



Configurare la replica sincrona con NetApp SnapMirror Active Sync e cluster Microsoft Stretch

NetApp virtualization solutions

NetApp
August 18, 2025

Sommario

- Configurare la replica sincrona con NetApp SnapMirror Active Sync e cluster Microsoft Stretch 1
 - Introduzione 1
 - Casi d'uso 1
 - Architettura della soluzione 2
 - Installa un cluster di failover Microsoft Stretch 3
 - Crea peering intercluster 5
 - Configurare Mediator con ONTAP 6
 - Configurare la protezione simmetrica attiva/attiva 8
 - Eseguire il test di convalida del failover del cluster 9
 - Riepilogo 11

Configurare la replica sincrona con NetApp SnapMirror Active Sync e cluster Microsoft Stretch

Utilizzare SnapMirror Active Sync per configurare la replica sincrona e bidirezionale tra cluster di failover Microsoft Stretch. Questa procedura include l'installazione di un cluster di failover esteso, la creazione di peering intercluster, la configurazione di un mediatore con ONTAP, l'abilitazione della protezione simmetrica attiva/attiva e l'esecuzione di test di convalida del failover del cluster.

Introduzione

A partire da ONTAP 9.15.1, SnapMirror Active Sync supporta distribuzioni attive/attive simmetriche, consentendo operazioni di I/O in lettura e scrittura da entrambe le copie di una LUN protetta con replica sincrona bidirezionale. Un cluster esteso di Windows è un'estensione della funzionalità Cluster di failover di Windows che si estende su più posizioni geografiche per garantire elevata disponibilità e ripristino di emergenza. Grazie alle applicazioni attive/attive simmetriche e in cluster SnapMirror Active Sync, come il clustering di failover di Windows, possiamo ottenere una disponibilità continua per le applicazioni aziendali critiche di Microsoft Hyper-V, ottenendo RTO e RPO pari a zero durante incidenti imprevisti. Questa soluzione offre i seguenti vantaggi:

- Nessuna perdita di dati: garantisce che i dati vengano replicati in modo sincrono, raggiungendo un Recovery Point Objective (RPO) pari a zero.
- Alta disponibilità e bilanciamento del carico: entrambi i siti possono gestire attivamente le richieste, garantendo bilanciamento del carico ed elevata disponibilità.
- Continuità aziendale: implementare una configurazione attiva/attiva simmetrica per garantire che entrambi i data center forniscano attivamente le applicazioni e possano subentrare senza problemi in caso di guasto.
- Miglioramento delle prestazioni: utilizzare una configurazione simmetrica attiva/attiva per distribuire il carico su più sistemi di archiviazione, migliorando i tempi di risposta e le prestazioni complessive del sistema.

Questo documento documenta la replica bidirezionale sincrona della tecnologia SnapMirror ActiveSync tra cluster di failover Microsoft Stretch, consentendo ai dati delle applicazioni multisito, ad esempio MSSQL e Oracle, di essere attivamente accessibili e sincronizzati su entrambi i siti. In caso di guasto, le applicazioni vengono immediatamente reindirizzate al sito attivo rimanente, senza perdita di dati né di accesso, garantendo elevata disponibilità, ripristino di emergenza e ridondanza geografica.

Casi d'uso

In caso di interruzioni come un attacco informatico, un'interruzione di corrente o un disastro naturale, un ambiente aziendale connesso a livello globale richiede un rapido ripristino dei dati delle applicazioni aziendali critiche, senza alcuna perdita di dati. Tali esigenze sono più elevate in settori quali la finanza e quelli che aderiscono a obblighi normativi quali il Regolamento generale sulla protezione dei dati (GDPR). Distribuire una configurazione attiva/attiva simmetrica per replicare i dati tra posizioni geograficamente disperse, fornendo accesso locale ai dati e garantendo la continuità in caso di interruzioni regionali.

