaggio dalla compattazione. Al contrario, i file di dati appena inizializzati contenenti poco più dei metadati dei blocchi e la compressione di zeri fino a 80:1.

Efficienza di conservazione sensibile alla temperatura

L'efficienza di stoccaggio sensibile alla temperatura (TSSE) è disponibile in ONTAP 9.8 e versioni successive. Si affida alle mappe termiche di accesso ai blocchi per identificare i blocchi a cui si accede raramente e comprimerli con una maggiore efficienza.

Deduplica

La deduplica consiste nella rimozione di dimensioni dei blocchi duplicate da un set di dati. Ad esempio, se lo stesso blocco 4KB esistesse in 10 file diversi, la deduplica reindirizzerebbe quel blocco 4KB in tutti i file 10 allo stesso blocco fisico da 4KB KB. Il risultato sarebbe un miglioramento di 10:1 volte in efficienza per quei dati.

Dati come i LUN di avvio guest di VMware si deduplicano in genere in modo estremamente efficace poiché sono costituiti da più copie degli stessi file del sistema operativo. Sono state osservate un'efficienza pari o superiore a 100:1.

Alcuni dati non contengono dati duplicati. Ad esempio, un blocco Oracle contiene un'intestazione univoca a livello globale per il database e un trailer quasi univoco. Di conseguenza, la deduplica di un database Oracle raramente offre un risparmio superiore al 1%. La deduplica con i database MS SQL è leggermente migliore, ma i metadati univoci a livello di blocco rimangono un limite.

In pochi casi, sono stati osservati risparmi di spazio fino al 15% nei database con blocchi di dimensioni grandi e 16KB. Il 4KB iniziale di ciascun blocco contiene la testata unica a livello globale, mentre il 4KB finale contiene il rimorchio quasi unico. I blocchi interni sono candidati per la deduplica, sebbene in pratica ciò sia quasi interamente attribuito alla deduplica di dati azzerati.

Molti array della concorrenza rivendicano la capacità di deduplicare i database sulla base del presupposto che un database venga copiato più volte. Anche in questo caso è possibile utilizzare la deduplica NetApp, ma ONTAP offre un'opzione migliore: La tecnologia FlexClone di NetApp. Il risultato finale è lo stesso; vengono create più copie di un database che condividono la maggior parte dei blocchi fisici sottostanti. L'utilizzo di FlexClone è molto più efficiente della necessità di dedicare tempo alla copia e alla deduplica dei file di database. In effetti, non viene effettuata alcuna duplicazione piuttosto che deduplica, poiché al primo posto non viene mai creato un duplicato.

Efficienza e thin provisioning

Le funzionalità di efficienza sono forme di thin provisioning. Ad esempio, una LUN da 100GB GB che occupa un volume da 100GB GB potrebbe comprimere fino a 50GB GB. Non ci sono risparmi effettivi ancora realizzati perché il volume è ancora 100GB. Le dimensioni del volume devono essere innanzitutto ridotte in modo che lo spazio salvato possa essere utilizzato in un'altra posizione del sistema. Se successivamente le modifiche apportate al LUN da 100GB GB rendono i dati meno comprimibili, il LUN aumenta le dimensioni e il volume potrebbe riempirsi.

Il thin provisioning è vivamente consigliato in quanto consente di semplificare la gestione, offrendo al contempo un sostanziale miglioramento della capacità utilizzabile con conseguenti risparmi sui costi. Il motivo è semplice: Gli ambienti di database includono spesso molto spazio vuoto, un elevato numero di volumi e LUN e dati comprimibili. Il thick provisioning crea la riserva di spazio sullo storage per volumi e LUN, nel caso in cui un giorno raggiungano il 100% di riempimento e contengano dati non comprimibili al 100%. È improbabile che ciò accada mai. Il thin provisioning consente di recuperare lo spazio e di utilizzarlo altrove e consente la gestione della capacità basata sul sistema storage stesso piuttosto che su molti volumi e LUN più piccoli.

Alcuni clienti preferiscono utilizzare il thick provisioning, per carichi di lavoro specifici o generalmente basato su pratiche operative e di approvvigionamento consolidate.



Se un volume viene sottoposto a thick provisioning, è necessario fare attenzione a disattivare completamente tutte le funzionalità di efficienza per quel volume, inclusa la decompressione e la rimozione della deduplica tramite il `sis undo` comando. Il volume non dovrebbe comparire nell'`volume efficiency show`output. In tal caso, il volume è ancora parzialmente configurato per le funzioni di efficienza. Di conseguenza, la sovrascrittura garantisce un funzionamento diverso, aumentando le possibilità che le sovrascritture causino l'esaurimento inaspettato dello spazio del volume, con conseguenti errori di i/o del database.

Best practice di efficienza

NetApp consiglia quanto segue:

Valori predefiniti AFF

I volumi creati su ONTAP in esecuzione su un sistema AFF all-flash vengono sottoposti a thin provisioning con tutte le funzionalità di efficienza inline abilitate. Sebbene in genere i database non beneficino della deduplica e possano includere dati non comprimibili, le impostazioni predefinite sono comunque appropriate per quasi tutti i carichi di lavoro. ONTAP è progettato per elaborare in modo efficiente tutti i tipi di dati e gli schemi i/o, indipendentemente dal fatto che comportino risparmi. Le impostazioni predefinite devono essere modificate solo se le ragioni sono pienamente comprese e se vi è un vantaggio a deviare.

Raccomandazioni generali

- Se i volumi e/o le LUN non sono dotati di thin provisioning, è necessario disabilitare tutte le impostazioni di efficienza perché queste funzionalità non offrono risparmi e la combinazione del thick provisioning con l'efficienza dello spazio può causare comportamenti imprevisti, inclusi errori di spazio esaurito.
- Se i dati non sono soggetti a sovrascritture, ad esempio con i backup o i log delle transazioni dei database, puoi ottenere una maggiore efficienza abilitando TSSE con un periodo di raffreddamento ridotto.
- Alcuni file potrebbero contenere una quantità significativa di dati non comprimibili, ad esempio quando la compressione è già abilitata a livello di applicazione dei file sono crittografati. Se uno di questi scenari è vero, considerare la possibilità di disattivare la compressione per consentire un funzionamento più efficiente su altri volumi che contengono dati comprimibili.
- Non utilizzare sia la compressione 32KB che la deduplica con i backup del database. Vedere la sezione [Compressione adattiva](#) per ulteriori informazioni.

Compressione dei database

SQL Server dispone inoltre di funzionalità per comprimere e gestire in modo efficiente i dati. Attualmente SQL Server supporta due tipi di compressione dati: Compressione riga e compressione pagina.

La compressione riga modifica il formato di memorizzazione dei dati. Ad esempio, cambia interi e decimali nel formato a lunghezza variabile invece del formato a lunghezza fissa nativo. Inoltre, le stringhe di caratteri a lunghezza fissa vengono modificate nel formato a lunghezza variabile eliminando gli spazi vuoti. La compressione della pagina implementa la compressione della riga e altre due strategie di compressione (compressione del prefisso e compressione del dizionario). Per ulteriori dettagli sulla compressione delle pagine, consultare ["Implementazione della compressione pagina"](#).

La compressione dei dati è attualmente supportata nelle edizioni Enterprise, Developer e Evaluation di SQL Server 2008 e versioni successive. Sebbene la compressione possa essere eseguita dal database stesso, ciò si verifica raramente in un ambiente SQL Server.

Di seguito sono riportati i suggerimenti per la gestione dello spazio per i file di dati di SQL Server

- Utilizzo del thin provisioning negli ambienti SQL Server per migliorare l'utilizzo dello spazio e ridurre i requisiti generali di storage quando viene utilizzata la funzionalità di garanzia di spazio.
 - Utilizza l'espansione automatica per la maggior parte delle configurazioni di implementazione più comuni, perché l'amministratore dello storage deve solo monitorare l'utilizzo dello spazio nell'aggregato.
- Non abilitare la deduplica su alcun volume su FAS contenente file di dati di SQL Server a meno che il volume non contenga più copie degli stessi dati, come ad esempio il ripristino del database da un backup su un singolo volume.

Bonifica dello spazio

Il recupero di spazio può essere avviato periodicamente per recuperare spazio inutilizzato in un LUN. Con SnapCenter, puoi usare il seguente comando PowerShell per iniziare il recupero dello spazio.

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

Se è necessario eseguire il recupero di spazio, questo processo deve essere eseguito durante i periodi di attività bassa, poiché inizialmente consuma cicli sull'host.

Protezione dei dati

Le strategie di backup dei database devono basarsi su requisiti aziendali identificati, non su capacità teoriche. Combinando la tecnologia Snapshot di ONTAP e sfruttando le API di Microsoft SQL Server, è possibile eseguire rapidamente un backup coerente delle applicazioni indipendentemente dalle dimensioni dei database utente. Per requisiti di gestione dei dati più avanzati o scale-out, NetApp offre SnapCenter.

SnapCenter

SnapCenter è il software di data Protection di NetApp per le applicazioni aziendali. I database di SQL Server possono essere protetti in modo rapido e semplice con il plug-in SnapCenter per SQL Server e con operazioni del sistema operativo gestite dal plug-in SnapCenter per Microsoft Windows.

L'istanza di SQL Server può essere un'installazione autonoma, un'istanza cluster di failover o può essere un gruppo di disponibilità sempre attivo. Il risultato è che, grazie a un singolo pannello di controllo, i database possono essere protetti, clonati e ripristinati da una copia primaria o secondaria. SnapCenter può gestire database SQL Server sia on-premise, nel cloud che in configurazioni ibride. Le copie dei database possono essere create in pochi minuti sull'host originale o alternativo per lo sviluppo o per il reporting.

SQL Server richiede inoltre un coordinamento tra il sistema operativo e lo storage per garantire che i dati corretti siano presenti negli snapshot al momento della creazione. Nella maggior parte dei casi, l'unico metodo sicuro per eseguire questa operazione è SnapCenter o T-SQL. Gli snapshot creati senza questo coordinamento aggiuntivo potrebbero non essere recuperabili in modo affidabile.

Per ulteriori informazioni sul plug-in di SQL Server per SnapCenter, vedere ["TR-4714: Guida alle Best practice per SQL Server con NetApp SnapCenter"](#).

Protezione del database mediante snapshot T-SQL

In SQL Server 2022, Microsoft ha introdotto le istantanee T-SQL che offrono un percorso per la creazione di script e l'automazione delle operazioni di backup. Invece di eseguire copie di dimensioni normali, è possibile preparare il database per le snapshot. Una volta che il database è pronto per il backup, è possibile sfruttare le API REST di ONTAP per creare snapshot.

Di seguito è riportato un esempio di flusso di lavoro di backup:

1. Bloccare un database con il comando ALTER. In questo modo il database viene preparato per uno snapshot coerente sullo storage sottostante. Dopo il blocco è possibile scongelare il database e registrare lo snapshot con il comando di BACKUP.
2. Eseguire snapshot di più database sui volumi di storage contemporaneamente con il nuovo GRUPPO DI BACKUP e i comandi DEL SERVER DI BACKUP.
3. Eseguire backup COMPLETI o backup COMPLETI COPY_ONLY. Anche questi backup sono registrati in msdb.
4. Eseguire il recovery point-in-time utilizzando i backup di log eseguiti con il normale approccio di streaming dopo il backup COMPLETO delle snapshot. Se lo si desidera, sono supportati anche i backup differenziali in streaming.

Per ulteriori informazioni, vedere ["Documentazione Microsoft per conoscere le istantanee T-SQL"](#).



NetApp recommended Using SnapCenter to create Snapshot copy. Anche il metodo T-SQL descritto sopra funziona, ma SnapCenter offre un'automazione completa sul processo di backup, ripristino e cloning. Esegue inoltre il rilevamento per garantire che vengano creati gli snapshot corretti. Non è necessaria alcuna pre-configurazione.

Gruppo di disponibilità di SQL Server con SnapCenter

SnapCenter supporta il backup del database del gruppo di disponibilità SQL Server configurato con il cluster di failover Windows.

Il plugin SnapCenter per Microsoft SQL Server deve essere installato su tutti i nodi del cluster di failover del server Windows. Consultare i ["documentazione"](#) prerequisiti di ON e la procedura per configurare i plug-in di SnapCenter.

SnapCenter rileva che tutti i database, le istanze e i gruppi di disponibilità negli host e nelle risorse di Windows sono elencati nella pagina delle risorse di SnapCenter.

Protezione dei database nel gruppo di disponibilità always-on

I database del gruppo di disponibilità possono essere protetti in più modi.

- Backup a livello di database: Selezionare il database di disponibilità per la pagina delle risorse del database, aggiungere il criterio costituito dal backup completo/registro, pianificare il backup. SnapCenter utilizza il backup indipendentemente dal ruolo del database, sia che si tratti di una replica primaria che di una replica secondaria. La protezione può anche essere configurata aggiungendo database al gruppo di risorse.
- Backup a livello di istanza: Selezionare l'istanza per proteggere tutti i database in esecuzione sull'istanza in base al criterio selezionato. Viene eseguito il backup di tutti i database, incluso il database di disponibilità in esecuzione come replica primaria o secondaria, utilizzando SnapCenter. La protezione può anche essere configurata aggiungendo un'istanza al gruppo di risorse.

- Backup a livello di gruppo di disponibilità: Durante la configurazione del criterio, SnapCenter dispone di un'opzione avanzata per il backup a livello di gruppo di disponibilità. L'impostazione del gruppo di disponibilità nel criterio consente agli utenti di selezionare la preferenza di replica per il backup. È possibile selezionare la replica primaria, secondaria o tutte. L'opzione predefinita si basa sulla replica di backup impostata nella configurazione del gruppo di disponibilità di SQL Server.

L'impostazione del gruppo di disponibilità nel criterio SnapCenter verrà applicata solo se il backup a livello di gruppo di disponibilità viene utilizzato per proteggere i database del gruppo di disponibilità e non viene applicato per il backup a livello di database o istanza.



NetApp consiglia di utilizzare il backup a livello di disponibilità per il backup di tutta la replica in esecuzione sullo storage NetApp ONTAP.

Configurazione del backup del registro in SnapCenter

Se il gruppo di disponibilità è impostato su un'installazione autonoma di SQL Server, è necessario montare un disco dedicato su ciascun nodo di un cluster di failover del server Windows. Utilizzare un disco dedicato per configurare la directory del registro per salvare i backup del registro delle transazioni.

Se il gruppo di disponibilità è impostato sul cluster di failover di SQL Server, è necessario creare un disco cluster nell'istanza del cluster di failover di SQL Server per la directory del registro host.

Ripristino del database nella configurazione del gruppo di disponibilità con SnapCenter

- SnapCenter fornisce l'opzione di reseeding per ripristinare automaticamente il database dall'ultimo snapshot disponibile nella replica secondaria. L'operazione di risigillatura ripristinerà automaticamente e unirà il backup del database al gruppo di disponibilità.
- Un modo alternativo per ripristinare il database di replica nel gruppo di disponibilità consiste nell'interrompere il gruppo di disponibilità ed eseguire il ripristino completo e completo del registro. Utilizzare SnapCenter per ripristinare il database in modalità norecovery, quindi utilizzare SQL Server Management Studio o T-SQL per accedere nuovamente al gruppo di disponibilità del database.
- Per ripristinare solo il sottoinsieme di dati, è possibile utilizzare le funzionalità di cloning di SnapCenter per creare una copia clone del database. La copia del database viene creata in pochi minuti utilizzando SnapCenter, quindi esportare i dati nella replica primaria utilizzando gli strumenti nativi di SQL Server.

Per le procedure consigliate per configurare il layout dello storage del database in modo da soddisfare i requisiti RTO e RPO, vedere ["TR-4714 Best practice per Microsoft SQL Server che utilizza NetApp SnapCenter"](#).



SnapCenter non supporta il gruppo di disponibilità distribuita e il gruppo di disponibilità contenuta.

Disaster recovery

Disaster recovery

I database e le infrastrutture applicative aziendali spesso richiedono la replica per proteggersi da disastri naturali o interruzioni impreviste del business, con tempi di inattività minimi.

La funzionalità di replica del gruppo di disponibilità always-on di SQL Server può essere un'opzione eccellente e NetApp offre opzioni per integrare la protezione dei dati con Always-on. In alcuni casi, tuttavia, è consigliabile

prendere in considerazione la tecnologia di replica ONTAP. Sono disponibili tre opzioni di base.

SnapMirror

La tecnologia SnapMirror offre una soluzione aziendale rapida e flessibile per la replica dei dati su LAN e WAN. La tecnologia SnapMirror trasferisce solo i blocchi di dati modificati a destinazione dopo la creazione del mirror iniziale, riducendo in modo significativo i requisiti di larghezza di banda della rete. Può essere configurato in modalità sincrona o asincrona.

Sincronizzazione attiva di NetApp MetroCluster e SnapMirror

Per molti clienti, il disaster recovery non richiede solo una copia remota dei dati, ma anche la capacità di sfruttarli in maniera rapida. NetApp offre due tecnologie che soddisfano questa esigenza: MetroCluster e SnapMirror Active Sync

MetroCluster fa riferimento a ONTAP in una configurazione hardware che include storage con mirroring sincrono di basso livello e numerose funzionalità aggiuntive. Le soluzioni integrate come MetroCluster semplificano le complesse e scalabili infrastrutture di database, applicazioni e virtualizzazione. Sostituisce diversi prodotti e strategie di protezione dati esterni con un unico semplice storage array centrale. Fornisce inoltre backup, recovery, disaster recovery e alta disponibilità (ha) integrati in un singolo sistema storage in cluster.

SnapMirror Active Sync si basa su SnapMirror Synchronous. Con MetroCluster, ogni controller ONTAP è responsabile della replica dei dati dell'unità in una posizione remota. Con la sincronizzazione attiva di SnapMirror, avrai essenzialmente due sistemi ONTAP diversi che mantengono copie indipendenti dei dati LUN, ma cooperano per presentare una singola istanza di tale LUN. Dal punto di vista dell'host, si tratta di una singola entità LUN.

Confronto SM-AS e MCC

SM-AS e MetroCluster sono simili per quanto riguarda le funzionalità generali, ma esistono importanti differenze nel modo in cui è stata implementata la replica RPO=0 e nel modo in cui viene gestita. Anche se è possibile utilizzare la modalità asincrona e sincrona di SnapMirror come parte di un piano di disaster recovery, non sono progettate come tecnologie di replica ha.

- Una configurazione MetroCluster è più simile a un cluster integrato con nodi distribuiti tra i siti. SM-AS si comporta come due cluster altrimenti indipendenti che stanno cooperando nel servire un RPO selezionato=0 LUN replicati in modo sincrono.
- I dati in una configurazione MetroCluster sono accessibili solo da un determinato sito alla volta. Una seconda copia dei dati è presente sul sito opposto, ma i dati sono passivi. Non è possibile accedervi senza un failover del sistema storage.
- MetroCluster e SM-as eseguono il mirroring a diversi livelli. Il mirroring MetroCluster viene eseguito al livello RAID. I dati di basso livello sono memorizzati in un formato di mirroring utilizzando SyncMirror. L'utilizzo del mirroring è praticamente invisibile ai livelli di LUN, volume e protocollo.
- Al contrario, il mirroring SM-AS avviene a livello di protocollo. I due cluster sono complessivamente cluster indipendenti. Una volta sincronizzate le due copie di dati, i due cluster devono solo eseguire il mirroring delle scritture. Quando si verifica una scrittura su un cluster, questa viene replicata nell'altro cluster. La scrittura viene riconosciuta all'host solo quando la scrittura è stata completata su entrambi i siti. A parte questo comportamento di suddivisione del protocollo, i due cluster sono altrimenti normali cluster ONTAP.
- Il ruolo principale di MetroCluster è la replica su larga scala. Puoi replicare un intero array con RPO=0 e RTO prossimo allo zero. Questo semplifica il processo di failover perché esiste un solo "problema" da eseguire e consente una scalabilità perfetta in termini di capacità e IOPS.

- Un caso d'utilizzo chiave per SM-AS è la replica granulare. A volte non vuoi replicare tutti i dati come una singola unità oppure devi eseguire il failover selettivo su alcuni carichi di lavoro.
- Un altro caso d'utilizzo chiave per SM-AS è per operazioni Active-Active, dove desideri che siano disponibili copie dei dati completamente utilizzabili su due cluster diversi situati in due posizioni diverse con caratteristiche di performance identiche e, se desiderato, non richiedere l'estensione della SAN tra i siti. Le applicazioni possono essere già in esecuzione su entrambi i siti, riducendo così l'RTO complessivo durante le operazioni di failover.