La sincronizzazione attiva SnapMirror offre i seguenti casi d'uso:

Distribuzione dell'applicazione per oggetti con tempo di ripristino zero (RTO)

In una distribuzione di sincronizzazione attiva SnapMirror , si dispone di un cluster primario e di un cluster mirror. Una LUN nel cluster primario (L1P) ha un mirror (L1S) sul secondario; le operazioni di lettura e scrittura vengono gestite dal sito locale agli host in base alle impostazioni di Hot Proximity.

Distribuzione dell'applicazione per RTO o TAF pari a zero

Il Transparent Application Failover (TAF) si basa sul failover del percorso basato sul software MPIO host per ottenere un accesso senza interruzioni allo storage. Entrambe le copie LUN, ad esempio la copia primaria (L1P) e quella mirror (L1S), hanno la stessa identità (numero di serie) e vengono segnalate come leggibili e scrivibili dall'host.

Applicazioni in cluster

Le applicazioni in cluster, tra cui VMware vSphere Metro Storage Cluster (vMSC), Oracle RAC e Windows Failover Clustering con SQL, richiedono l'accesso simultaneo in modo che le VM possano effettuare il failover sull'altro sito senza alcun sovraccarico di prestazioni. SnapMirror ActiveSync Symmetric Active/Active fornisce I/O localmente con replica bidirezionale per soddisfare i requisiti delle applicazioni in cluster.

Scenario di disastro

Replicare in modo sincrono più volumi per un'applicazione tra siti situati in posizioni geograficamente distanti. In caso di interruzione della copia primaria, è possibile eseguire automaticamente il failover sulla copia secondaria, garantendo così la continuità aziendale per le applicazioni di primo livello.

Failover di Windows

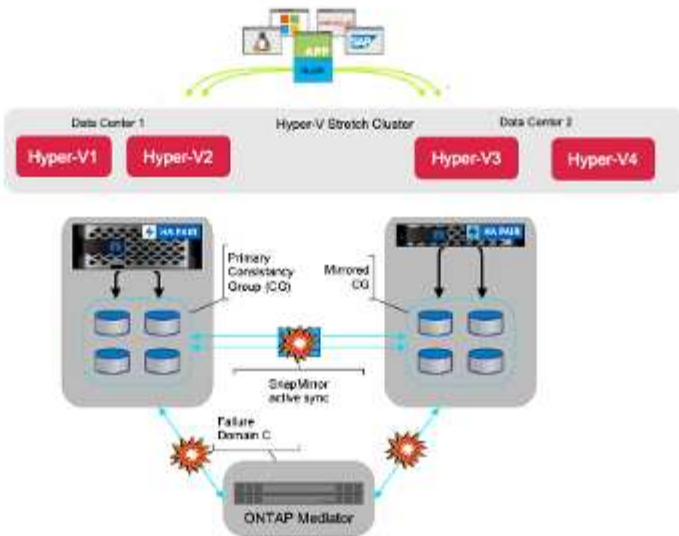
SnapMirror Active Sync offre flessibilità con granularità a livello di applicazione di facile utilizzo e failover automatico per ottenere un'elevata disponibilità dei dati e una rapida replica dei dati per le applicazioni aziendali critiche come Oracle, Microsoft SQL Server e così via, sia in ambienti virtuali che fisici.

Architettura della soluzione

Il cluster Microsoft Stretch ha due nodi Hyper-V su ciascun sito. Questi due nodi condividono lo storage NetApp e utilizzano SnapMirror ActiveSync Symmetric Active-Active per replicare i volumi tra i due siti. Un gruppo di coerenza garantisce che tutti i volumi di un set di dati vengano messi in stato di quiescenza e quindi acquisiti esattamente nello stesso momento. Ciò fornisce un punto di ripristino coerente con i dati su tutti i volumi che supportano il set di dati. Il mediatore ONTAP riceve informazioni sullo stato di salute dei cluster e dei nodi ONTAP peer, orchestrando i due e determinando se ciascun nodo/cluster è integro e in esecuzione.