SnapMirror

Di seguito sono riportati alcuni consigli su SnapMirror per SQL Server:

- In caso di utilizzo di SMB, la SVM di destinazione deve appartenere allo stesso dominio Active Directory del quale fa parte la SVM di origine, in modo da non interrompere le liste per il controllo degli accessi (ACL) archiviate nei file NAS durante il ripristino in caso di disastro.
- L'utilizzo di nomi di volumi di destinazione identici ai nomi di volumi di origine non è necessario, ma può semplificare la gestione del processo di montaggio dei volumi di destinazione nella destinazione. Se viene utilizzato SMB, occorre rendere identico il namespace NAS di destinazione nei percorsi e nella struttura delle directory al namespace di origine.
- Per motivi di coerenza, non pianificare gli update SnapMirror dai controller. Attiva invece gli update di SnapMirror da SnapCenter per aggiornare SnapMirror al termine del backup completo o del log.
- Distribuire volumi che contengono dati SQL Server tra diversi nodi nel cluster per consentire a tutti i nodi del cluster di condividere l'attività di replica di SnapMirror. Questa distribuzione ottimizza l'utilizzo delle risorse dei nodi.
- Utilizza la replica sincrona in cui la richiesta di un rapido data recovery è maggiore e soluzioni asincrone per la flessibilità negli RPO.

Per ulteriori informazioni su SnapMirror, vedere ["TR-4015: Guida alle Best practice e alla configurazione di SnapMirror per ONTAP 9"](#).

MetroCluster

Architettura

La distribuzione di Microsoft SQL Server con ambiente MetroCluster richiede alcune spiegazioni sulla progettazione fisica di un sistema MetroCluster.

MetroCluster esegue il mirroring sincrono di dati e configurazione tra due cluster ONTAP in posizioni separate o domini di errore. MetroCluster offre storage sempre disponibile per le applicazioni gestendo automaticamente due obiettivi:

- RPO (Zero Recovery Point Objective) eseguendo il mirroring sincrono dei dati scritti nel cluster.
- RTO (Recovery Time Objective) quasi nullo attraverso la configurazione del mirroring e l'automazione dell'accesso ai dati del secondo sito.

MetroCluster offre semplicità con mirroring automatico dei dati e configurazione tra i due cluster indipendenti situati nei due siti. Poiché lo storage viene fornito all'interno di un cluster, viene automaticamente eseguito il mirroring nel secondo cluster del secondo sito. NetApp SyncMirror® fornisce una copia completa di tutti i dati con RPO pari a zero. Ciò significa che i carichi di lavoro da un sito possono passare in qualsiasi momento al sito opposto e continuare a fornire i dati senza perdita di dati. MetroCluster gestisce il processo di switchover per fornire accesso ai dati forniti da NAS e SAN al secondo sito. La progettazione di MetroCluster come

soluzione validata contiene dimensionamento e configurazione che consente di eseguire uno switchover entro i periodi di timeout del protocollo (generalmente inferiori a 120 secondi). Questo consente un RPO prossimo allo zero e le applicazioni possono continuare ad accedere ai dati senza incorrere in guasti. Il MetroCluster è disponibile in diverse variazioni definite dal fabric dello storage back-end.

MetroCluster è disponibile in 3 diverse configurazioni

- Coppie HA con connettività IP
- Coppie HA con connettività FC
- Controller singolo con connettività FC



Il termine connettività si riferisce alla connessione cluster utilizzata per la replica tra siti. Non si riferisce ai protocolli host. Tutti i protocolli lato host sono supportati come di consueto in una configurazione MetroCluster indipendentemente dal tipo di connessione utilizzata per la comunicazione tra cluster.

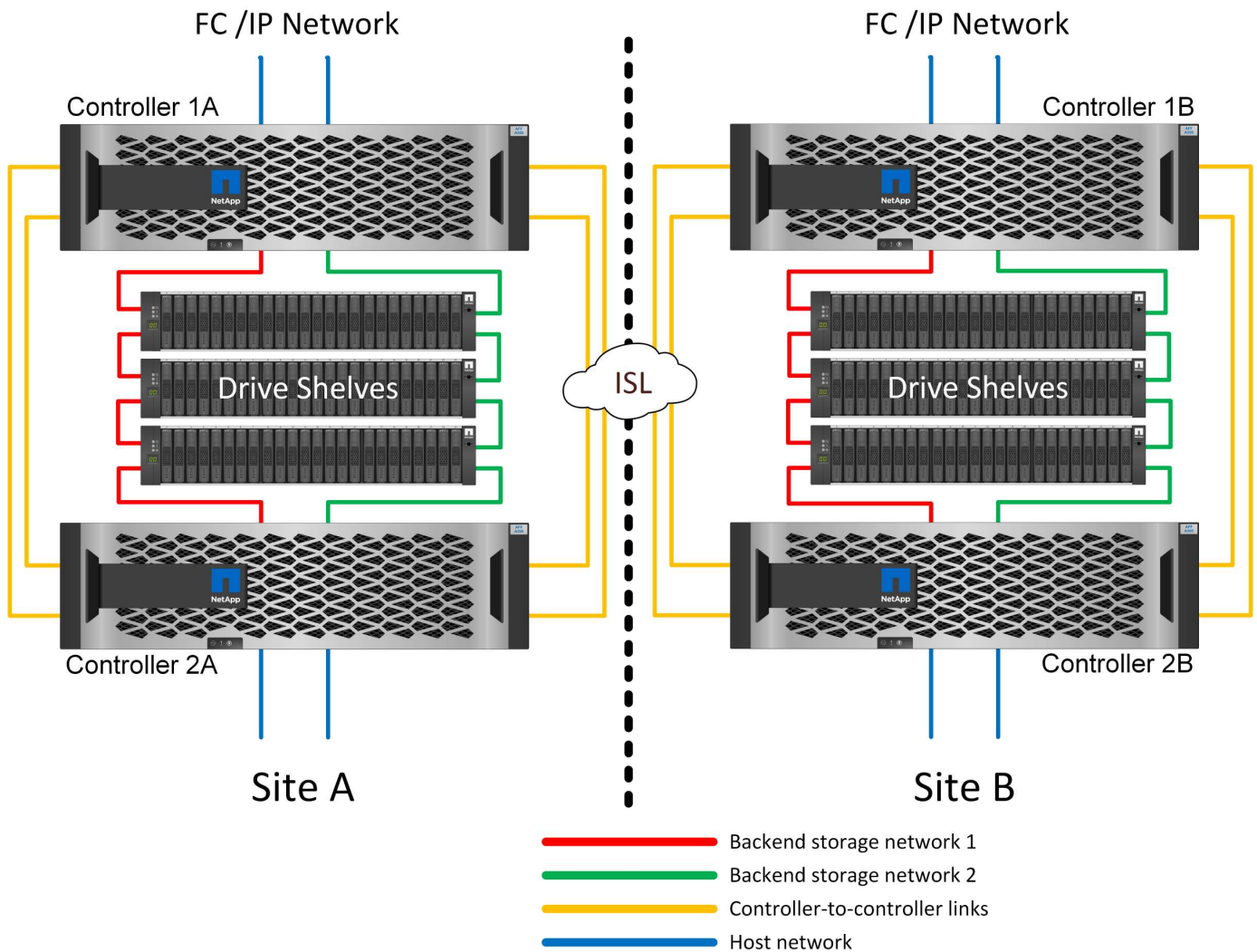
IP MetroCluster

La configurazione MetroCluster IP ha-Pair utilizza due o quattro nodi per sito. Questa opzione di configurazione aumenta la complessità e i costi rispetto all'opzione a due nodi, ma offre un vantaggio importante: La ridondanza intrasite. Un semplice errore del controller non richiede l'accesso ai dati nella WAN. L'accesso ai dati rimane locale attraverso il controller locale alternativo.

La maggior parte dei clienti sceglie la connettività IP perché i requisiti dell'infrastruttura sono più semplici. In passato, la connettività cross-site ad alta velocità era generalmente più semplice da fornire utilizzando gli switch FC e in fibra scura, ma oggi i circuiti IP ad alta velocità e a bassa latenza sono più prontamente disponibili.

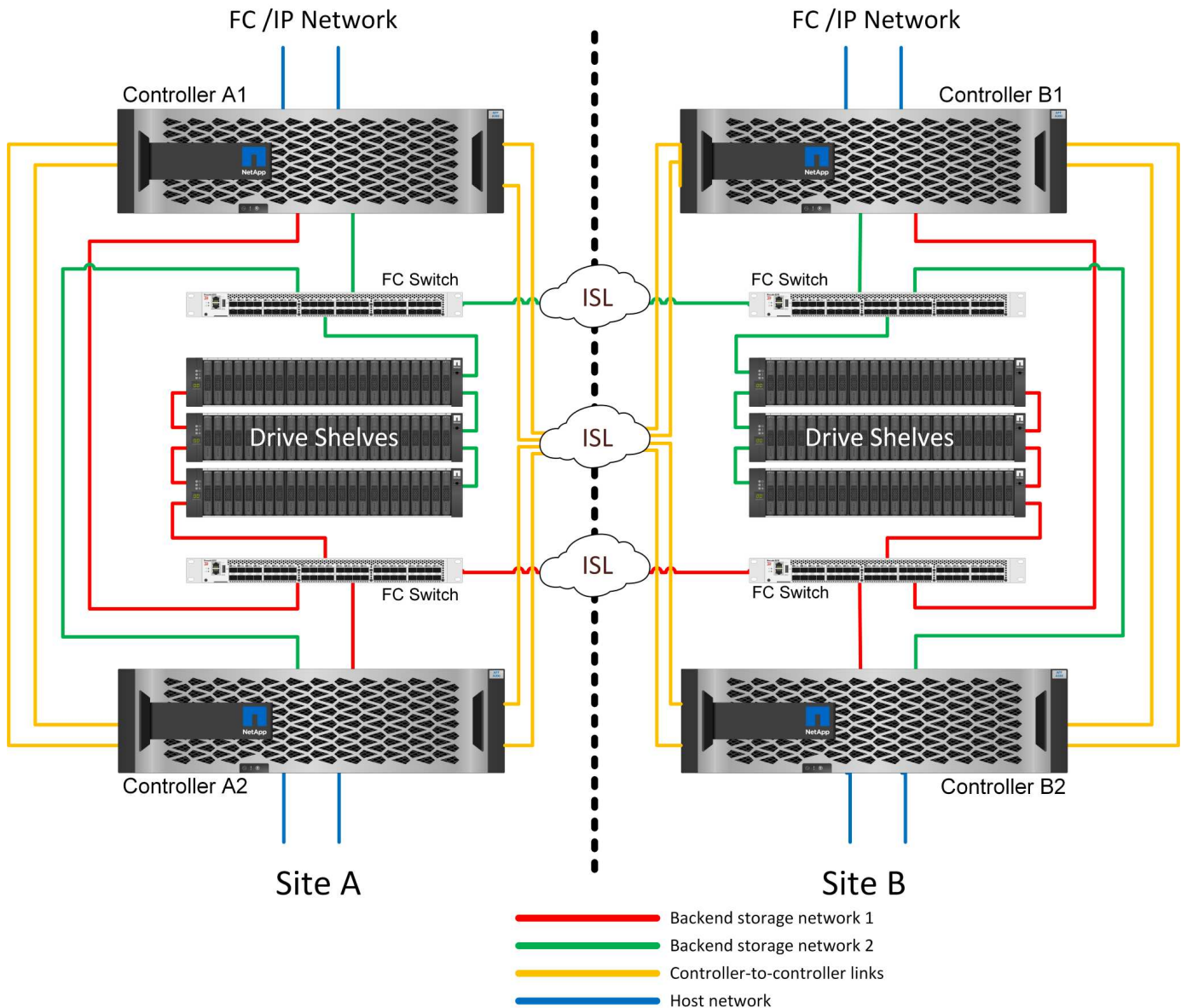
L'architettura è anche più semplice perché le uniche connessioni cross-site sono per i controller. Nei MetroClusters collegati a FC SAN, un controller scrive direttamente sulle unità del sito opposto e quindi richiede connessioni SAN, switch e bridge aggiuntivi. Al contrario, un controller in una configurazione IP scrive sulle unità opposte tramite il controller.

Per ulteriori informazioni, consultare la documentazione ufficiale di ONTAP e ["Architettura e progettazione della soluzione IP di MetroCluster"](#).



MetroCluster HA-Pair FC SAN-Attached

La configurazione ha-Pair MetroCluster FC utilizza due o quattro nodi per sito. Questa opzione di configurazione aumenta la complessità e i costi rispetto all'opzione a due nodi, ma offre un vantaggio importante: La ridondanza intrasite. Un semplice errore del controller non richiede l'accesso ai dati nella WAN. L'accesso ai dati rimane locale attraverso il controller locale alternativo.

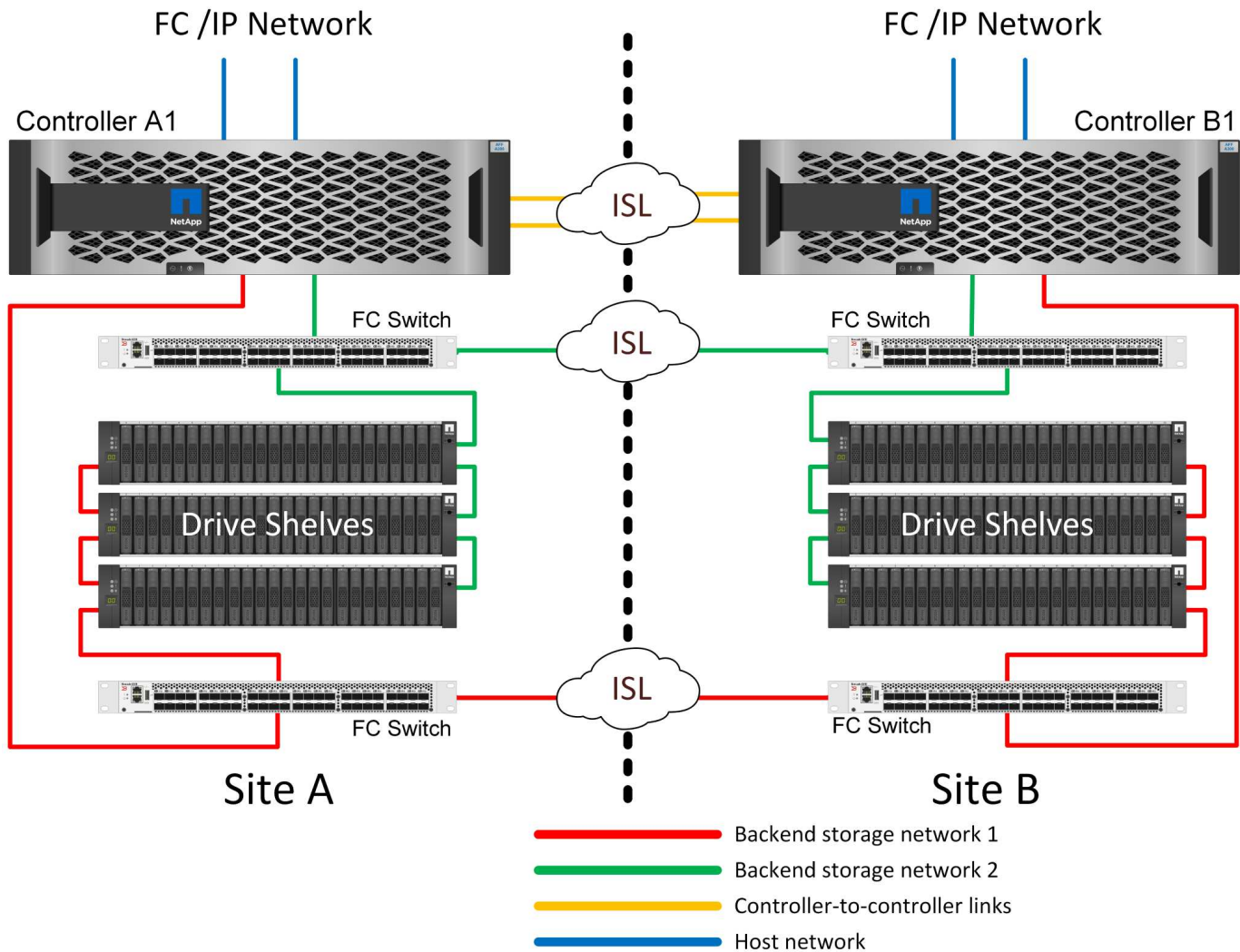


Alcune infrastrutture multisito non sono progettate per le operazioni Active-Active, ma vengono utilizzate maggiormente come sito primario e sito di disaster recovery. In questa situazione, è generalmente preferibile un'opzione ha-Pair MetroCluster per i seguenti motivi:

- Anche se un cluster MetroCluster a due nodi è un sistema ha, un guasto imprevisto di un controller o una manutenzione pianificata richiedono che i servizi dati vengano online sul sito opposto. Se la connettività di rete tra i siti non supporta la larghezza di banda richiesta, le prestazioni ne risentono. L'unica opzione sarebbe anche eseguire il failover dei vari sistemi operativi host e dei servizi associati al sito alternativo. Il cluster MetroCluster ha-Pair elimina questo problema grazie alla perdita di un controller che consente di eseguire un semplice failover all'interno dello stesso sito.
- Alcune topologie di rete non sono progettate per l'accesso tra siti, ma utilizzano sottoreti o SAN FC isolate. In questi casi, il cluster MetroCluster a due nodi non funziona più come sistema ha, perché il controller alternativo non può fornire dati ai server del sito opposto. L'opzione ha-Pair MetroCluster è necessaria per garantire ridondanza completa.
- Se un'infrastruttura a due siti viene vista come una singola infrastruttura ad alta disponibilità, la configurazione MetroCluster a due nodi è adatta. Tuttavia, se il sistema deve funzionare per un periodo di tempo prolungato dopo il guasto del sito, è preferibile una coppia ha perché continua a fornire ha all'interno di un singolo sito.

MetroCluster FC SAN-attached a due nodi

La configurazione MetroCluster a due nodi utilizza un solo nodo per sito. Questo design è più semplice rispetto all'opzione ha-Pair perché richiede meno componenti da configurare e gestire. Inoltre, ha ridotto le richieste di infrastruttura in termini di cablaggio e switch FC. Infine, riduce i costi.



L'evidente impatto di questa progettazione è che un guasto del controller su un singolo sito implica che i dati sono disponibili dal sito opposto. Questa restrizione non è necessariamente un problema. Molte aziende hanno operazioni di data center multisito con reti estese, ad alta velocità e a bassa latenza che funzionano essenzialmente come una singola infrastruttura. In questi casi, la configurazione preferita è la versione a due nodi di MetroCluster. Diversi service provider utilizzano attualmente sistemi a due nodi con scalabilità di petabyte.

Funzionalità di resilienza di MetroCluster

Non esistono single point of failure in una soluzione MetroCluster:

- Ogni controller dispone di due percorsi indipendenti verso gli shelf di dischi sul sito locale.
- Ogni controller dispone di due percorsi indipendenti verso gli shelf di dischi sul sito remoto.
- Ciascun controller dispone di due percorsi indipendenti verso i controller sul sito opposto.
- Nella configurazione ha-Pair, ogni controller ha due percorsi verso il partner locale.

Riassumendo, qualsiasi componente della configurazione può essere rimosso senza compromettere la capacità di MetroCluster di fornire dati. L'unica differenza in termini di resilienza tra le due opzioni è che la versione ha-Pair è ancora un sistema storage ha generale dopo un guasto del sito.

SyncMirror

La protezione per SQL Server con MetroCluster si basa su SyncMirror, che offre una tecnologia di mirroring sincrono scale-out dalle performance massime.

Data Protection con SyncMirror

Al livello più semplice, la replica sincrona significa che qualsiasi modifica deve essere apportata a entrambi i lati dello storage con mirroring prima che venga riconosciuta. Ad esempio, se un database sta scrivendo un registro o un guest VMware viene aggiornato, non deve mai andare persa una scrittura. Come livello di protocollo, il sistema di storage non deve riconoscere la scrittura fino a quando non è stato assegnato a un supporto non volatile in entrambi i siti. Solo allora è sicuro procedere senza il rischio di perdita dei dati.

L'utilizzo di una tecnologia di replica sincrona è il primo passo nella progettazione e nella gestione di una soluzione di replica sincrona. La considerazione più importante è capire cosa potrebbe accadere durante i vari scenari di guasto pianificati e non pianificati. Non tutte le soluzioni di replica sincrona offrono le stesse funzionalità. Se hai bisogno di una soluzione che offra un recovery point objective (RPO) pari a zero, ovvero zero data loss, devi prendere in considerazione tutti gli scenari di guasto. In particolare, qual è il risultato previsto quando la replica è impossibile a causa della perdita di connettività tra i siti?

Disponibilità dei dati SyncMirror

La replica MetroCluster si basa sulla tecnologia NetApp SyncMirror, che è progettata per passare in modo efficiente dalla modalità sincrona alla modalità asincrona e viceversa. Questa funzionalità soddisfa i requisiti dei clienti che richiedono una replica sincrona, ma che hanno bisogno anche di un'alta disponibilità per i propri servizi dati. Ad esempio, se la connettività a un sito remoto viene interrotta, è generalmente preferibile che il sistema di archiviazione continui a funzionare in uno stato non replicato.

Molte soluzioni di replica sincrona sono in grado di funzionare solo in modalità sincrona. Questo tipo di replica "tutto o niente" viene talvolta chiamato modalità domino. Tali sistemi storage smettono di fornire i dati piuttosto che permettere che le copie locali e remote dei dati diventino non sincronizzate. Se la replica viene forzata, la risincronizzazione può richiedere molto tempo e lasciare un cliente esposto a una perdita di dati completa durante il tempo in cui il mirroring viene ristabilita.

Non solo SyncMirror può passare alla modalità asincrona senza problemi se il sito remoto non è raggiungibile, ma può anche risincronizzare rapidamente uno stato RPO = 0 al ripristino della connettività. La copia obsoleta dei dati nel sito remoto può anche essere preservata in uno stato utilizzabile durante la risincronizzazione, garantendo l'esistenza in ogni momento di copie locali e remote dei dati.

Quando è richiesta la modalità domino, NetApp offre SnapMirror Synchronous (SM-S). Esistono anche opzioni a livello di applicazione, come Oracle DataGuard o SQL Server Always on Availability Groups. Il mirroring del disco a livello del sistema operativo può essere opzionale. Per ulteriori informazioni e opzioni, consulta il tuo NetApp o il partner account team.

SQL Server con MetroCluster

Un'opzione per la protezione dei database di SQL Server con RPO pari a zero è MetroCluster. MetroCluster è una semplice tecnologia di replica RPO=0 dalle performance elevate che consente di replicare un'intera infrastruttura tra i siti in modo semplice.

SQL Server è in grado di scalare fino a migliaia di database su un unico sistema MetroCluster. Potrebbero esistere istanze standalone di SQL Server o istanze cluster di failover, MetroCluster System non aggiunge o modifica necessariamente le Best practice per la gestione di un database.

Una spiegazione completa di MetroCluster esula dall'ambito di questo documento, ma i principi sono semplici. MetroCluster può offrire una soluzione di replica con RPO=0 e failover rapido. Ciò che costruite su questa base dipende dalle vostre esigenze.

Ad esempio, una procedura di DR rapida di base dopo una perdita improvvisa del sito potrebbe utilizzare la seguente procedura di base:

- Forzare uno switchover MetroCluster
- Rilevamento di LUN FC/iSCSI (solo SAN)
- Montare i file system
- Avviare SQL Services

Il requisito principale di questo approccio è rappresentato da un sistema operativo in esecuzione sul sito remoto. Deve essere preconfigurato con l'installazione di SQL Server e deve essere aggiornato con una versione di build equivalente. È inoltre possibile eseguire il mirroring dei database di sistema di SQL Server nel sito remoto e montarli se viene dichiarata un'emergenza.

Se i volumi, i file system e il datastore che ospitano database virtualizzati non vengono utilizzati nel sito di disaster recovery prima dello switchover, non è necessario impostare i `dr-force-nvfail` volumi associati.

Sincronizzazione attiva di SnapMirror

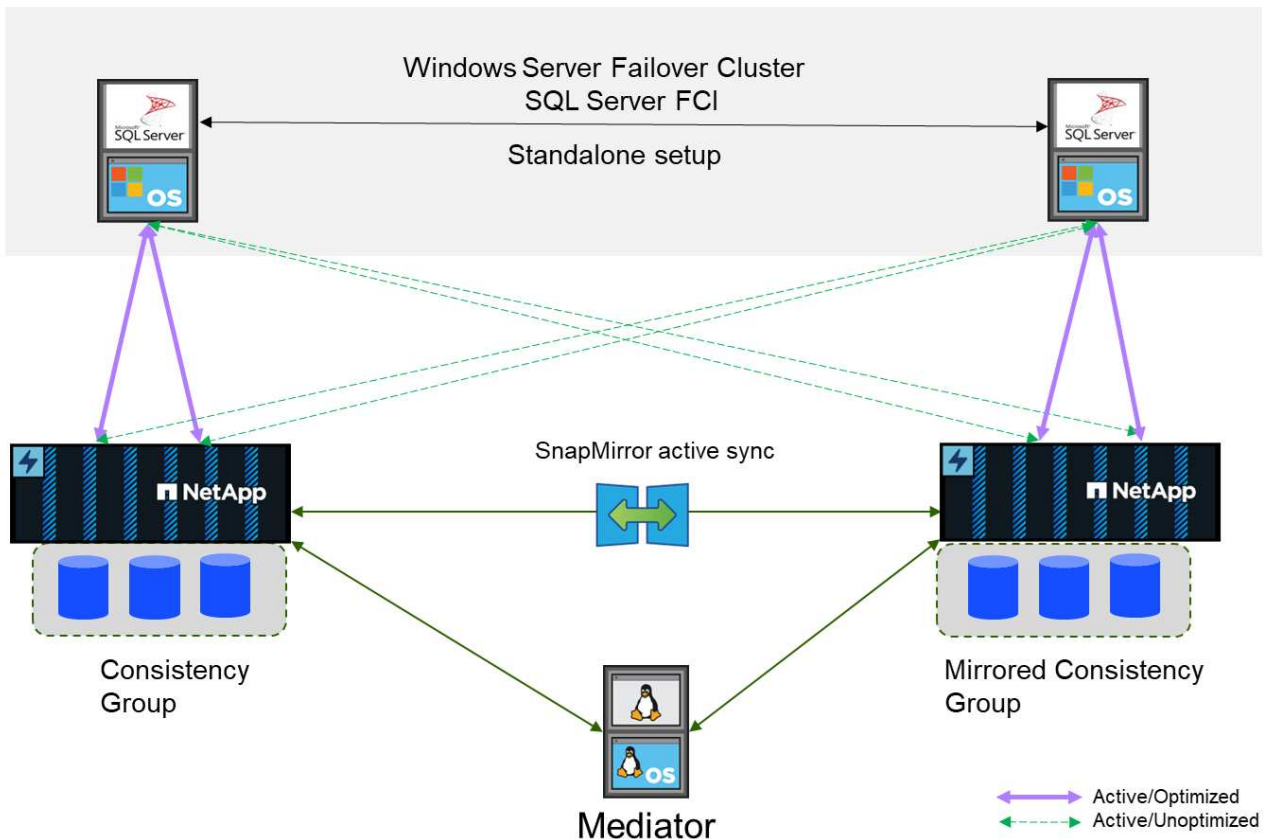
Panoramica

La sincronizzazione attiva di SnapMirror consente a singoli database e applicazioni SQL Server di continuare le operazioni durante interruzioni di rete e storage, con failover trasparente dello storage senza interventi manuali.

A partire da ONTAP 9.15.1, SnapMirror Active Sync supporta l'architettura Active/Active simmetrica oltre alla configurazione asimmetrica esistente. La funzionalità Active/Active simmetrica offre replica bidirezionale sincrona per la business continuity e il disaster recovery. Protegge l'accesso ai dati per carichi di lavoro critici SAN con accesso simultaneo in lettura e scrittura ai dati in diversi domini di errore, garantendo operazioni senza interruzioni e riducendo al minimo i downtime in caso di disastri o errori di sistema.

Gli host SQL Server accedono allo storage utilizzando LUN Fiber Channel (FC) o iSCSI. Replica tra ciascun cluster in cui risiede una copia dei dati replicati. Poiché questa funzionalità è la replica a livello di storage, le istanze di SQL Server in esecuzione su istanze di cluster di failover o host standalone possono eseguire operazioni di lettura/scrittura in entrambi i cluster. Per le fasi di pianificazione e configurazione, fare riferimento a ["Documentazione di ONTAP sulla sincronizzazione attiva di SnapMirror"](#).

Architettura di sincronizzazione attiva SnapMirror con Active/Active simmetrico



Replica sincrona

Durante l'utilizzo normale, ciascuna copia è una replica sincrona con RPO=0/7, con un'unica eccezione. Se i dati non possono essere replicati, ONTAP rilascerà il requisito di replicare i dati e riprendere la distribuzione io su un sito mentre le LUN dell'altro sito vengono portate offline.

Hardware di archiviazione

A differenza di altre soluzioni di disaster recovery per lo storage, SnapMirror Active Sync offre una flessibilità asimmetrica della piattaforma. Non è necessario che l'hardware di ciascun sito sia identico. Questa funzionalità consente di dimensionare correttamente l'hardware utilizzato per supportare la sincronizzazione attiva di SnapMirror. Il sistema di storage remoto può essere identico al sito primario se deve supportare un carico di lavoro di produzione completo, ma se un disastro determina una riduzione dell'i/o, rispetto a un sistema più piccolo nel sito remoto potrebbe risultare più conveniente.

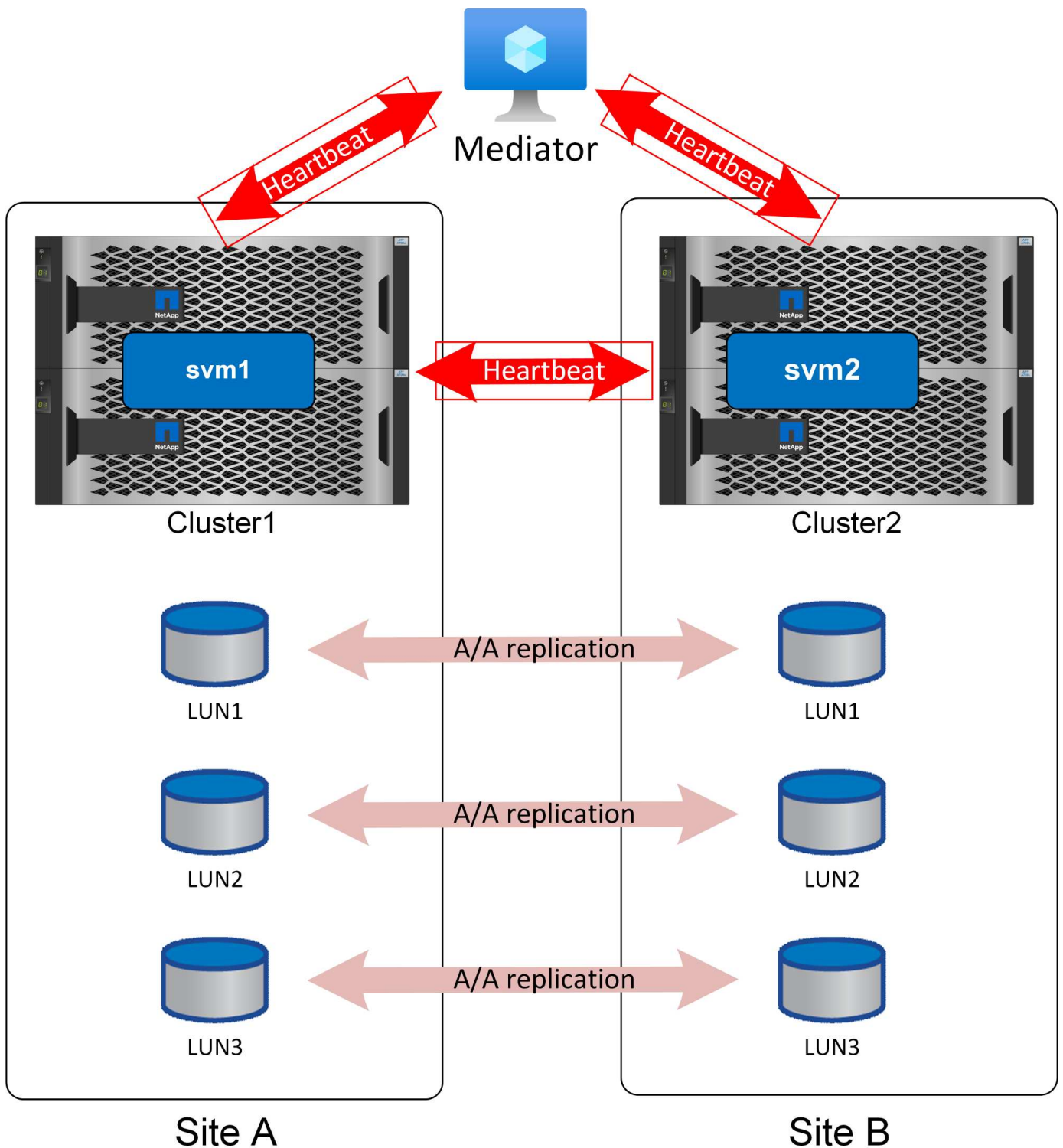
ONTAP mediatore

ONTAP Mediator è un'applicazione software che viene scaricata dal supporto NetApp e che viene in genere distribuita su una piccola macchina virtuale. Il ONTAP Mediator non è un tiebreaker. È un canale di comunicazione alternativo per i due cluster che partecipano alla replica sincrona attiva SnapMirror. Le operazioni automatizzate sono gestite da ONTAP in base alle risposte ricevute dal partner tramite connessioni dirette e tramite il mediatore.

Mediatore ONTAP

Mediator è necessario per automatizzare in modo sicuro il failover. Idealmente, sarebbe posizionato su un sito 3rd indipendente, ma può comunque funzionare per la maggior parte delle esigenze se colocated con uno dei cluster che partecipano alla replica.

Il mediatore non è propriamente uno strumento decisivo, sebbene questa sia effettivamente la sua funzione. Il mediatore aiuta a determinare lo stato dei nodi del cluster e supporta il processo di commutazione automatica in caso di guasto del sito. Il mediatore non trasferisce dati in nessun caso.



La sfida #1 con il failover automatizzato è il problema split-brain, e questo problema sorge se i due siti perdono la connettività tra loro. Che cosa dovrebbe accadere? Non si desidera che due siti diversi si designino come copie sopravvissute dei dati, ma in che modo un singolo sito può distinguere tra la perdita effettiva del sito opposto e l'impossibilità di comunicare con il sito opposto?

Qui entra il mediatore nell'immagine. Se si trova in un sito 3rd e ciascun sito dispone di una connessione di rete separata per tale sito, è disponibile un percorso aggiuntivo per ciascun sito per convalidare lo stato dell'altro. Esaminare nuovamente l'immagine sopra riportata e considerare i seguenti scenari.

- Cosa succede se il mediatore non riesce o è irraggiungibile da uno o entrambi i siti?
 - I due cluster possono ancora comunicare tra loro sullo stesso link utilizzato per i servizi di replica.
 - I dati sono ancora serviti con protezione RPO=0/7
- Cosa succede se il sito A non funziona?
 - Il sito B vedrà che entrambi i canali di comunicazione si interrompono.
 - Il sito B sostituirà i servizi dati, ma senza RPO = mirroring 0:1
- Cosa succede se il sito B non funziona?
 - Il sito A vedrà che entrambi i canali di comunicazione si interrompono.
 - Il sito A sostituirà i servizi dati, ma senza RPO = mirroring 0:1

Esiste un altro scenario da considerare: La perdita del collegamento di replica dei dati. In caso di perdita del link di replica tra i siti, RPO=0 Mirroring sarà ovviamente impossibile. Che cosa dovrebbe accadere allora?

Questo è controllato dallo stato del sito preferito. In una relazione SM-AS, uno dei siti è secondario all'altro. Questo non ha alcun effetto sulle normali operazioni e tutto l'accesso ai dati è simmetrico, ma se la replica viene interrotta, il legame dovrà essere interrotto per riprendere le operazioni. Ne risulta che il sito preferito continuerà le operazioni senza mirroring e il sito secondario interromperà l'elaborazione io fino al ripristino della comunicazione di replica.

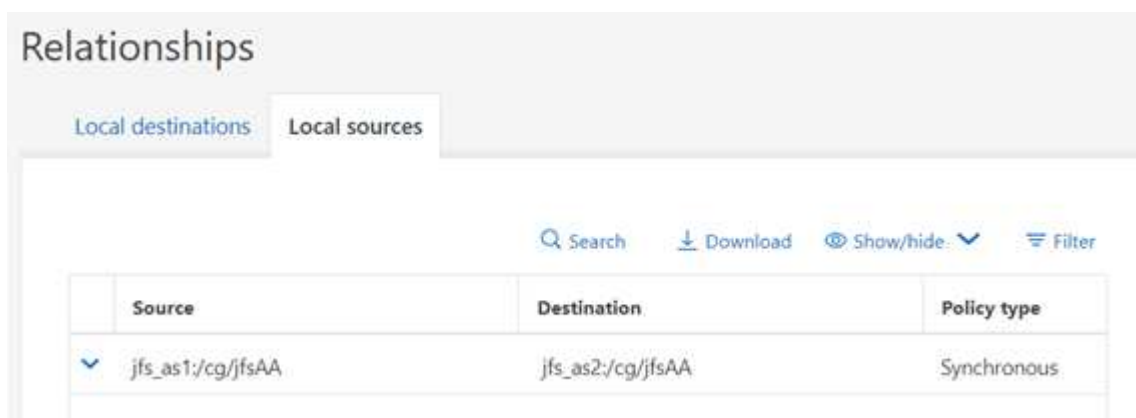
Sito preferito

Il comportamento di sincronizzazione attiva di SnapMirror è simmetrico, con una eccezione importante: Configurazione del sito preferito.

La sincronizzazione attiva di SnapMirror considererà un sito la "fonte" e l'altro la "destinazione". Ciò implica una relazione di replica unidirezionale, ma ciò non si applica al comportamento io. La replica è bidirezionale e simmetrica, mentre i tempi di risposta io sono identici su entrambi i lati del mirror.

La `source` designazione controlla il sito preferito. In caso di perdita del link di replica, i percorsi delle LUN nella copia di origine continueranno a fornire i dati mentre i percorsi delle LUN nella copia di destinazione non saranno disponibili finché la replica non viene ristabilita e SnapMirror ritorna allo stato sincrono. I percorsi riprenderanno a fornire i dati.

La configurazione di origine/destinazione può essere visualizzata tramite SystemManager:



The screenshot shows the 'Relationships' section of the SystemManager interface. It has two tabs: 'Local destinations' and 'Local sources'. Below the tabs is a table with columns 'Source', 'Destination', and 'Policy type'. A single row is visible with a dropdown arrow on the left, showing 'jfs_as1:/cg/jfsAA' as the Source, 'jfs_as2:/cg/jfsAA' as the Destination, and 'Synchronous' as the Policy type. Above the table are controls for Search, Download, Show/hide, and Filter.