Componenti della soluzione:

- Due sistemi di storage NetApp ONTAP 9.15.1: primo e secondo dominio di errore
- Una VM Redhat 8.7 per il mediatore ONTAP
- Tre cluster di failover Hyper-V su Windows 2022:
 - sito1, sito 2 per le applicazioni
 - sito 3 per mediatore
- VM su Hyper-V: Microsoft Domain Controller, istanza del cluster di failover MSSQL Always On, mediatore ONTAP



Installa un cluster di failover Microsoft Stretch

È possibile utilizzare Windows Admin Center, PowerShell o la console di Server Manager per installare la funzionalità Failover Clustering e i cmdlet PowerShell associati. Per maggiori dettagli sui prerequisiti e sui passaggi, consultare la sezione Creare un cluster di failover.

Ecco una guida dettagliata per configurare un Windows Stretch Cluster:

1. Installa Windows 2022 su tutti e quattro i server hyperv1, hyperv2, hyperv3 e hyperv4
2. Unire tutti e quattro i server allo stesso dominio Active Directory: hyperv.local.
3. Installare le funzionalità di Windows failover-clustering, Hyper-V, Hyper-V_Powershell e MPIO su ciascun server.

```
Install-WindowsFeature -Name "Failover-Clustering", "Hyper-V", "Hyper-V-Powershell", "MPIO" -IncludeManagementTools
```

4. Configura MPIO, aggiungi il supporto per i dispositivi iSCSI.



5. Sugli storage ONTAP del sito 1 e del sito 2, creare due LUN iSCSI (SQLdata e SQLlog) e mapparli al gruppo iqn dei server Windows. Utilizzare l'iniziatore software iSCSI Microsoft per connettere i LUN. Per

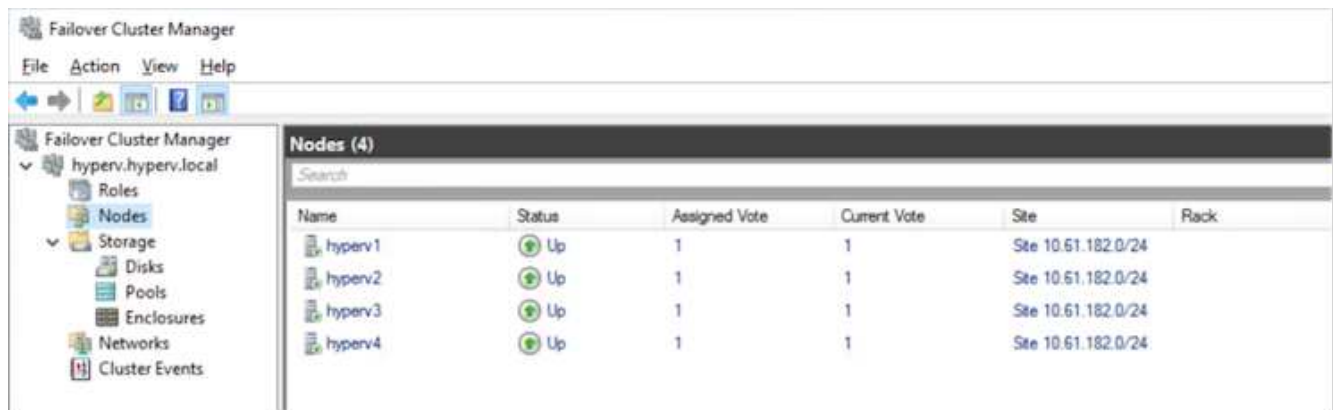
maggiori dettagli, controlla "[Configurazione iSCSI per Windows](#)".