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

O all'interfaccia 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
```

La chiave è che source è l'SVM su cluster1. Come menzionato sopra, i termini "origine" e "destinazione" non descrivono il flusso di dati replicati. Entrambi i siti possono elaborare una scrittura e replicarla nel sito opposto. In effetti, entrambi i cluster sono origini e destinazioni. L'effetto della designazione di un cluster come origine controlla semplicemente quale cluster sopravvive come sistema di storage in lettura e scrittura in caso di perdita del link di replica.

Topologia di rete

Accesso uniforme

Una rete ad accesso uniforme significa che gli host sono in grado di accedere ai percorsi su entrambi i siti (o ai domini di errore all'interno dello stesso sito).

Una caratteristica importante di SM-AS è la capacità di configurare i sistemi storage per sapere dove si trovano gli host. Quando si mappano i LUN a un determinato host, è possibile indicare se sono prossimi o meno a un determinato sistema di archiviazione.

Impostazioni di prossimità

La prossimità si riferisce a una configurazione per cluster che indica che un determinato WWN host o ID iniziatore iSCSI appartiene a un host locale. Si tratta di un secondo passo opzionale per la configurazione dell'accesso LUN.

Il primo passo è la normale configurazione di igroup. Ogni LUN deve essere mappato a un igroup che contiene gli ID WWN/iSCSI degli host che devono accedere a quel LUN. Controlla quale host ha accesso a un LUN.

Il secondo passo, opzionale, consiste nel configurare la prossimità all'host. Questo non controlla l'accesso, controlla *priority*.

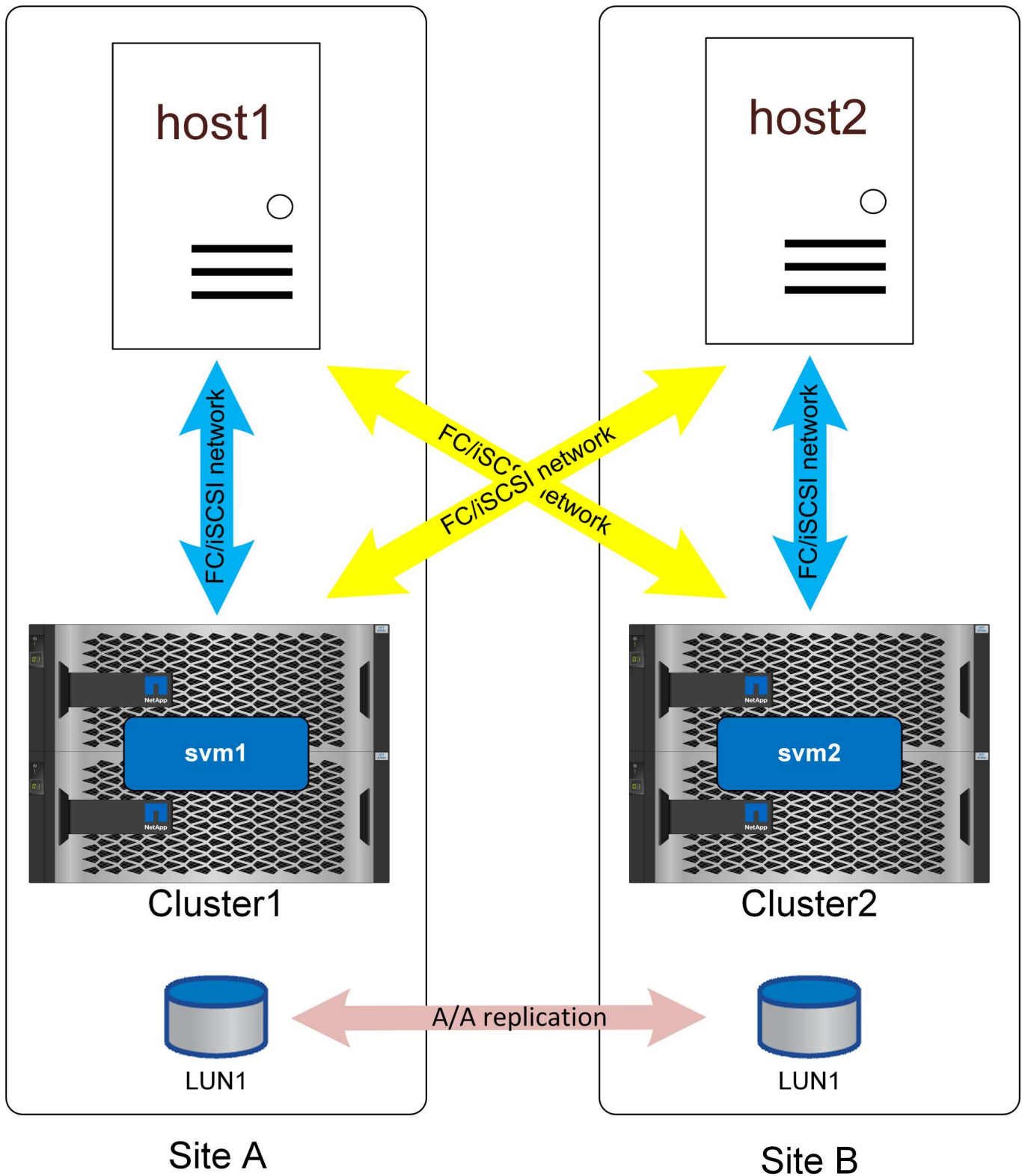
Ad esempio, un host del sito A potrebbe essere configurato in modo da accedere a una LUN protetta dalla sincronizzazione attiva di SnapMirror e, poiché la SAN è estesa tra i siti, i percorsi sono disponibili per tale LUN utilizzando lo storage sul sito A o lo storage sul sito B.

Senza impostazioni di prossimità, l'host utilizzerà entrambi i sistemi storage allo stesso modo perché entrambi

i sistemi storage pubblicizzeranno i percorsi attivi/ottimizzati. Se la latenza SAN e/o la larghezza di banda tra i siti è limitata, questa operazione potrebbe non essere disattivabile e potrebbe essere necessario assicurarsi che durante il normale funzionamento ogni host utilizzi preferenzialmente i percorsi verso il sistema di storage locale. Viene configurato aggiungendo l'ID WWN/iSCSI dell'host al cluster locale come host prossimale. Questa operazione può essere eseguita dalla CLI o da SystemManager.

AFF

Con un sistema AFF, i percorsi vengono visualizzati come mostrato di seguito quando è stata configurata la prossimità dell'host.



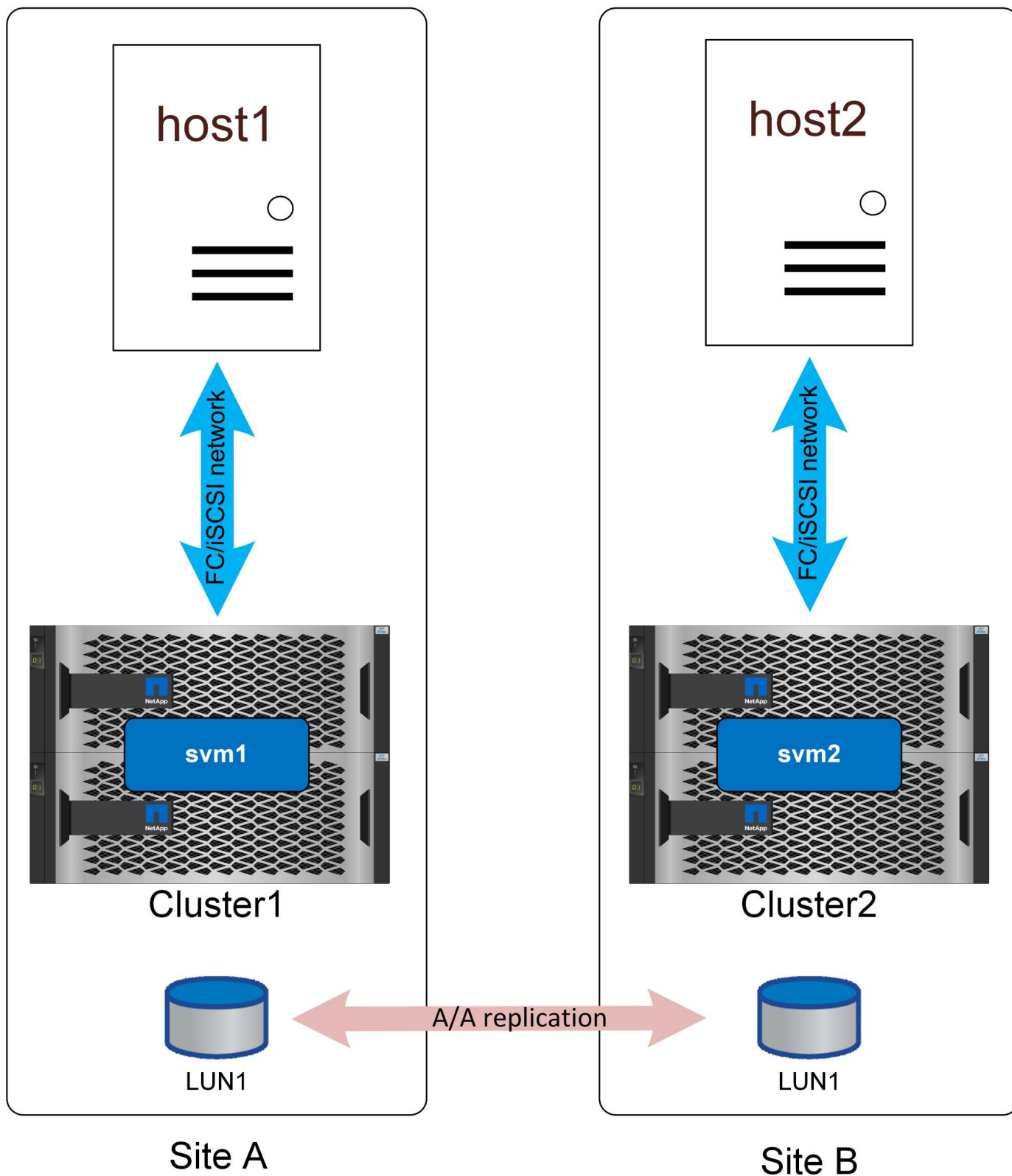
Durante le normali operazioni, tutti i io sono i/o locali. Le letture e le scritture sono gestite dallo storage array locale. Gli io in scrittura, naturalmente, dovranno anche essere replicati dal controller locale sul sistema remoto prima di essere riconosciuti, ma tutti gli io in lettura saranno serviti localmente e non subiranno una latenza aggiuntiva attraverso il collegamento SAN tra i siti.

L'unica volta in cui verranno utilizzati i percorsi non ottimizzati è quando tutti i percorsi attivi/ottimizzati vengono persi. Ad esempio, se l'intero array sul sito A perde energia, gli host sul sito A sarebbero comunque in grado di accedere ai percorsi dell'array sul sito B e di rimanere quindi operativi, anche se sperimenterebbero una latenza più elevata.

Esistono percorsi ridondanti attraverso il cluster locale non mostrati in questi diagrammi per semplicità. I sistemi di storage ONTAP sono ad alta disponibilità, pertanto un guasto a un controller non dovrebbe causare guasti nel sito. Ciò dovrebbe comportare solo una modifica dei percorsi locali utilizzati nel sito interessato.

Accesso non uniforme

Una rete di accesso non uniforme significa che ogni host ha solo accesso alle porte sul sistema di storage locale. LA SAN non è estesa a più siti (o presenta errori nei domini dello stesso sito).



Active/Optimized Path

Il vantaggio principale di questo approccio è la semplicità DELLE SAN, eliminando l'esigenza di stretching di una SAN via rete. Alcuni clienti non dispongono di connettività a latenza sufficientemente bassa tra i siti o non

dispongono dell'infrastruttura per il tunnel del traffico FC SAN su una rete intersito.

Lo svantaggio legato all'accesso non uniforme è che alcuni scenari di errore, inclusa la perdita del collegamento di replica, provocheranno la perdita dell'accesso allo storage da parte di alcuni host. In caso di interruzione della connettività dello storage locale, le applicazioni eseguite come istanze singole, come ad esempio i database non in cluster, eseguiti in maniera intrinseca solo su un singolo host in uno qualsiasi dei supporti di montaggio, si guasterebbero. I dati sarebbero comunque protetti, ma il server di database non avrebbe più accesso. Dovrebbe essere riavviato su un sito remoto, preferibilmente tramite un processo automatizzato. Ad esempio, VMware ha è in grado di rilevare una situazione di tutti i percorsi verso l'esterno su un server e di riavviare una macchina virtuale su un altro server in cui sono disponibili i percorsi.

Al contrario, un'applicazione in cluster come Oracle RAC può offrire un servizio disponibile contemporaneamente in due siti diversi. Perdere un sito non significa perdere il servizio dell'applicazione nel suo complesso. Le istanze sono ancora disponibili e in esecuzione nel sito sopravvissuto.

In molti casi, l'overhead della latenza aggiuntivo di un'applicazione che accede allo storage attraverso un collegamento da sito a sito sarebbe inaccettabile. Ciò significa che la migliore disponibilità di una rete uniforme è minima, poiché la perdita di storage su un sito comporterebbe comunque la necessità di arrestare i servizi sul sito in cui si è verificato l'errore.



Esistono percorsi ridondanti attraverso il cluster locale non mostrati in questi diagrammi per semplicità. I sistemi di storage ONTAP sono ad alta disponibilità, pertanto un guasto a un controller non dovrebbe causare guasti nel sito. Ciò dovrebbe comportare solo una modifica dei percorsi locali utilizzati nel sito interessato.

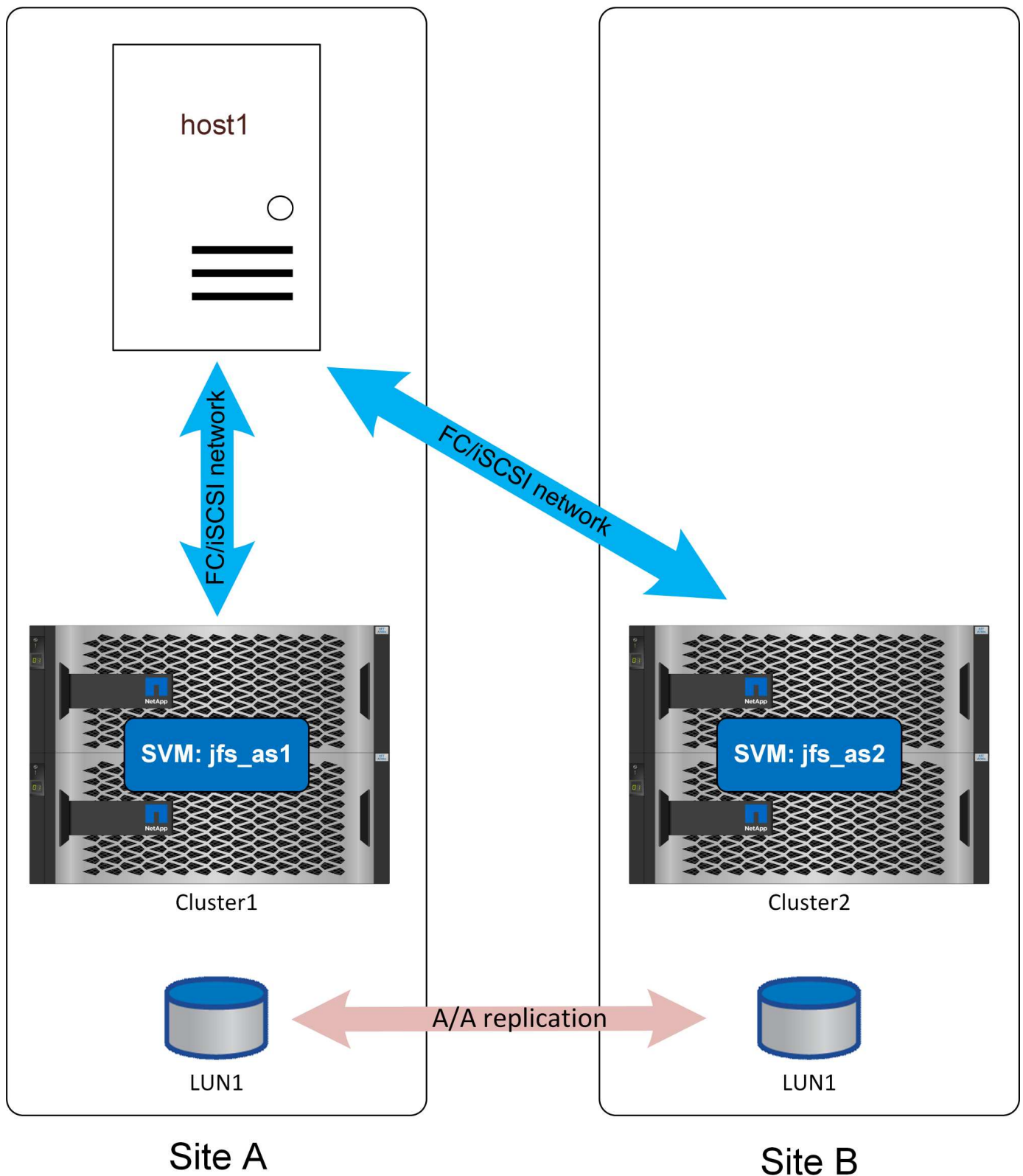
Panoramica

SQL Server può essere configurato per funzionare con la sincronizzazione attiva di SnapMirror in diversi modi. La risposta giusta dipende dalla connettività di rete disponibile, dai requisiti RPO e dai requisiti di disponibilità.

Istanza standalone di SQL Server

Le procedure consigliate per il layout dei file e la configurazione del server sono identiche a quelle consigliate nella ["Server SQL su ONTAP"](#) documentazione.

Con una configurazione standalone, SQL Server potrebbe essere eseguito solo in un sito. Presumibilmente ["uniforme"](#) si userebbe l'accesso.



Grazie a un accesso uniforme, un guasto dello storage in uno dei siti non interromperebbe le operazioni di database. Un errore completo del sito che includeva il server di database comporterebbe, ovviamente, un'interruzione del servizio.

Alcuni clienti potrebbero configurare un sistema operativo in esecuzione nel sito remoto con un'installazione di SQL Server preconfigurata, aggiornata con una versione di build equivalente a quella dell'istanza di

produzione. Il failover richiede l'attivazione dell'istanza standalone di SQL Server nel sito alternativo, il rilevamento dei LUN e l'avvio del database. È possibile automatizzare il processo completo con il cmdlet di Windows PowerShell, in quanto non sono richieste operazioni dal lato storage.

"Non uniforme" è possibile utilizzare anche l'accesso, ma il risultato sarebbe un'interruzione del database se il sistema storage in cui si trovava il server del database non avesse avuto esito positivo, perché il database non avrebbe percorsi disponibili per lo storage. In alcuni casi ciò può ancora essere accettabile. La sincronizzazione attiva di SnapMirror garantirebbe comunque una data Protection con RPO=0 e, in caso di guasto del sito, la copia restante sarebbe attiva e pronta a riprendere le operazioni seguendo la stessa procedura utilizzata con un accesso uniforme descritta sopra.

Un processo di failover semplice e automatizzato può essere configurato più facilmente con l'uso di un host virtualizzato. Ad esempio, se i file di dati di SQL Server vengono replicati in modo sincrono su storage secondario insieme a un VMDK di avvio, in caso di disastro è possibile attivare l'ambiente completo nel sito alternativo. Un amministratore può attivare manualmente l'host nel sito rimasto o automatizzare il processo tramite un servizio come VMware ha.

Istanza del cluster di failover di SQL Server

Le istanze di failover di SQL Server possono essere ospitate anche in un cluster di failover di Windows in esecuzione su un server fisico o virtuale come sistema operativo guest. Questa architettura multi-host offre un'istanza di SQL Server e la resilienza dello storage. Tale implementazione è utile in ambienti a domanda elevata che richiedono solidi processi di failover senza rinunciare a prestazioni avanzate. In una configurazione del cluster di failover, quando un host o uno storage primario viene colpito, SQL Services eseguirà il failover sull'host secondario e, allo stesso tempo, lo storage secondario sarà disponibile per servire io. Non è richiesto alcuno script di automazione o intervento dell'amministratore.

Scenari di errore

La pianificazione di un'architettura completa dell'applicazione SnapMirror Active Sync richiede la comprensione del modo in cui SM-AS risponderà in vari scenari di failover pianificati e non pianificati.

Per gli esempi seguenti, si supponga che il sito A sia configurato come sito preferito.

Interruzione della connettività di replica

Se la replica SM-AS viene interrotta, non è possibile completare la scrittura io perché sarebbe impossibile per un cluster replicare le modifiche al sito opposto.

Sito A (sito preferito)

Il risultato dell'errore del collegamento di replica sul sito preferito sarà una pausa di circa 15 secondi nell'elaborazione io in scrittura, poiché ONTAP ritenta le operazioni di scrittura replicate prima di determinare che il collegamento di replica è veramente irraggiungibile. Trascorsi i 15 secondi, il sistema del sito A riprende l'elaborazione io in lettura e scrittura. I percorsi SAN non vengono modificati e i LUN rimangono online.

Sito B

Poiché il sito B non è il sito preferito di sincronizzazione attiva SnapMirror, i relativi percorsi LUN non saranno più disponibili dopo circa 15 secondi.

Errore del sistema di storage

Il risultato di un errore del sistema di storage è quasi identico al risultato della perdita del collegamento di replica. Il sito sopravvissuto dovrebbe subire una pausa io di circa 15 secondi. Trascorso questo periodo di 15 secondi, io riprenderà sul sito come di consueto.

Perdita del mediatore

Il servizio di mediazione non controlla direttamente le operazioni di storage. Funziona come un percorso di controllo alternativo tra cluster. Esiste principalmente per automatizzare il failover senza il rischio di uno scenario split-brain. Durante l'utilizzo normale, ogni cluster replica le modifiche al partner e pertanto ogni cluster può verificare che il cluster partner sia online e fornisca i dati. Se il collegamento di replica non è riuscito, la replica viene interrotta.

Il motivo per cui è necessario un mediatore per il failover automatizzato sicuro è perché altrimenti sarebbe impossibile per un cluster di storage determinare se la perdita di comunicazione bidirezionale fosse il risultato di un'interruzione della rete o di un errore effettivo dello storage.

Il mediatore fornisce un percorso alternativo per ciascun cluster per verificare lo stato di salute del partner. Gli scenari sono i seguenti:

- Se un cluster può contattare direttamente il partner, i servizi di replica sono operativi. Non è richiesta alcuna azione.
- Se un sito preferito non può contattare direttamente il proprio partner o tramite il mediatore, presuppone che il partner sia effettivamente non disponibile oppure è stato isolato e ha portato i percorsi LUN offline. Il sito preferito procede quindi al rilascio dello stato RPO=0 e continua l'elaborazione dell'io in lettura e in scrittura.
- Se un sito non preferito non può contattare direttamente il proprio partner, ma può contattarlo tramite il mediatore, prenderà i suoi percorsi offline e attenderà il ritorno della connessione di replica.
- Se un sito non preferito non può contattare direttamente il proprio partner o tramite un mediatore operativo, supporterà che il partner sia effettivamente non disponibile, oppure che sia stato isolato e che abbia portato i percorsi LUN offline. Il sito non preferito procede quindi al rilascio dello stato RPO=0 e continua l'elaborazione dell'i/o in lettura e scrittura. Assumerà il ruolo dell'origine della replica e diventerà il nuovo sito preferito.

Se il mediatore non è completamente disponibile:

- In caso di guasto dei servizi di replica per qualsiasi motivo, incluso un guasto del sito o del sistema storage non preferito, il sito preferito rilascerà lo stato RPO=0 e riprenderà l'elaborazione i/o in lettura e scrittura. Il sito non preferito prenderà i suoi percorsi offline.
- Il guasto del sito preferito causerà un'interruzione poiché il sito non preferito non sarà in grado di verificare che il sito opposto sia effettivamente offline e quindi non sarebbe sicuro per il sito non preferito riprendere i servizi.

Ripristino dei servizi in corso

Dopo aver risolto un errore, come il ripristino della connettività da sito a sito o l'accensione di un sistema guasto, gli endpoint di sincronizzazione attivi di SnapMirror rilevano automaticamente la presenza di una relazione di replica difettosa e la riportano allo stato RPO=0. Una volta ristabilita la replica sincrona, i percorsi non riusciti torneranno in linea.

In molti casi, le applicazioni in cluster rilevano automaticamente la restituzione dei percorsi non riusciti e tali applicazioni tornano online. In altri casi, potrebbe essere necessaria una scansione SAN a livello di host

oppure potrebbe essere necessario riportare le applicazioni online manualmente. Dipende dall'applicazione e dal modo in cui è configurata, e in generale tali attività possono essere facilmente automatizzate. ONTAP si sta auto-riparando e non deve richiedere alcun intervento da parte dell'utente per riprendere le operazioni di storage RPO = 0 KB.

Failover manuale

La modifica del sito preferito richiede un'operazione semplice. I/o si fermeranno per un secondo o due come autorità sugli switch del comportamento di replica tra i cluster, ma in caso contrario i/o non vengono influenzati.

Configurazione dello storage sui sistemi ASA R2

Panoramica

NetApp ASA R2 è una soluzione potente e semplificata per i clienti solo SAN che eseguono carichi di lavoro mission-critical. La combinazione della piattaforma ASA R2 con soluzioni di storage ONTAP e Microsoft SQL Server offre design di storage dei database di livello Enterprise in grado di soddisfare le esigenze applicative più esigenti di oggi.

Le seguenti piattaforme ASA sono classificate come sistemi ASA R2 che supportano tutti i protocolli SAN (iSCSI, FC, NVMe/FC, NVMe/TCP). I protocolli iSCSI, FC, NVMe/FC e NVMe/TCP supportano l'architettura Active-Active simmetrica per il multipathing, in modo che tutti i percorsi tra gli host e lo storage siano attivi/ottimizzati:

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

Per ulteriori informazioni, vedere ["NetApp ASA"](#)

L'ottimizzazione di una soluzione SQL Server su ONTAP richiede la comprensione del modello e delle caratteristiche di i/o di SQL Server. Un layout di storage ben progettato per un database SQL Server deve supportare i requisiti relativi alle performance di SQL Server, offrendo al contempo la massima capacità di gestione dell'infrastruttura nel suo complesso. Un buon layout dello storage permette inoltre di avere successo nell'implementazione iniziale e di far crescere l'ambiente senza problemi nel tempo, con il crescere dell'azienda.

Progettazione dello storage dei dati

Microsoft consiglia di collocare i dati e i file di registro su unità separate. Per le applicazioni che aggiornano e richiedono contemporaneamente i dati, il file di log è intensivo in scrittura e il file di dati (a seconda dell'applicazione) è intensivo in lettura/scrittura. Per il recupero dei dati, il file di log non è necessario. Pertanto, le richieste di dati possono essere soddisfatte dal file di dati posto sul proprio disco.

Quando si crea un nuovo database, Microsoft consiglia di specificare unità separate per i dati e i registri. Per spostare i file dopo la creazione del database, il database deve essere portato offline. Per ulteriori consigli

Microsoft, vedere ["Posizionare i file di dati e di registro su unità separate"](#).

Considerazioni sull'unità di conservazione

L'unità storage in ASA si riferisce a LUN per host SCSI/FC o a un namespace NVMe per host NVMe. In base al protocollo supportato, ti verrà richiesto di creare LUN, namespace NVMe o entrambi. Prima di creare un'unità di storage per la distribuzione del database, è importante comprendere in che modo il modello i/o di SQL Server e le relative caratteristiche variano in base al carico di lavoro e ai requisiti di backup e ripristino. Vedere le seguenti raccomandazioni NetApp per l'unità di conservazione:

- Evitare la condivisione della stessa unità di storage tra più SQL Server in esecuzione sullo stesso host, per evitare una gestione complicata. Nel caso di esecuzione di più istanze di SQL Server sullo stesso host, a meno che non si sia vicini al limite dell'unità di archiviazione su un nodo, evitare la condivisione e disporre invece di un'unità di archiviazione separata per istanza per host per semplificare la gestione dei dati.
- Utilizzare i punti di montaggio NTFS invece delle lettere dell'unità per superare il limite di 26 lettere di unità in Windows.
- Disattivare le pianificazioni delle snapshot e i criteri di conservazione. Utilizzare invece SnapCenter per coordinare le copie Snapshot dell'unità di archiviazione dati di SQL Server.
- Posizionare i database del sistema SQL Server su un'unità di archiviazione dedicata.
- Tempdb è un database di sistema utilizzato da SQL Server come area di lavoro temporanea, in particolare per operazioni DBCC CHECKDB i/o intensive. Pertanto, collocare questo database su un'unità di archiviazione dedicata. In ambienti di grandi dimensioni in cui il numero di unità di storage rappresenta una sfida, è possibile consolidare tempdb con database di sistema nella stessa unità di storage dopo un'attenta pianificazione. La protezione dei dati per tempdb non è una priorità elevata perché questo database viene ricreato ogni volta che SQL Server viene riavviato.
- Collocare i file di dati utente (.mdf) su un'unità di archiviazione separata perché si tratta di carichi di lavoro di lettura/scrittura casuali. È comune creare backup del log delle transazioni con maggiore frequenza rispetto ai backup del database. Per questo motivo, inserire i file di log delle transazioni (.ldf) in un'unità di archiviazione separata o VMDK dai file di dati in modo che sia possibile creare pianificazioni di backup indipendenti per ciascuno di essi. Questa separazione isola inoltre l'i/o di scrittura sequenziale dei file di log dall'i/o di lettura/scrittura casuale dei file di dati e migliora significativamente le prestazioni di SQL Server.
- Assicurarsi che i file del database utente e la directory di log per l'archiviazione del backup del log si trovino su un'unità di archiviazione separata per evitare che il criterio di conservazione sovrascriva gli snapshot quando vengono utilizzati con la funzione SnapMirror con i criteri del vault.
- Non mischiare file di database e non di database, come file di ricerca full-text, sulla stessa unità di archiviazione.
- L'inserimento dei file secondari del database (come parte di un filegroup) in un'unità di archiviazione separata migliora le prestazioni del database di SQL Server. Questa separazione è valida solo se il file del database .mdf non condivide l'unità di archiviazione con altri .mdf file.
- Durante la formattazione del disco utilizzando il gestore dischi nel server Windows, assicurarsi che la dimensione dell'unità di allocazione sia impostata su 64K per la partizione.
- Non posizionare database utente o database di sistema su un'unità di archiviazione che ospita punti di montaggio.
- Vedere ["Microsoft Windows e MPIO nativo nelle Best practice ONTAP per le SAN moderne"](#) Per applicare il supporto multipathing in Windows ai dispositivi iSCSI nelle proprietà MPIO.
- Se si utilizza un'istanza cluster di failover sempre attiva, i database utente devono essere collocati nell'unità di storage condivisa tra i nodi cluster di failover del server Windows e le risorse del cluster di dischi fisici vengono assegnate al gruppo di cluster associato all'istanza di SQL Server.

File di database e filegroup

Il corretto posizionamento dei file del database SQL Server su ONTAP è fondamentale durante la fase di distribuzione iniziale. Ciò garantisce prestazioni ottimali, gestione dello spazio, tempi di backup e ripristino che possono essere configurati in base alle esigenze aziendali.

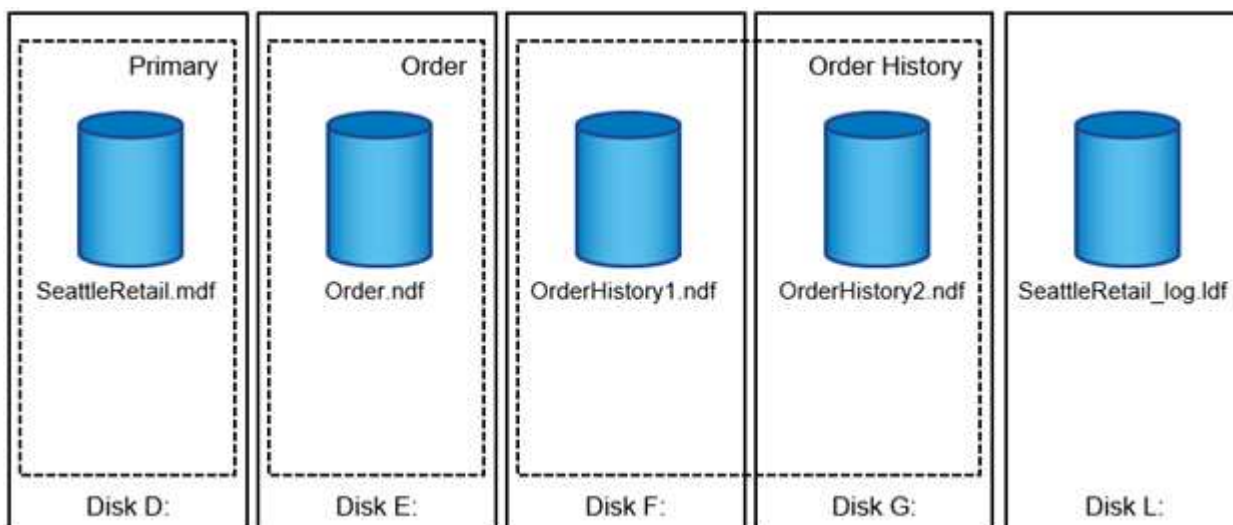
In teoria, SQL Server (a 64 bit) supporta 32.767 database per istanza e 524.272TB di dimensioni del database, sebbene l'installazione tipica abbia in genere diversi database. Tuttavia, il numero di database che SQL Server è in grado di gestire dipende dal carico e dall'hardware. Non è insolito vedere le istanze di SQL Server che ospitano decine, centinaia o persino migliaia di database di piccole dimensioni.

File di database e filegroup

Ogni database è costituito da uno o più file di dati e da uno o più file di registro delle transazioni. Il registro delle transazioni memorizza le informazioni sulle transazioni del database e tutte le modifiche apportate ai dati da ciascuna sessione. Ogni volta che i dati vengono modificati, SQL Server memorizza informazioni sufficienti nel log delle transazioni per annullare (eseguire il rollback) o ripristinare (riprodurre nuovamente) l'azione. Un log delle transazioni di SQL Server è parte integrante della reputazione di SQL Server in termini di integrità e robustezza dei dati. Il log delle transazioni è fondamentale per le funzionalità di atomicità, coerenza, isolamento e durata (ACID) di SQL Server. SQL Server scrive nel registro delle transazioni non appena si verifica una modifica alla pagina dei dati. Ogni istruzione DML (Data Manipulation Language) (ad esempio, SELECT, INSERT, Update o DELETE) è una transazione completa e il log delle transazioni garantisce che l'intera operazione basata su set abbia luogo, assicurando l'atomicità della transazione.

Ogni database dispone di un file di dati primario che, per impostazione predefinita, ha l'estensione .mdf. Inoltre, ogni database può disporre di file di database secondari. Questi file, per impostazione predefinita, hanno estensioni .ndf.

Tutti i file di database sono raggruppati in filegroup. Un filegroup è l'unità logica, che semplifica l'amministrazione del database. Consentono la separazione tra il posizionamento degli oggetti logici e i file di database fisici. Quando si creano le tabelle degli oggetti del database, si specifica in quale filegroup devono essere posizionati senza preoccuparsi della configurazione del file di dati sottostante.



La possibilità di inserire più file di dati all'interno del filegroup consente di distribuire il carico su diversi dispositivi di archiviazione, migliorando le prestazioni di i/o del sistema. Al contrario, il log delle transazioni non trae vantaggio dai file multipli poiché SQL Server scrive nel log delle transazioni in modo sequenziale.

La separazione tra il posizionamento degli oggetti logici nei filegroup e i file di database fisici consente di ottimizzare il layout dei file di database, ottenendo il massimo dal sottosistema di storage. Il numero di file di dati che supportano un carico di lavoro può essere variato in base alle necessità per supportare i requisiti di i/o e la capacità prevista, senza influire sull'applicazione. Queste variazioni nel layout del database sono trasparenti per gli sviluppatori di applicazioni, che posizionano gli oggetti del database nei filegroup piuttosto che nei file di database.



NetApp recommended evitare l'utilizzo del filegroup primario per oggetti diversi da quelli di sistema. La creazione di un filegroup separato o di un set di filegroup per gli oggetti utente semplifica l'amministrazione del database e il ripristino di emergenza, soprattutto nel caso di database di grandi dimensioni.

Inizializzazione del file di istanza del database

È possibile specificare le dimensioni iniziali del file e i parametri di crescita automatica al momento della creazione del database o dell'aggiunta di nuovi file a un database esistente. SQL Server utilizza un algoritmo di riempimento proporzionale quando sceglie in quale file di dati scrivere i dati. Scrive una quantità di dati proporzionalmente allo spazio libero disponibile nei file. Maggiore è lo spazio libero nel file, maggiore è il numero di scritture gestite.



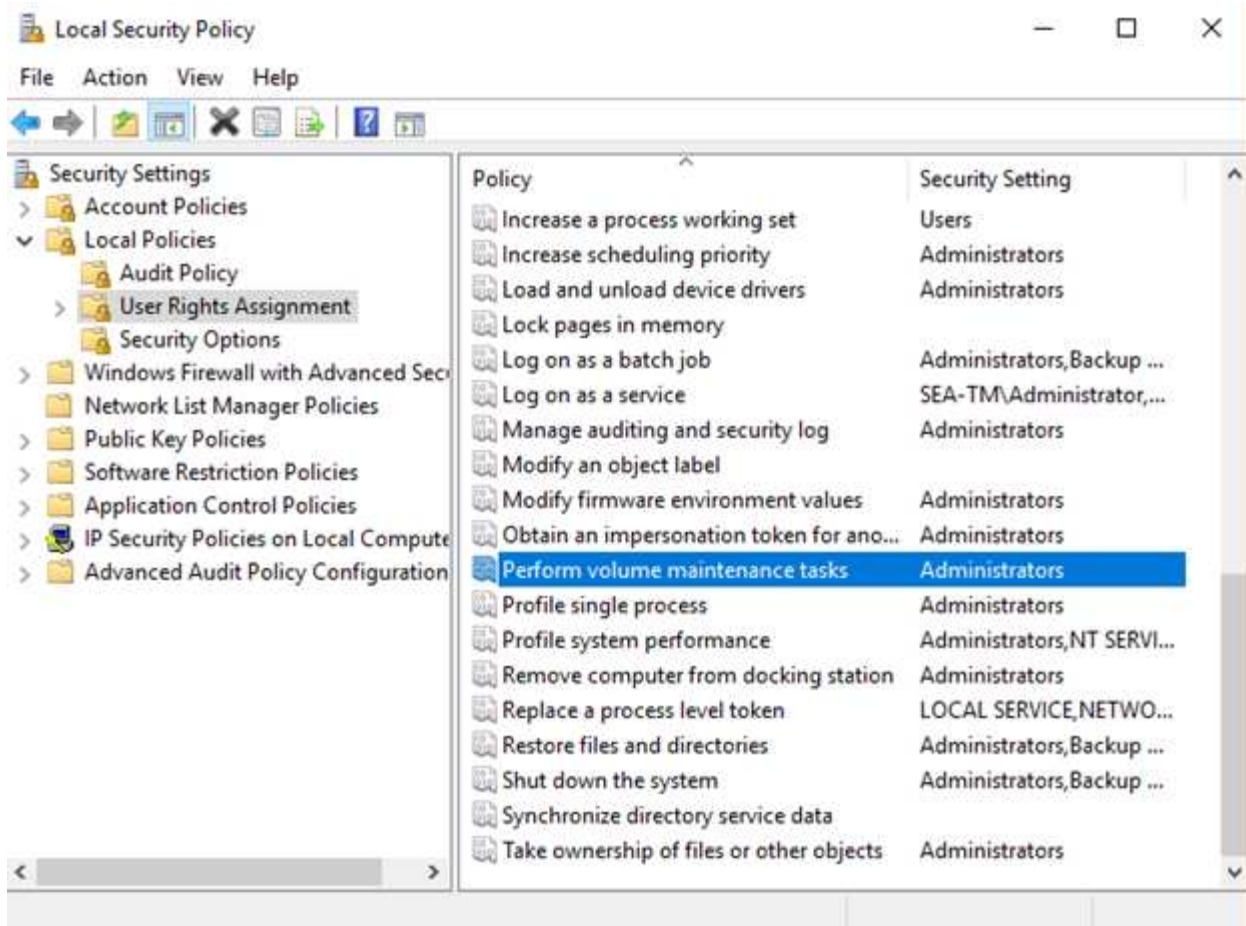
NetApp consiglia che tutti i file nel singolo filegroup abbiano le stesse dimensioni iniziali e parametri di crescita automatica, con la dimensione di crescita definita in megabyte piuttosto che in percentuali. Questo aiuta l'algoritmo di riempimento proporzionale a bilanciare uniformemente le attività di scrittura nei file di dati.

Ogni volta che SQL Server espande i file, riempie di zero lo spazio appena allocato. Questo processo blocca tutte le sessioni che devono scrivere nel file corrispondente o, in caso di crescita del log delle transazioni, genera record di log delle transazioni.

SQL Server azzerà sempre il log delle transazioni e questo comportamento non può essere modificato. Tuttavia, è possibile controllare se i file di dati vengono azzerati attivando o disattivando l'inizializzazione istantanea dei file. L'attivazione dell'inizializzazione immediata dei file consente di velocizzare la crescita dei file di dati e di ridurre il tempo necessario per creare o ripristinare il database.

Un piccolo rischio per la sicurezza è associato all'inizializzazione immediata dei file. Quando questa opzione è attivata, le parti non allocate del file di dati possono contenere informazioni provenienti da file del sistema operativo eliminati in precedenza. Gli amministratori di database possono esaminare tali dati.

È possibile attivare l'inizializzazione immediata dei file aggiungendo l'autorizzazione SA_MANAGE_VOLUME_NAME, nota anche come "Esegui attività di manutenzione del volume" all'account di avvio di SQL Server. È possibile eseguire questa operazione nell'applicazione di gestione dei criteri di protezione locale (secpol.msc), come illustrato nella figura seguente. Aprire le proprietà per l'autorizzazione "Esegui attività di manutenzione del volume" e aggiungere l'account di avvio di SQL Server all'elenco degli utenti.



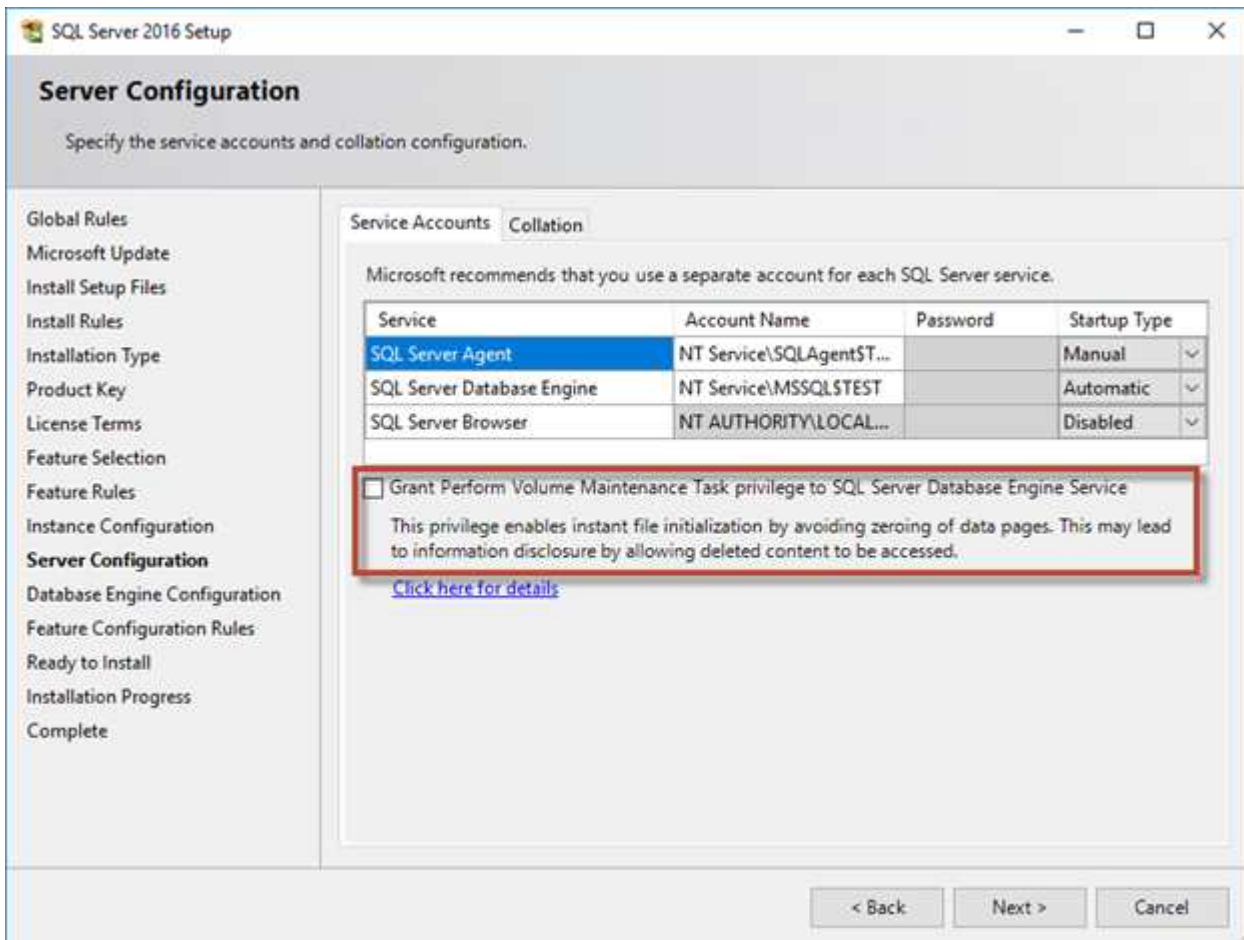
Per verificare se l'autorizzazione è attivata, è possibile utilizzare il codice riportato nell'esempio seguente. Questo codice imposta due flag di traccia che obbligano SQL Server a scrivere informazioni aggiuntive nel registro degli errori, a creare un database di piccole dimensioni e a leggere il contenuto del registro.

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

Quando l'inizializzazione immediata del file non è attivata, il registro degli errori di SQL Server mostra che SQL Server sta azzerando il file di dati mdf oltre a azzerare il file di registro ldf, come illustrato nell'esempio seguente. Quando l'inizializzazione immediata del file è attivata, viene visualizzato solo l'azzeramento del file di registro.

	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\Microsoft SQL Server\90\Shared\
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQL\DATA\
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL Server\MSSQL\DATA\
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.

L'attività Esegui manutenzione volume è semplificata in SQL Server 2016 e viene fornita come opzione durante il processo di installazione. In questa figura viene visualizzata l'opzione per concedere al servizio del motore di database di SQL Server il privilegio di eseguire l'attività di manutenzione del volume.



Un'altra importante opzione del database che controlla le dimensioni dei file di database è l'autohrink. Quando questa opzione è attivata, SQL Server riduce regolarmente i file di database, ne riduce le dimensioni e rilascia spazio al sistema operativo. Questa operazione richiede molte risorse ed è raramente utile perché i file di database crescono di nuovo dopo un certo periodo di tempo quando nuovi dati entrano nel sistema. Il collegamento automatico non deve essere attivato nel database.

Directory di log

La directory di registro è specificata in SQL Server per memorizzare i dati di backup del registro delle transazioni a livello di host. Se si utilizza SnapCenter per eseguire il backup dei file di registro, ciascun host SQL Server utilizzato da SnapCenter deve disporre di una directory di registro host configurata per eseguire i backup dei registri.

Posizionare la directory di registro su un'unità di archiviazione dedicata. La quantità di dati nella directory del registro host dipende dalle dimensioni dei backup e dal numero di giorni in cui i backup vengono conservati. SnapCenter consente una sola directory di registro host per host SQL Server. È possibile configurare la directory del registro host in SnapCenter → host → Configura plug-in.