6. Eseguire il report di convalida del cluster per individuare eventuali errori o avvisi.

```
Test-Cluster -Node hyperv1, hyperv2, hyperv3, hyperv4
```

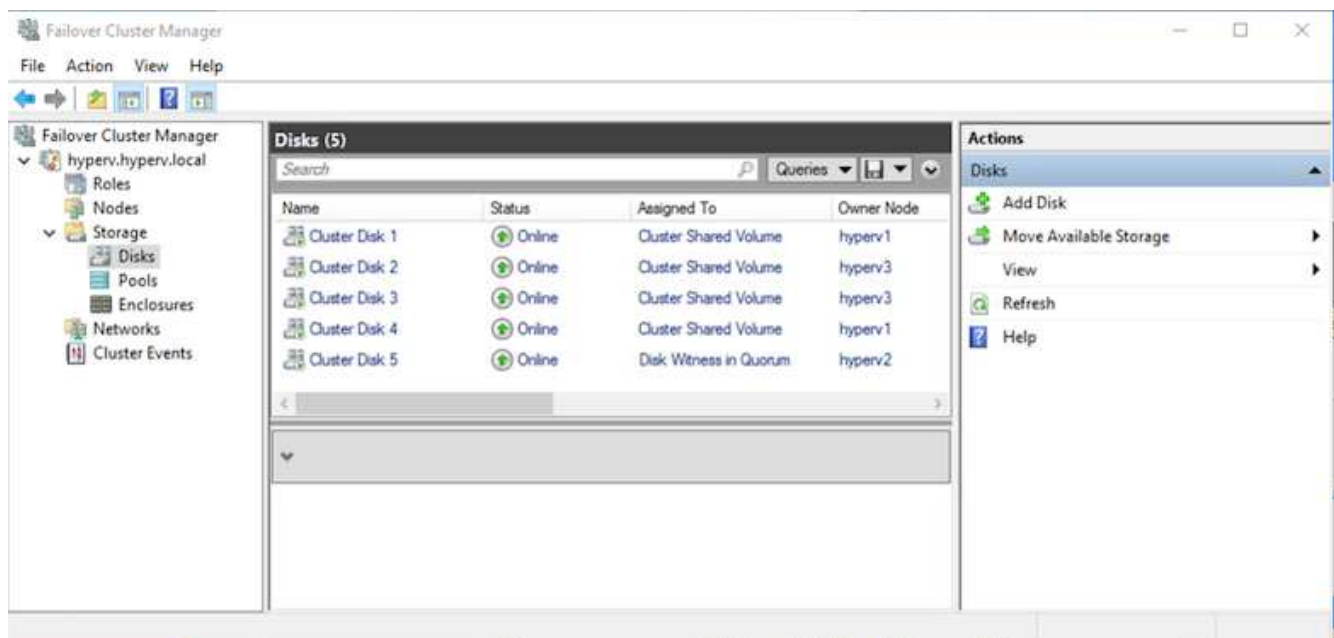
7. Creare un cluster di failover, assegnare un indirizzo IP statico,

```
New-Cluster -Name <clustername> -Node hyperv1, hyperv2, hyperv3, hyperv4, StaticAddress <IPaddress>
```



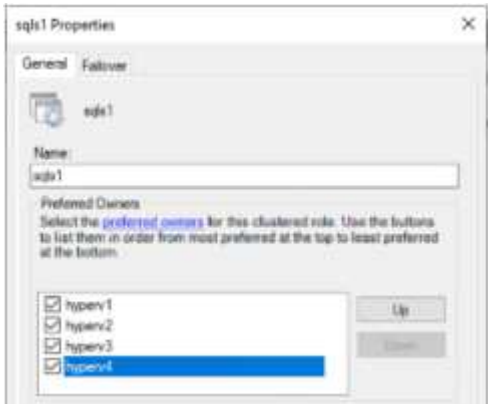
8. Aggiungere gli archivi iSCSI mappati al cluster di failover.
9. Configurare un witness per il quorum, fare clic con il pulsante destro del mouse sul cluster → Altre azioni → Configura impostazioni quorum cluster, scegliere witness disco.

Il diagramma seguente mostra quattro LUN condivise in cluster: due siti sqldata e sqllog e un disco witness in quorum.