NetApp consiglia quanto segue per una directory del registro host:



- Assicurarsi che la directory del registro host non sia condivisa da altri tipi di dati che potrebbero danneggiare i dati dello snapshot di backup.
- Creare la directory del registro host su un'unità di archiviazione dedicata in cui SnapCenter copia i registri delle transazioni.
- Se si utilizza un'istanza cluster di failover sempre attiva, l'unità di storage utilizzata per la directory di log dell'host deve essere una risorsa disco del cluster nello stesso gruppo di cluster dell'istanza di SQL Server di cui si esegue il backup in SnapCenter.

Protezione dei dati

Le strategie di backup dei database devono basarsi su requisiti aziendali identificati, non su capacità teoriche. Combinando la tecnologia Snapshot di ONTAP e sfruttando le API di Microsoft SQL Server, è possibile eseguire rapidamente un backup coerente delle applicazioni indipendentemente dalle dimensioni dei database utente. Per requisiti di gestione dei dati più avanzati o scale-out, NetApp offre SnapCenter.

SnapCenter

SnapCenter è il software di data Protection di NetApp per le applicazioni aziendali. I database di SQL Server possono essere protetti in modo rapido e semplice con il plug-in SnapCenter per SQL Server e con operazioni del sistema operativo gestite dal plug-in SnapCenter per Microsoft Windows.

L'istanza di SQL Server può essere un'installazione autonoma, un'istanza cluster di failover o può essere un gruppo di disponibilità sempre attivo. Il risultato è che, grazie a un singolo pannello di controllo, i database possono essere protetti, clonati e ripristinati da una copia primaria o secondaria. SnapCenter può gestire database SQL Server sia on-premise, nel cloud che in configurazioni ibride. Le copie dei database possono essere create in pochi minuti sull'host originale o alternativo per lo sviluppo o per il reporting.

SQL Server richiede inoltre un coordinamento tra il sistema operativo e lo storage per garantire che i dati corretti siano presenti negli snapshot al momento della creazione. Nella maggior parte dei casi, l'unico metodo sicuro per eseguire questa operazione è SnapCenter o T-SQL. Gli snapshot creati senza questo coordinamento aggiuntivo potrebbero non essere recuperabili in modo affidabile.

Per ulteriori informazioni sul plug-in di SQL Server per SnapCenter, vedere ["TR-4714: Guida alle Best practice per SQL Server con NetApp SnapCenter"](#).

Protezione del database mediante snapshot T-SQL

In SQL Server 2022, Microsoft ha introdotto le istantanee T-SQL che offrono un percorso per la creazione di script e l'automazione delle operazioni di backup. Invece di eseguire copie di dimensioni normali, è possibile preparare il database per le snapshot. Una volta che il database è pronto per il backup, è possibile sfruttare le API REST di ONTAP per creare snapshot.

Di seguito è riportato un esempio di flusso di lavoro di backup:

1. Bloccare un database con il comando ALTER. In questo modo il database viene preparato per uno snapshot coerente sullo storage sottostante. Dopo il blocco è possibile scongelare il database e registrare lo snapshot con il comando di BACKUP.
2. Eseguire istantanee di più database sulle unità di archiviazione contemporaneamente con il nuovo GRUPPO DI BACKUP e i comandi del SERVER DI BACKUP.
3. Se il carico di lavoro del database viene eseguito su più unità di storage, creare gruppi di coerenza per semplificare l'attività di gestione. Il gruppo di coerenza è un insieme di unità di archiviazione gestite come unità singola.
4. Eseguire backup COMPLETI o backup COMPLETI COPY_ONLY. Anche questi backup sono registrati in msdb.
5. Eseguire il recovery point-in-time utilizzando i backup di log eseguiti con il normale approccio di streaming dopo il backup COMPLETO delle snapshot. Se lo si desidera, sono supportati anche i backup differenziali in streaming.

Per ulteriori informazioni, vedere ["Documentazione Microsoft per conoscere le istantanee T-SQL"](#).



NetApp recommended Using SnapCenter to create Snapshot copy. Anche il metodo T-SQL descritto sopra funziona, ma SnapCenter offre un'automazione completa sul processo di backup, ripristino e cloning. Esegue inoltre il rilevamento per garantire che vengano creati gli snapshot corretti.

Disaster recovery

Disaster recovery

I database e le infrastrutture applicative aziendali spesso richiedono la replica per proteggersi da disastri naturali o interruzioni impreviste del business, con tempi di inattività minimi.

La funzionalità di replica del gruppo di disponibilità always-on di SQL Server può essere un'opzione eccellente e NetApp offre opzioni per integrare la protezione dei dati con Always-on. In alcuni casi, tuttavia, è consigliabile prendere in considerazione la tecnologia di replica ONTAP utilizzando le seguenti opzioni.

SnapMirror

La tecnologia SnapMirror offre una soluzione aziendale rapida e flessibile per la replica dei dati su LAN e WAN. La tecnologia SnapMirror trasferisce solo i blocchi di dati modificati a destinazione dopo la creazione del mirror iniziale, riducendo in modo significativo i requisiti di larghezza di banda della rete. Può essere configurato in modalità sincrona o asincrona. La replica sincrona SnapMirror in NetApp ASA è configurata con la sincronizzazione attiva SnapMirror.

Sincronizzazione attiva di SnapMirror

Per molti clienti, la business continuity richiede molto più del semplice possesso di una copia remota dei dati, ma richiede la capacità di sfruttarli rapidamente, cosa possibile in NetApp ONTAP utilizzando la sincronizzazione attiva di SnapMirror.

Con la sincronizzazione attiva di SnapMirror, avrai essenzialmente due sistemi ONTAP diversi che mantengono copie indipendenti dei dati LUN, ma cooperano per presentare una singola istanza di tale LUN. Dal punto di vista dell'host, si tratta di una singola entità LUN. La sincronizzazione attiva di SnapMirror è supportata per LUN basata su iSCSI/FC.

La SnapMirror Active Sync può fornire una replica con RPO=0 ed è semplice da implementare tra due cluster indipendenti. Una volta sincronizzate le due copie di dati, i due cluster devono solo mirrorare le scritture. Quando si verifica una scrittura su un cluster, questa viene replicata nell'altro cluster. La scrittura viene riconosciuta all'host solo quando la scrittura è stata completata su entrambi i siti. A parte questo comportamento di suddivisione del protocollo, i due cluster sono altrimenti normali cluster ONTAP.

Un caso d'utilizzo chiave per SM-AS è la replica granulare. A volte non vuoi replicare tutti i dati come una singola unità oppure devi eseguire il failover selettivo su alcuni carichi di lavoro.

Un altro caso d'utilizzo chiave per SM-AS è per operazioni Active-Active, dove desideri che siano disponibili copie dei dati completamente utilizzabili su due cluster diversi situati in due posizioni diverse con caratteristiche di performance identiche e, se desiderato, non richiedere l'estensione della SAN tra i siti. Le applicazioni potranno essere già in esecuzione su entrambi i siti, a condizione che sia supportata un'applicazione, con una conseguente riduzione dell'RTO complessivo durante le operazioni di failover.

SnapMirror

Di seguito sono riportati alcuni consigli su SnapMirror per SQL Server:

- Utilizza la replica sincrona con la sincronizzazione attiva SnapMirror, in cui la richiesta di un recovery di dati rapido è maggiore e soluzioni asincrone per la flessibilità negli RPO.
- Se stai utilizzando SnapCenter per eseguire il backup dei database e replicare le snapshot su un cluster remoto, non pianificare gli aggiornamenti SnapMirror dai controller per motivi di coerenza. Attiva invece gli update di SnapMirror da SnapCenter per aggiornare SnapMirror al termine del backup completo o del log.
- Bilancia le unità di storage che contengono dati SQL Server nei diversi nodi del cluster per consentire a tutti i nodi del cluster di condividere l'attività di replica di SnapMirror. Questa distribuzione ottimizza l'utilizzo delle risorse dei nodi.

Per ulteriori informazioni su SnapMirror, vedere ["TR-4015: Guida alle Best practice e alla configurazione di SnapMirror per ONTAP 9"](#).

Sincronizzazione attiva di SnapMirror

Panoramica

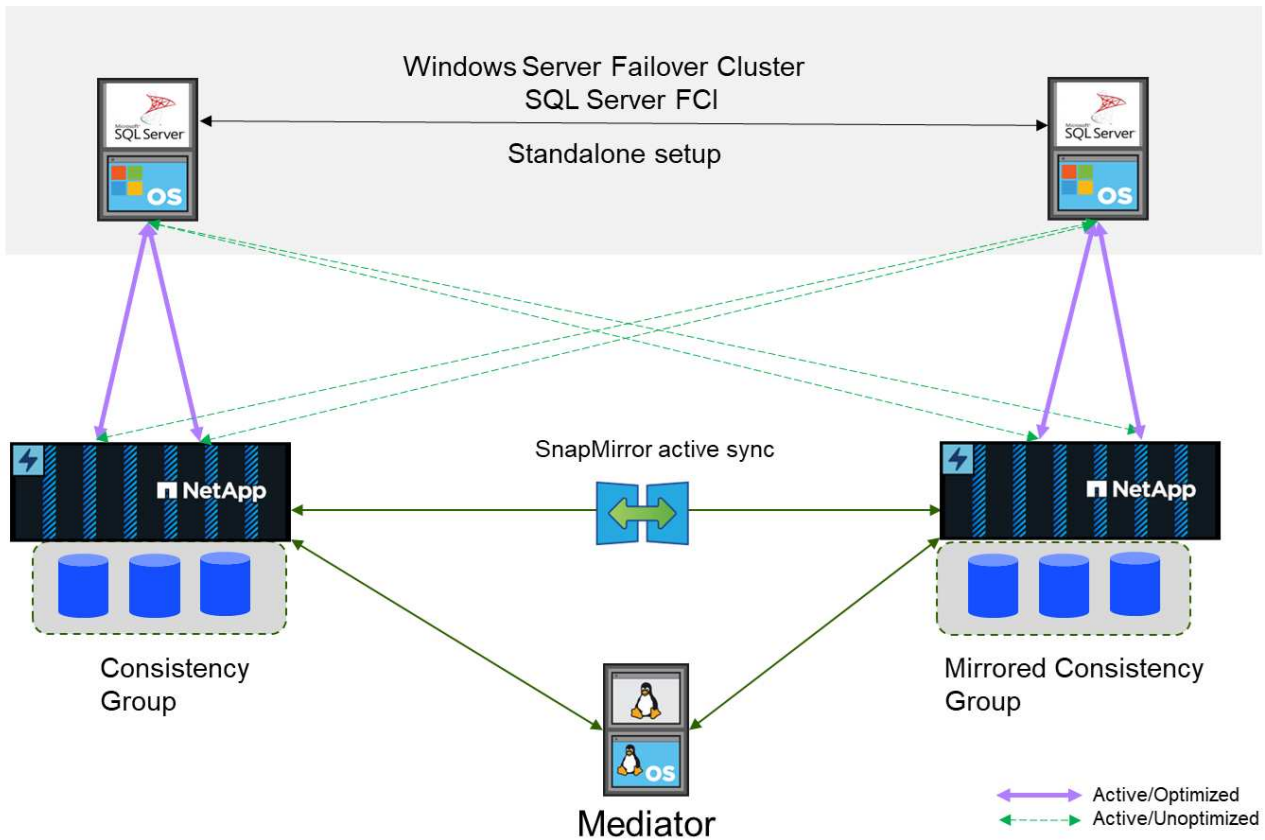
La sincronizzazione attiva di SnapMirror consente a singoli database e applicazioni SQL Server di continuare le operazioni durante interruzioni di rete e storage, con failover trasparente dello storage senza interventi manuali.

SnapMirror Active Sync supporta l'architettura Active/Active simmetrica che offre replica bidirezionale sincrona per la business continuity e il disaster recovery. Protegge l'accesso ai dati per carichi di lavoro critici SAN con accesso simultaneo in lettura e scrittura ai dati in diversi domini di errore, garantendo operazioni senza

interruzioni e riducendo al minimo i downtime in caso di disastri o errori di sistema.

Gli host SQL Server accedono allo storage utilizzando LUN Fiber Channel (FC) o iSCSI. Replica tra ciascun cluster in cui risiede una copia dei dati replicati. Poiché questa funzionalità è la replica a livello di storage, le istanze di SQL Server in esecuzione su istanze di cluster di failover o host standalone possono eseguire operazioni di lettura/scrittura in entrambi i cluster. Per le fasi di pianificazione e configurazione, fare riferimento a ["Documentazione di ONTAP sulla sincronizzazione attiva di SnapMirror"](#).

Architettura di SnapMirror Active con Active/Active simmetrico



Replica sincrona

Durante l'utilizzo normale, ciascuna copia è una replica sincrona con RPO=0/7, con un'unica eccezione. Se i dati non possono essere replicati, ONTAP rilascerà il requisito di replicare i dati e riprendere la distribuzione io su un sito mentre le LUN dell'altro sito vengono portate offline.

Hardware di archiviazione

A differenza di altre soluzioni di disaster recovery per lo storage, SnapMirror Active Sync offre una flessibilità asimmetrica della piattaforma. Non è necessario che l'hardware di ciascun sito sia identico. Questa funzionalità consente di dimensionare correttamente l'hardware utilizzato per supportare la sincronizzazione attiva di SnapMirror. Il sistema di storage remoto può essere identico al sito primario se deve supportare un carico di lavoro di produzione completo, ma se un disastro determina una riduzione dell'i/o, rispetto a un sistema più piccolo nel sito remoto potrebbe risultare più conveniente.

ONTAP mediatore

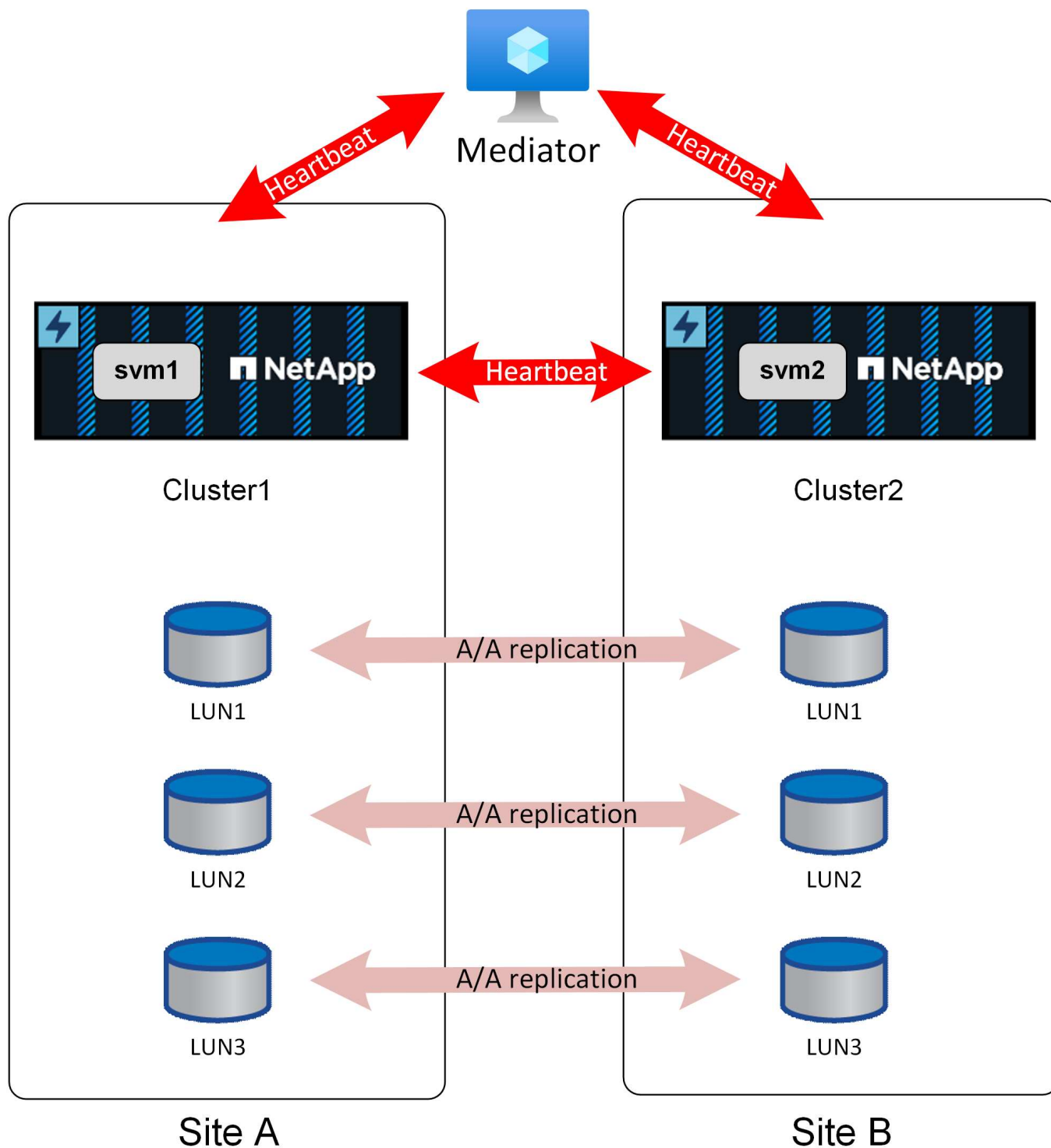
ONTAP Mediator è un'applicazione software che viene scaricata dal supporto NetApp e che viene in genere distribuita su una piccola macchina virtuale. Il ONTAP Mediator non è un tiebreaker. È un canale di

comunicazione alternativo per i due cluster che partecipano alla replica sincrona attiva SnapMirror. Le operazioni automatizzate sono gestite da ONTAP in base alle risposte ricevute dal partner tramite connessioni dirette e tramite il mediatore.

Mediatore ONTAP

Il mediatore è necessario per automatizzare in modo sicuro il failover. Idealmente, sarebbe posizionato su un sito 3rd indipendente, ma può comunque funzionare per la maggior parte delle esigenze se colocated con uno dei cluster che partecipano alla replica.

Il mediatore non è realmente un tiebreaker, anche se quella è effettivamente la funzione che fornisce. Non esegue alcuna azione, ma fornisce un canale di comunicazione alternativo per la comunicazione tra cluster e cluster.



La sfida #1 con il failover automatizzato è il problema split-brain, e questo problema sorge se i due siti perdono la connettività tra loro. Che cosa dovrebbe accadere? Non si desidera che due siti diversi si designino come copie sopravvissute dei dati, ma in che modo un singolo sito può distinguere tra la perdita effettiva del sito opposto e l'impossibilità di comunicare con il sito opposto?

Qui entra il mediatore nell'immagine. Se si trova in un sito 3rd e ciascun sito dispone di una connessione di rete separata per tale sito, è disponibile un percorso aggiuntivo per ciascun sito per convalidare lo stato dell'altro. Esaminare nuovamente l'immagine sopra riportata e considerare i seguenti scenari.

- Cosa succede se il mediatore non riesce o è irraggiungibile da uno o entrambi i siti?
 - I due cluster possono ancora comunicare tra loro sullo stesso link utilizzato per i servizi di replica.
 - I dati sono ancora serviti con protezione RPO=0/7
- Cosa succede se il sito A non funziona?
 - Il sito B vedrà che entrambi i canali di comunicazione si interrompono.
 - Il sito B sostituirà i servizi dati, ma senza RPO = mirroring 0:1
- Cosa succede se il sito B non funziona?
 - Il sito A vedrà che entrambi i canali di comunicazione si interrompono.
 - Il sito A sostituirà i servizi dati, ma senza RPO = mirroring 0:1

Esiste un altro scenario da considerare: La perdita del collegamento di replica dei dati. In caso di perdita del link di replica tra i siti, RPO=0 Mirroring sarà ovviamente impossibile. Che cosa dovrebbe accadere allora?

Questo è controllato dallo stato del sito preferito. In una relazione SM-AS, uno dei siti è secondario all'altro. Questo non ha alcun effetto sulle normali operazioni e tutto l'accesso ai dati è simmetrico, ma se la replica viene interrotta, il legame dovrà essere interrotto per riprendere le operazioni. Ne risulta che il sito preferito continuerà le operazioni senza mirroring e il sito secondario interromperà l'elaborazione io fino al ripristino della comunicazione di replica.

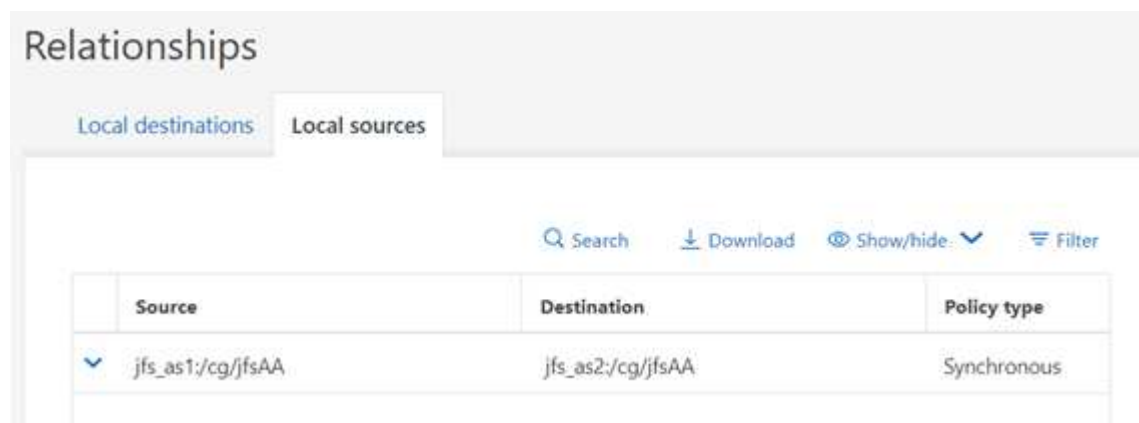
Sito preferito

Il comportamento di sincronizzazione attiva di SnapMirror è simmetrico, con una eccezione importante: Configurazione del sito preferito.

La sincronizzazione attiva di SnapMirror considererà un sito la "fonte" e l'altro la "destinazione". Ciò implica una relazione di replica unidirezionale, ma ciò non si applica al comportamento io. La replica è bidirezionale e simmetrica, mentre i tempi di risposta io sono identici su entrambi i lati del mirror.

La `source` designazione controlla il sito preferito. In caso di perdita del link di replica, i percorsi delle LUN nella copia di origine continueranno a fornire i dati mentre i percorsi delle LUN nella copia di destinazione non saranno disponibili finché la replica non viene ristabilita e SnapMirror ritorna allo stato sincrono. I percorsi riprenderanno a fornire i dati.

La configurazione di origine/destinazione può essere visualizzata tramite SystemManager:



Relationships		
Local destinations		Local sources
<div> Search Download Show/hide Filter </div>		
Source	Destination	Policy type
<div> ▼ jfs_as1:/cg/jfsAA </div>	jfs_as2:/cg/jfsAA	Synchronous

O all'interfaccia 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
```

La chiave è che source è l'SVM su cluster1. Come menzionato sopra, i termini "origine" e "destinazione" non descrivono il flusso di dati replicati. Entrambi i siti possono elaborare una scrittura e replicarla nel sito opposto. In effetti, entrambi i cluster sono origini e destinazioni. L'effetto della designazione di un cluster come origine controlla semplicemente quale cluster sopravvive come sistema di storage in lettura e scrittura in caso di perdita del link di replica.

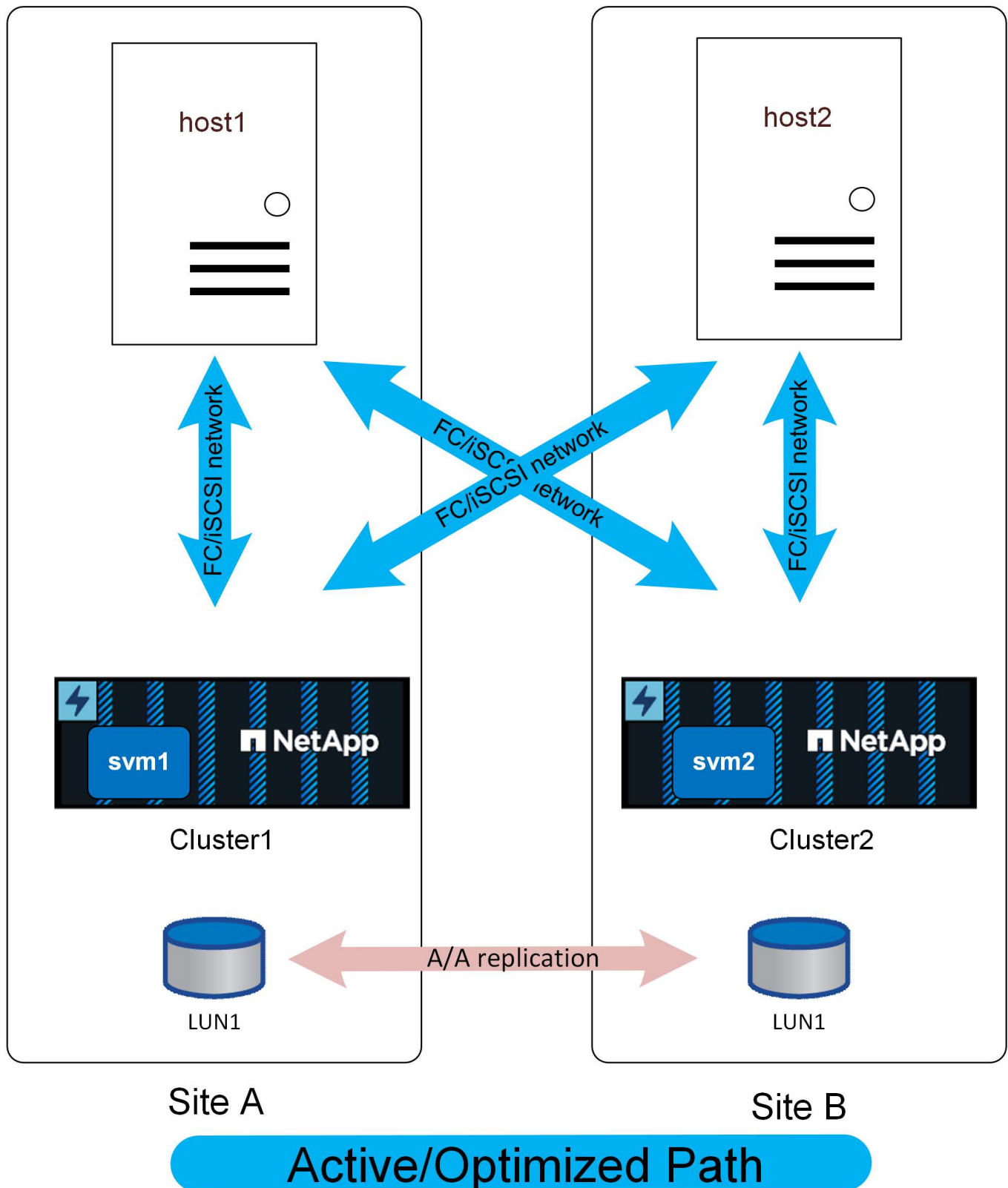
Topologia di rete

Accesso uniforme

Una rete ad accesso uniforme significa che gli host sono in grado di accedere ai percorsi su entrambi i siti (o ai domini di errore all'interno dello stesso sito).

Una caratteristica importante di SM-AS è la capacità di configurare i sistemi storage per sapere dove si trovano gli host. Quando si mappano i LUN a un determinato host, è possibile indicare se sono prossimi o meno a un determinato sistema di archiviazione.

I sistemi NetApp ASA offrono multipathing Active-Active su tutti i percorsi di un cluster. Questo vale anche per le configurazioni SM-AS.



Con un accesso uniforme, io attraverserebbe la WAN. Si tratta di un cluster completamente mesh collegato in rete e questo può essere o meno auspicabile per tutti i casi di utilizzo.

Se i due siti fossero a una distanza di 100 metri con connettività in fibra non dovrebbe esserci una latenza aggiuntiva rilevabile che attraversa la WAN, ma se i siti fossero a lunga distanza gli uni dagli altri, le

performance in lettura risulterebbero compromesse su entrambi i siti. ASA con rete di accesso non uniforme sarebbe un'opzione per ottenere i vantaggi in termini di costi e funzionalità di ASA senza incorrere in penalizzazioni per l'accesso alla latenza tra siti o utilizzare la funzionalità di prossimità dell'host per consentire l'accesso in lettura/scrittura locale tra siti per entrambi i siti.

ASA con SM-as in una configurazione a bassa latenza offre due benefici interessanti. In primo luogo, essenzialmente **raddoppia** le prestazioni per ogni singolo host perché io può essere gestito dal doppio dei controller utilizzando il doppio dei percorsi. In secondo luogo, in un ambiente a sito singolo offre una disponibilità estrema, perché è possibile perdere un intero sistema storage senza interrompere l'accesso degli host.

Impostazioni di prossimità

La prossimità si riferisce a una configurazione per cluster che indica che un determinato WWN host o ID iniziatore iSCSI appartiene a un host locale. Si tratta di un secondo passo opzionale per la configurazione dell'accesso LUN.

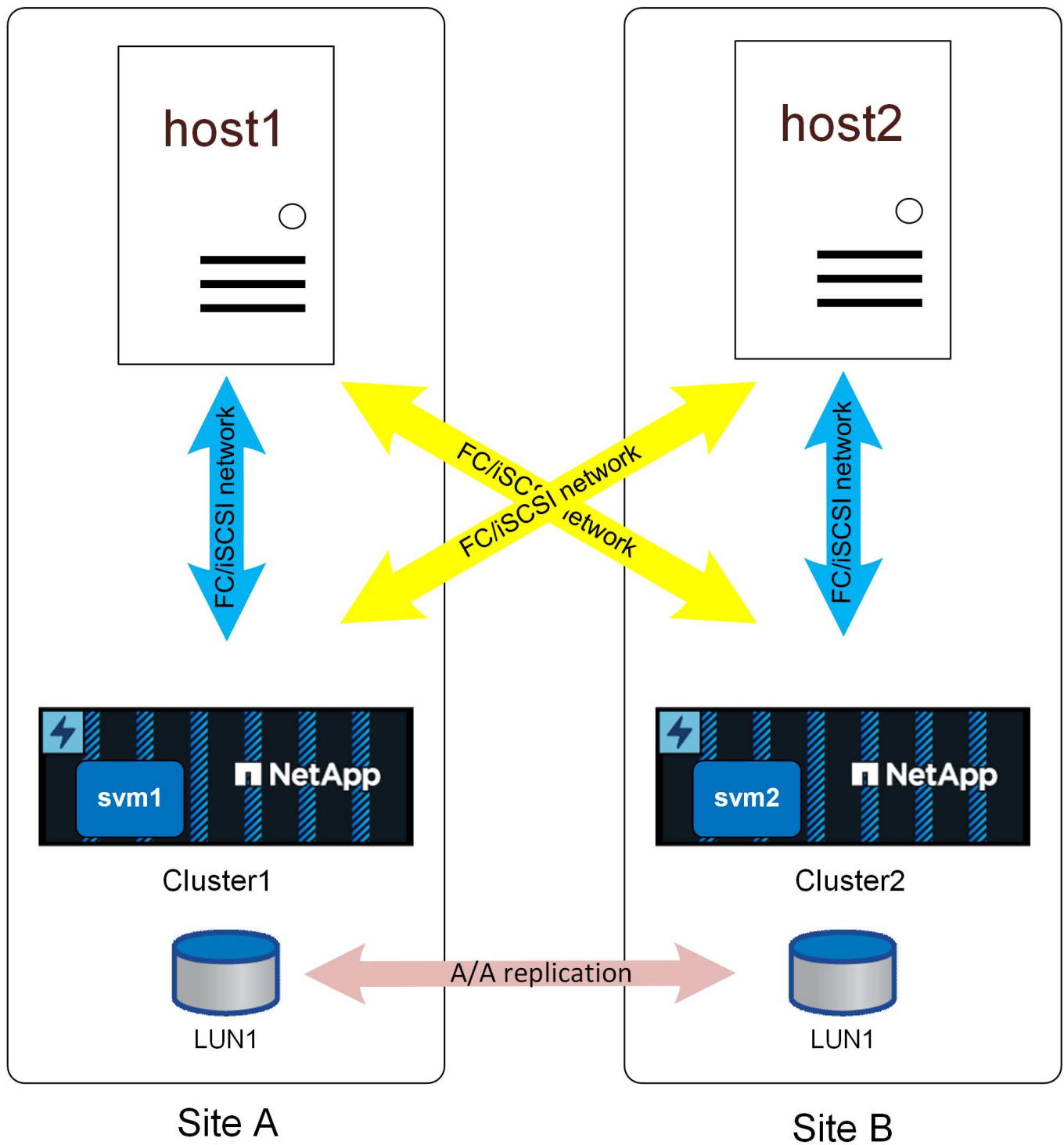
Il primo passo è la normale configurazione di igroup. Ogni LUN deve essere mappato a un igroup che contiene gli ID WWN/iSCSI degli host che devono accedere a quel LUN. Controlla quale host ha *accesso* a un LUN.

Il secondo passo, opzionale, consiste nel configurare la prossimità all'host. Questo non controlla l'accesso, controlla *priority*.

Ad esempio, un host del sito A potrebbe essere configurato in modo da accedere a una LUN protetta dalla sincronizzazione attiva di SnapMirror e, poiché la SAN è estesa tra i siti, i percorsi sono disponibili per tale LUN utilizzando lo storage sul sito A o lo storage sul sito B.

Senza impostazioni di prossimità, l'host utilizzerà entrambi i sistemi storage allo stesso modo perché entrambi i sistemi storage pubblicizzeranno i percorsi attivi/ottimizzati. Se la latenza SAN e/o la larghezza di banda tra i siti è limitata, questa operazione potrebbe non essere disattivabile e potrebbe essere necessario assicurarsi che durante il normale funzionamento ogni host utilizzi preferenzialmente i percorsi verso il sistema di storage locale. Viene configurato aggiungendo l'ID WWN/iSCSI dell'host al cluster locale come host prossimale. Questa operazione può essere eseguita dalla CLI o da SystemManager.

I percorsi vengono visualizzati come mostrato di seguito quando è stata configurata la prossimità host.

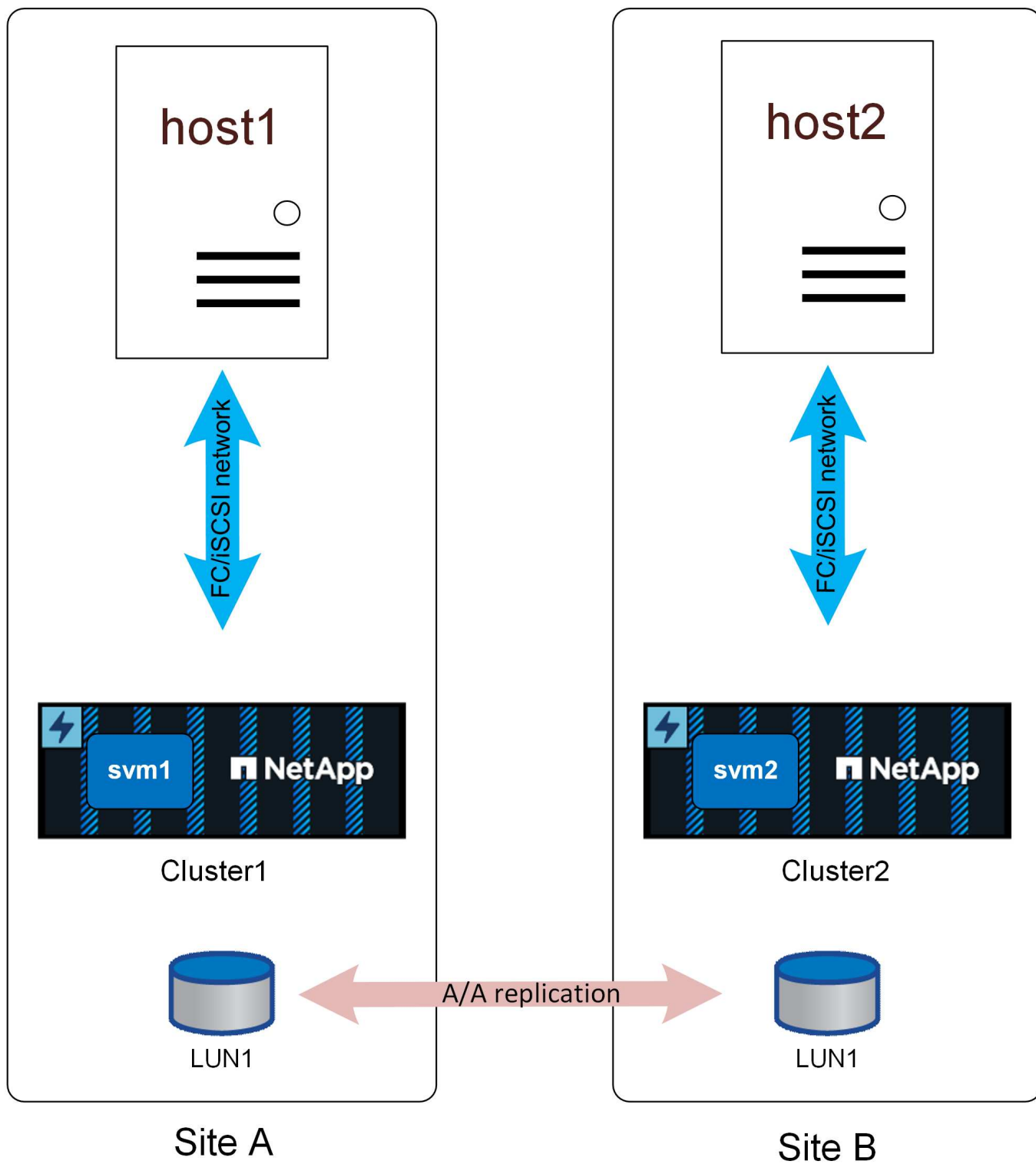


Active/Optimized Path

Active Path

Accesso non uniforme

Una rete di accesso non uniforme significa che ogni host ha solo accesso alle porte sul sistema di storage locale. LA SAN non è estesa a più siti (o presenta errori nei domini dello stesso sito).