Istanza del cluster di failover sempre attiva

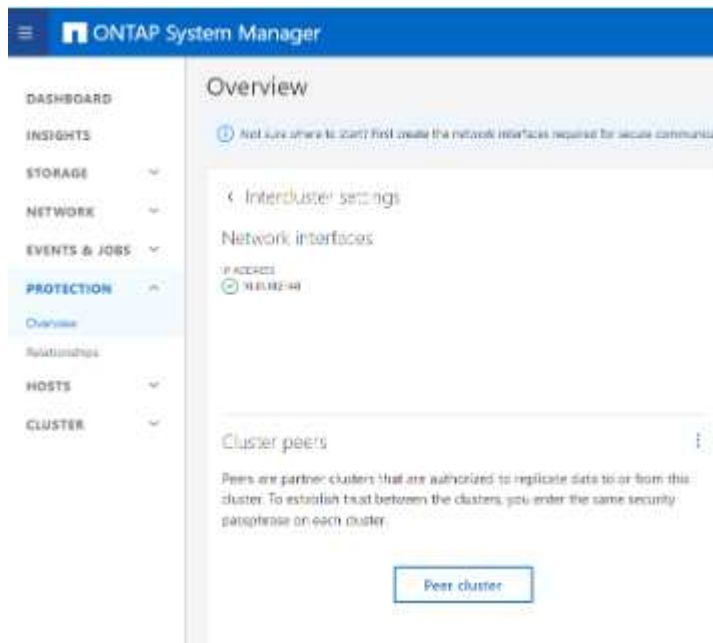
Un'istanza del cluster di failover Always On (FCI) è un'istanza di SQL Server installata su nodi con archiviazione su disco condivisa SAN in un WSFC. Durante un failover, il servizio WSFC trasferisce la proprietà delle risorse dell'istanza a un nodo di failover designato. L'istanza di SQL Server viene quindi riavviata sul nodo di failover e i database vengono ripristinati come di consueto. Per maggiori dettagli sulla configurazione, consultare Windows Failover Clustering con SQL. Creare due VM Hyper-V SQL FCI su ciascun sito e impostare la priorità. Utilizzare hyperv1 e hyperv2 come proprietari preferiti per le VM del sito 1 e hyperv3 e hyperv4 come proprietari preferiti per le VM del sito 2.



Crea peering intercluster

È necessario creare relazioni peer tra cluster di origine e di destinazione prima di poter replicare copie Snapshot tramite SnapMirror.

1. Aggiungere interfacce di rete intercluster su entrambi i cluster



2. È possibile utilizzare il comando cluster peer create per creare una relazione peer tra un cluster locale e uno remoto. Dopo aver creato la relazione peer, è possibile eseguire cluster peer create sul cluster remoto per autenticarlo sul cluster locale.

Configurare Mediator con ONTAP

Il mediatore ONTAP riceve informazioni sullo stato di salute dei cluster e dei nodi ONTAP peering, orchestrando i due e determinando se ciascun nodo/cluster è integro e in esecuzione. SM-as consente di replicare i dati sulla destinazione non appena vengono scritti sul volume di origine. Il mediatore deve essere distribuito nel terzo dominio di errore. Prerequisiti

- Specifiche HW: 8 GB di RAM, 2 CPU da 2 GHz, rete da 1 Gb (<125 ms RTT)
- Installato il sistema operativo Red Hat 8.7, controlla ["Versione di ONTAP Mediator e versione Linux supportata"](#) .
- Configurare l'host Linux Mediator: configurazione di rete e porte firewall 31784 e 3260
- Installa il pacchetto yum-utils
- ["Registra una chiave di sicurezza quando UEFI Secure Boot è abilitato"](#)

Passi

1. Scaricare il pacchetto di installazione di Mediator da ["Pagina di download ONTAP Mediator"](#) .
2. Verificare la firma del codice del mediatore ONTAP .
3. Eseguire il programma di installazione e rispondere alle richieste come richiesto:

```
./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

4. Se è abilitato l'avvio protetto, è necessario eseguire ulteriori passaggi per registrare la chiave di sicurezza dopo l'installazione:
 - a. Seguire le istruzioni nel file README per firmare il modulo kernel SCST:


```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.m  
odule-signing
```

b. Individuare le chiavi richieste:

```
/opt/netapp/lib/ontap mediator/ontap mediator/SCST mod keys
```

5. Verificare l'installazione

a. Confermare i processi:

```
systemctl status ontap mediator mediator-scst
```

[illegible]

b. Confermare le porte utilizzate dal servizio ONTAP Mediator:

```
[root@mediator2 server_config]# netstat -anlt | grep -E '3260|31784'
```

tcp	0	0	0.0.0.0:3260	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:31784	0.0.0.0:*	LISTEN
tcp	0	0	10.61.182.163:31784	10.61.182.148:26429	ESTABLISHED
tcp	0	0	10.61.182.163:31784	10.61.182.148:24546	FIN_WAIT2
tcp6	0	0	:::3260	:::*	LISTEN

6. Inizializza ONTAP Mediator per SnapMirror ActiveSync utilizzando certificati autofirmati

a. Trovare il certificato CA di ONTAP Mediator nel percorso di installazione del software VM/host Linux
ONTAP Mediator `cd /opt/netapp/lib/ontap mediator/ontap mediator/server config.`

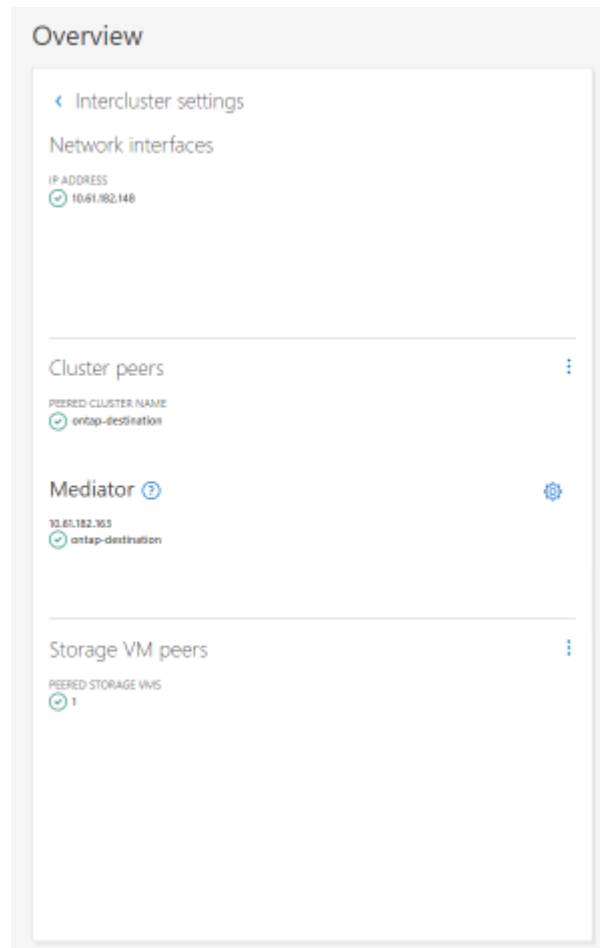
b. Aggiungere il certificato CA del mediatore ONTAP a un cluster ONTAP.

```
security certificate install -type server-ca -vserver <vserver name>
```

7. Aggiungere il mediatore, andare su Gestione sistema, proteggere>Panoramica>mediatore, immettere

l'indirizzo IP del mediatore, il nome utente (l'utente API predefinito è mediatoradmin), la password e la porta 31784.

Il diagramma seguente mostra come sono configurati l'interfaccia di rete intercluster, i peer del cluster, il mediatore e il peer SVM.



Configurare la protezione simmetrica attiva/attiva

I gruppi di coerenza facilitano la gestione del carico di lavoro delle applicazioni, fornendo policy di protezione locali e remote facilmente configurabili e copie snapshot simultanee, coerenti con gli arresti anomali o con l'applicazione, di una raccolta di volumi in un dato momento. Per maggiori dettagli fare riferimento a ["panoramica del gruppo di coerenza"](#) . Per questa configurazione utilizziamo una configurazione uniforme.

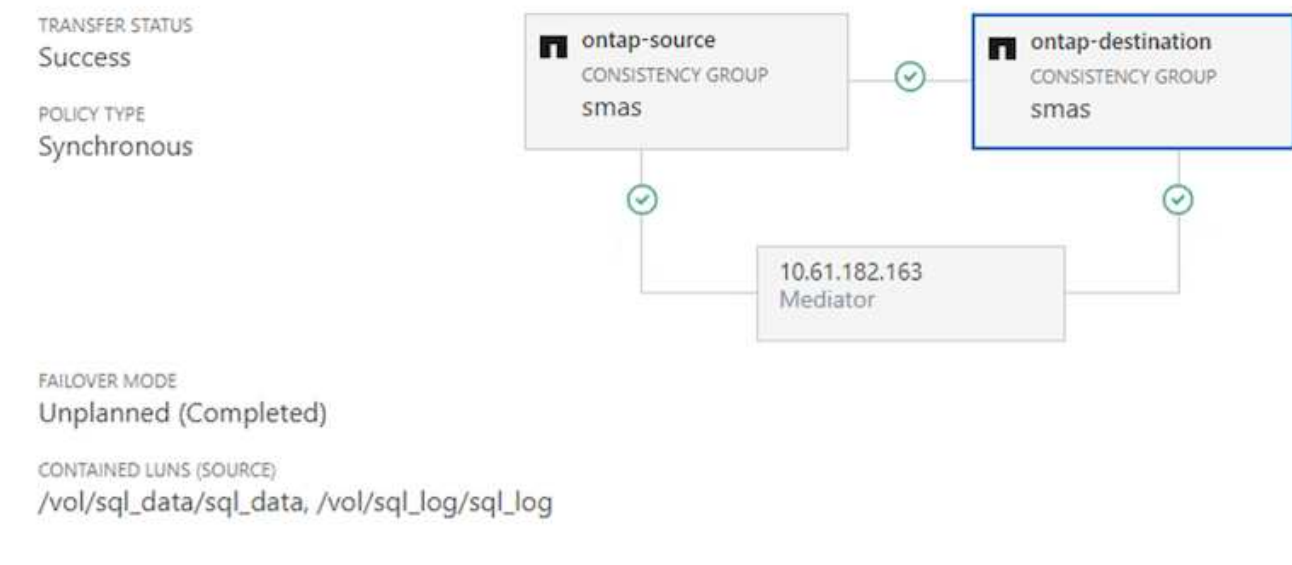
Passaggi per una configurazione uniforme

1. Quando si crea il gruppo di coerenza, specificare gli iniziatori host per creare gli igroup.
2. Selezionare la casella di controllo per abilitare SnapMirror , quindi scegliere il criterio AutomatedFailoverDuplex.
3. Nella finestra di dialogo visualizzata, seleziona la casella di controllo Replica gruppi iniziatori per replicare gli igroup. In Modifica impostazioni prossimali, imposta le SVM prossimali per i tuoi host.

Proximity settings	
Initiator	Initiator in proximity to
Initiator group: hyperv Mapped LUNs: 2	
iqn.1991-05.com:microsoft:hyperv2.hyperv.local	Destination
iqn.1991-05.com:microsoft:hyperv3.hyperv.local	Source
iqn.1991-05.com:microsoft:hyperv1.hyperv.local	Destination
iqn.1991-05.com:microsoft:hyperv4.hyperv.local	Source

4. Seleziona Salva

Il rapporto di protezione viene stabilito tra la sorgente e la destinazione.



Eseguire il test di convalida del failover del cluster

Si consiglia di eseguire test di failover pianificati per verificare la convalida del cluster, dei database SQL o di qualsiasi software in cluster su entrambi i siti: il sito primario o mirror deve continuare a essere accessibile durante i test.