Active/Optimized Path

Il vantaggio principale di questo approccio è la semplicità DELLE SAN, eliminando l'esigenza di stretching di una SAN via rete. Alcuni clienti non dispongono di connettività a latenza sufficientemente bassa tra i siti o non dispongono dell'infrastruttura per il tunnel del traffico FC SAN su una rete intersito.

Lo svantaggio legato all'accesso non uniforme è che alcuni scenari di errore, inclusa la perdita del collegamento di replica, provocheranno la perdita dell'accesso allo storage da parte di alcuni host. In caso di interruzione della connettività dello storage locale, le applicazioni eseguite come istanze singole, come ad esempio i database non in cluster, eseguiti in maniera intrinseca solo su un singolo host in uno qualsiasi dei supporti di montaggio, si guasterebbero. I dati sarebbero comunque protetti, ma il server di database non avrebbe più accesso. Dovrebbe essere riavviato su un sito remoto, preferibilmente tramite un processo automatizzato. Ad esempio, VMware ha è in grado di rilevare una situazione di tutti i percorsi verso l'esterno su un server e di riavviare una macchina virtuale su un altro server in cui sono disponibili i percorsi.

Al contrario, un'applicazione in cluster come Oracle RAC può offrire un servizio disponibile contemporaneamente in due siti diversi. Perdere un sito non significa perdere il servizio dell'applicazione nel suo complesso. Le istanze sono ancora disponibili e in esecuzione nel sito sopravvissuto.

In molti casi, l'overhead della latenza aggiuntivo di un'applicazione che accede allo storage attraverso un collegamento da sito a sito sarebbe inaccettabile. Ciò significa che la migliore disponibilità di una rete uniforme è minima, poiché la perdita di storage su un sito comporterebbe comunque la necessità di arrestare i servizi sul sito in cui si è verificato l'errore.

Esistono percorsi ridondanti attraverso il cluster locale non mostrati in questi diagrammi per semplicità. I sistemi di storage ONTAP sono ad alta disponibilità, pertanto un guasto a un controller non dovrebbe causare guasti nel sito. Ciò dovrebbe comportare solo una modifica dei percorsi locali utilizzati nel sito interessato.

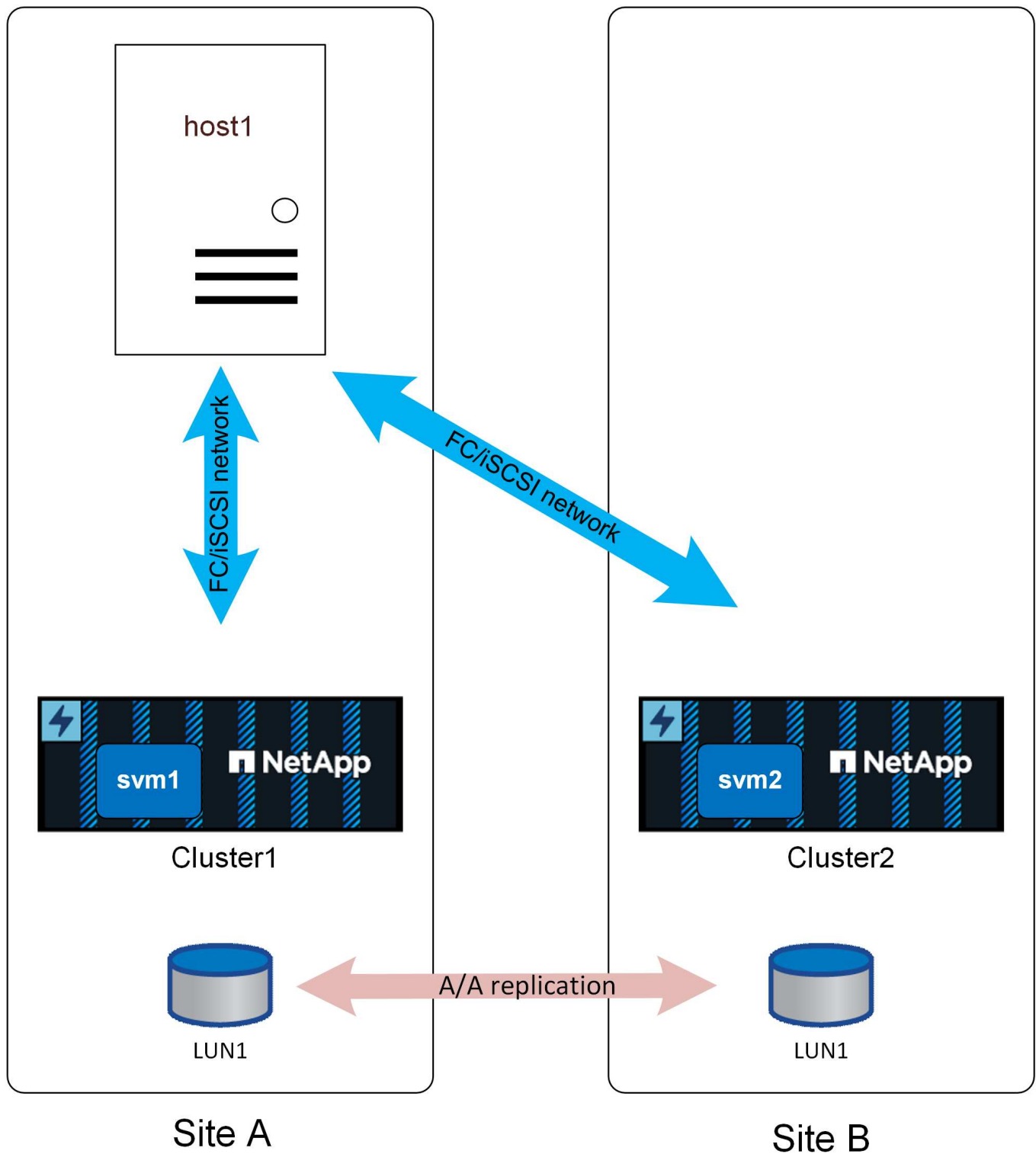
Panoramica

SQL Server può essere configurato per funzionare con la sincronizzazione attiva di SnapMirror in diversi modi. La risposta giusta dipende dalla connettività di rete disponibile, dai requisiti RPO e dai requisiti di disponibilità.

Istanza standalone di SQL Server

Le procedure consigliate per il layout dei file e la configurazione del server sono identiche a quelle consigliate nella ["Server SQL su ONTAP"](#) documentazione.

Con una configurazione standalone, SQL Server potrebbe essere eseguito solo in un sito. Presumibilmente ["uniforme"](#) si userebbe l'accesso.



Grazie a un accesso uniforme, un guasto dello storage in uno dei siti non interromperebbe le operazioni di database. Un errore completo del sito che includeva il server di database comporterebbe, ovviamente, un'interruzione del servizio.

Alcuni clienti potrebbero configurare un sistema operativo in esecuzione nel sito remoto con un'installazione di SQL Server preconfigurata, aggiornata con una versione di build equivalente a quella dell'istanza di produzione. Il failover richiede l'attivazione dell'istanza standalone di SQL Server nel sito alternativo, il rilevamento dei LUN e l'avvio del database. È possibile automatizzare il processo completo con il cmdlet di

Windows PowerShell, in quanto non sono richieste operazioni dal lato storage.

"Non uniforme" è possibile utilizzare anche l'accesso, ma il risultato sarebbe un'interruzione del database se il sistema storage in cui si trovava il server del database non avesse avuto esito positivo, perché il database non avrebbe percorsi disponibili per lo storage. In alcuni casi ciò può ancora essere accettabile. La sincronizzazione attiva di SnapMirror garantirebbe comunque una data Protection con RPO=0 e, in caso di guasto del sito, la copia restante sarebbe attiva e pronta a riprendere le operazioni seguendo la stessa procedura utilizzata con un accesso uniforme descritta sopra.

Un processo di failover semplice e automatizzato può essere configurato più facilmente con l'uso di un host virtualizzato. Ad esempio, se i file di dati di SQL Server vengono replicati in modo sincrono su storage secondario insieme a un VMDK di avvio, in caso di disastro è possibile attivare l'ambiente completo nel sito alternativo. Un amministratore può attivare manualmente l'host nel sito rimasto o automatizzare il processo tramite un servizio come VMware ha.

Istanza del cluster di failover di SQL Server

Le istanze di failover di SQL Server possono essere ospitate anche in un cluster di failover di Windows in esecuzione su un server fisico o virtuale come sistema operativo guest. Questa architettura multi-host offre un'istanza di SQL Server e la resilienza dello storage. Tale implementazione è utile in ambienti a domanda elevata che richiedono solidi processi di failover senza rinunciare a prestazioni avanzate. In una configurazione del cluster di failover, quando un host o uno storage primario viene colpito, SQL Services eseguirà il failover sull'host secondario e, allo stesso tempo, lo storage secondario sarà disponibile per servire io. Non è richiesto alcuno script di automazione o intervento dell'amministratore.

Scenari di errore

La pianificazione di un'architettura completa dell'applicazione SnapMirror Active Sync richiede la comprensione del modo in cui SM-AS risponderà in vari scenari di failover pianificati e non pianificati.

Per gli esempi seguenti, si supponga che il sito A sia configurato come sito preferito.

Interruzione della connettività di replica

Se la replica SM-AS viene interrotta, non è possibile completare la scrittura io perché sarebbe impossibile per un cluster replicare le modifiche al sito opposto.

Sito A (sito preferito)

Il risultato dell'errore del collegamento di replica sul sito preferito sarà una pausa di circa 15 secondi nell'elaborazione io in scrittura, poiché ONTAP ritenta le operazioni di scrittura replicate prima di determinare che il collegamento di replica è veramente irraggiungibile. Trascorsi i 15 secondi, il sistema del sito A riprende l'elaborazione io in lettura e scrittura. I percorsi SAN non vengono modificati e i LUN rimangono online.

Sito B

Poiché il sito B non è il sito preferito di sincronizzazione attiva SnapMirror, i relativi percorsi LUN non saranno più disponibili dopo circa 15 secondi.

Errore del sistema di storage

Il risultato di un errore del sistema di storage è quasi identico al risultato della perdita del collegamento di replica. Il sito sopravvissuto dovrebbe subire una pausa io di circa 15 secondi. Trascorso questo periodo di 15

secondi, io riprenderà sul sito come di consueto.

Perdita del mediatore

Il servizio di mediazione non controlla direttamente le operazioni di storage. Funziona come un percorso di controllo alternativo tra cluster. Esiste principalmente per automatizzare il failover senza il rischio di uno scenario split-brain. Durante l'utilizzo normale, ogni cluster replica le modifiche al partner e pertanto ogni cluster può verificare che il cluster partner sia online e fornisca i dati. Se il collegamento di replica non è riuscito, la replica viene interrotta.

Il motivo per cui è necessario un mediatore per il failover automatizzato sicuro è perché altrimenti sarebbe impossibile per un cluster di storage determinare se la perdita di comunicazione bidirezionale fosse il risultato di un'interruzione della rete o di un errore effettivo dello storage.

Il mediatore fornisce un percorso alternativo per ciascun cluster per verificare lo stato di salute del partner. Gli scenari sono i seguenti:

- Se un cluster può contattare direttamente il partner, i servizi di replica sono operativi. Non è richiesta alcuna azione.
- Se un sito preferito non può contattare direttamente il proprio partner o tramite il mediatore, presuppone che il partner sia effettivamente non disponibile oppure è stato isolato e ha portato i percorsi LUN offline. Il sito preferito procede quindi al rilascio dello stato RPO=0 e continua l'elaborazione dell'io in lettura e in scrittura.
- Se un sito non preferito non può contattare direttamente il proprio partner, ma può contattarlo tramite il mediatore, prenderà i suoi percorsi offline e attenderà il ritorno della connessione di replica.
- Se un sito non preferito non può contattare direttamente il proprio partner o tramite un mediatore operativo, supporterà che il partner sia effettivamente non disponibile, oppure che sia stato isolato e che abbia portato i percorsi LUN offline. Il sito non preferito procede quindi al rilascio dello stato RPO=0 e continua l'elaborazione dell'i/o in lettura e scrittura. Assumerà il ruolo dell'origine della replica e diventerà il nuovo sito preferito.

Se il mediatore non è completamente disponibile:

- In caso di guasto dei servizi di replica per qualsiasi motivo, incluso un guasto del sito o del sistema storage non preferito, il sito preferito rilascerà lo stato RPO=0 e riprenderà l'elaborazione i/o in lettura e scrittura. Il sito non preferito prenderà i suoi percorsi offline.
- Il guasto del sito preferito causerà un'interruzione poiché il sito non preferito non sarà in grado di verificare che il sito opposto sia effettivamente offline e quindi non sarebbe sicuro per il sito non preferito riprendere i servizi.

Ripristino dei servizi in corso

Dopo aver risolto un errore, come il ripristino della connettività da sito a sito o l'accensione di un sistema guasto, gli endpoint di sincronizzazione attivi di SnapMirror rilevano automaticamente la presenza di una relazione di replica difettosa e la riportano allo stato RPO=0. Una volta ristabilita la replica sincrona, i percorsi non riusciti torneranno in linea.

In molti casi, le applicazioni in cluster rilevano automaticamente la restituzione dei percorsi non riusciti e tali applicazioni tornano online. In altri casi, potrebbe essere necessaria una scansione SAN a livello di host oppure potrebbe essere necessario riportare le applicazioni online manualmente. Dipende dall'applicazione e dal modo in cui è configurata, e in generale tali attività possono essere facilmente automatizzate. ONTAP si sta auto-riparando e non deve richiedere alcun intervento da parte dell'utente per riprendere le operazioni di storage RPO = 0 KB.

Failover manuale

La modifica del sito preferito richiede un'operazione semplice. I/O si fermeranno per un secondo o due come autorità sugli switch del comportamento di replica tra i cluster, ma in caso contrario i/o non vengono influenzati.

Sicurezza dei dati

La protezione di un ambiente di database SQL Server è un'operazione multidimensionale che va oltre la gestione del database stesso. ONTAP offre diverse funzioni esclusive progettate per proteggere gli aspetti dello storage dell'infrastruttura di database.

Copie Snapshot

Le snapshot di storage sono repliche point-in-time dei dati di destinazione. L'implementazione di ONTAP include le funzionalità per impostare varie policy e memorizzare fino a 1024 snapshot per volume. Le Snapshot in ONTAP sono efficienti in termini di spazio. Lo spazio viene consumato solo quando viene modificato il set di dati originale. Sono anche di sola lettura. Uno snapshot può essere eliminato, ma non può essere modificato.

In alcuni casi, le snapshot possono essere pianificate direttamente su ONTAP. In altri casi, software come SnapCenter potrebbe essere necessario per orchestrare le operazioni dell'applicazione o del sistema operativo prima di creare snapshot. Qualunque sia l'approccio migliore per i tuoi workload, un'aggressiva strategia di snapshot può garantire sicurezza dei dati tramite un accesso frequente e facilmente accessibile ai backup di ogni elemento, dalle LUN di avvio ai database mission-critical.



Un volume flessibile ONTAP, o più semplicemente, un volume non è sinonimo di LUN. I volumi sono container di gestione per dati come file o LUN. Ad esempio, un database può essere posizionato su un set di stripe da 8 LUN, con tutti i LUN contenuti in un singolo volume.

Per ulteriori informazioni sulle istantanee, consultare la ["Documentazione ONTAP."](#)

Snapshot a prova di manomissione

A partire da ONTAP 9.12.1, gli snapshot non sono solo di lettura, ma possono anche essere protetti da eliminazioni accidentali o intenzionali. La funzione è denominata istantanee antimanomissione. È possibile impostare e applicare un periodo di conservazione tramite policy snapshot. Gli snapshot risultanti non possono essere eliminati fino a quando non hanno raggiunto la data di scadenza. Non sono presenti sostituzioni amministrative o del centro di supporto.

In questo modo, un intruso, un malintenzionato o persino un attacco ransomware non sono in grado di compromettere i backup, anche nel caso in cui abbiano accesso al sistema ONTAP stesso. Se combinato con una pianificazione degli snapshot frequente, offre una data Protection estremamente potente con un RPO molto basso.



Non è possibile eseguire il tiering delle snapshot a prova di manomissione utilizzando il fabric pool.

Per ulteriori informazioni sugli snapshot antimanomissione, consultare la ["Documentazione ONTAP."](#)



Nella nuova piattaforma ASA, replicare le snapshot nel cluster remoto utilizzando il criterio *vault*, quindi bloccare la destinazione per rendere le snapshot a prova di manomissione.

Replica SnapMirror

Gli snapshot possono anche essere replicati su un sistema remoto. Sono inclusi gli snapshot antimanomissione, in cui il periodo di conservazione viene applicato e applicato sul sistema remoto. Come risultato otterrai gli stessi vantaggi di protezione dei dati delle snapshot locali, ma i dati verranno posizionati in un secondo storage array. In questo modo si garantisce che la distruzione dell'array originale non comprometta i backup.

Un secondo sistema apre anche nuove opzioni per la sicurezza amministrativa. Ad esempio, alcuni clienti NetApp segregano le credenziali di autenticazione per i sistemi di storage primario e secondario. Nessun utente amministrativo singolo ha accesso a entrambi i sistemi, il che significa che un amministratore malintenzionato non può eliminare tutte le copie dei dati.

Per ulteriori informazioni su SnapMirror, consultare la ["Documentazione ONTAP."](#)

Macchine virtuali di storage

Un sistema di storage ONTAP appena configurato è simile a un server VMware ESX appena configurato, perché nessuno di questi può supportare gli utenti fino alla creazione di una macchina virtuale. Con ONTAP viene creata una Storage Virtual Machine (SVM) che diventa l'unità di gestione dello storage più base. Ciascuna SVM dispone di risorse di storage, configurazioni di protocolli, indirizzi IP e WWN FCP. Questa è la base della multi-tenancy di ONTAP.

Ad esempio, è possibile configurare una SVM per i carichi di lavoro di produzione critici e una seconda SVM su un segmento di rete diverso per le attività di sviluppo. Quindi, è possibile limitare l'accesso alla SVM di produzione a determinati amministratori, garantendo al contempo agli sviluppatori un controllo più esteso sulle risorse storage nella SVM di sviluppo. Potrebbe anche essere necessario fornire una terza SVM ai tuoi team finanziari e delle risorse umane per memorizzare dati particolarmente critici solo per gli occhi.

Per ulteriori informazioni sulle SVM, consulta la ["Documentazione ONTAP."](#)

RBAC amministrativo

ONTAP offre un potente role-based access control (RBAC) per gli accessi amministrativi. Alcuni amministratori potrebbero aver bisogno di un accesso completo al cluster, altri invece potrebbero aver bisogno solo dell'accesso a determinate SVM. Il personale avanzato dell'helpdesk potrebbe aver bisogno di aumentare le dimensioni dei volumi. Il risultato è la possibilità di concedere agli utenti amministrativi l'accesso necessario per eseguire le proprie responsabilità lavorative, e niente di più. Inoltre, è possibile proteggere questi accessi utilizzando PKI di vari fornitori, limitare l'accesso solo alle chiavi ssh e applicare blocchi dei tentativi di accesso non riusciti.

Per ulteriori informazioni sul controllo dell'accesso amministrativo, consultare la ["Documentazione ONTAP."](#)

Autenticazione multifattore (MFA)

ONTAP e alcuni altri prodotti NetApp supportano ora l'autenticazione a più fattori (MFA) utilizzando una vasta gamma di metodi. Il risultato è un nome utente/password compromesso da solo non è un thread di sicurezza senza i dati del secondo fattore, come un FOB o un'applicazione per smartphone.

Per ulteriori informazioni sull'autenticazione multifattore (MFA), vedere ["Documentazione ONTAP."](#)

RBAC API

L'automazione richiede chiamate API, ma non tutti gli strumenti richiedono un accesso amministrativo completo. Per contribuire a proteggere i sistemi di automazione, RBAC è disponibile anche a livello di API. È possibile limitare gli account utente di automazione alle chiamate API richieste. Ad esempio, il software di monitoraggio non richiede l'accesso alle modifiche, ma solo l'accesso in lettura. I workflow che forniscono storage non hanno bisogno della capacità di eliminare lo storage.

Per ulteriori informazioni su RBAC API, consulta la ["Documentazione ONTAP."](#)

Verifica multi-admin (MAV)

L'autenticazione a più "fattori" può essere ulteriormente eseguita richiedendo l'approvazione di determinate attività da parte di due amministratori diversi, ciascuno con le proprie credenziali. Ciò include la modifica delle autorizzazioni di accesso, l'esecuzione dei comandi diagnostici e l'eliminazione dei dati.

Per ulteriori informazioni sulla verifica multi-admin (MAV), vedere ["Documentazione ONTAP."](#)

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.