I requisiti del cluster di failover Hyper-V includono:

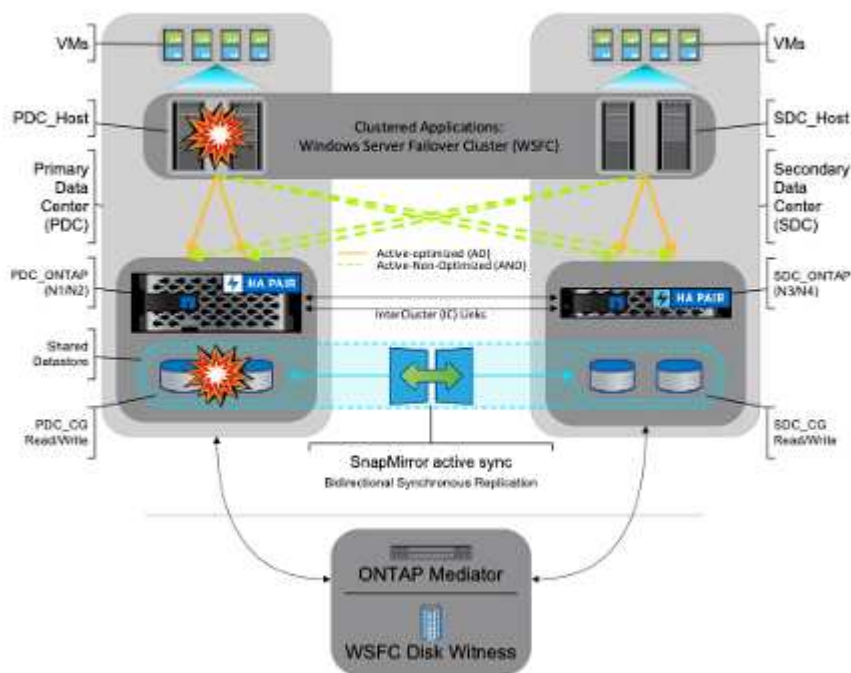
- La relazione di sincronizzazione attiva SnapMirror deve essere sincronizzata.
- Non è possibile avviare un failover pianificato quando è in corso un'operazione non distruttiva. Le operazioni non disruptive includono spostamenti di volumi, rilocalizzazioni aggregate e failover di storage.
- Il mediatore ONTAP deve essere configurato, connesso e in quorum.
- Almeno due nodi del cluster Hyper-V su ciascun sito con processori CPU appartengono alla stessa famiglia di CPU per ottimizzare il processo di migrazione delle VM. Le CPU devono essere CPU con

supporto per la virtualizzazione assistita da hardware e la prevenzione dell'esecuzione dei dati (DEP) basata su hardware.

- Per garantire la resilienza, i nodi del cluster Hyper-V devono essere gli stessi membri del dominio Active Directory.
- I nodi del cluster Hyper-V e i nodi di storage NetApp devono essere connessi tramite reti ridondanti per evitare un singolo punto di errore.
- Archiviazione condivisa, a cui possono accedere tutti i nodi del cluster tramite protocollo iSCSI, Fibre Channel o SMB 3.0.

Scenari di prova

Esistono molti modi per attivare un failover su un host, un archivio o una rete.



Nodo o sito Hyper-V non riuscito

- Guasto del nodo Un nodo del cluster di failover può assumere il carico di lavoro di un nodo guasto, un processo noto come failover. Azione: spegnere un nodo Hyper-V. Risultato previsto: l'altro nodo nel cluster assumerà il carico di lavoro. Le VM verranno migrate all'altro nodo.
- Errore di un sito È anche possibile interrompere l'intero sito e attivare il failover del sito primario sul sito mirror: Azione: disattivare entrambi i nodi Hyper-V su un sito. Risultato previsto: le VM sul sito primario migreranno al cluster Hyper-V del sito mirror perché SnapMirror ActiveSync simmetrico attivo/attivo fornisce l'I/O localmente con replica bidirezionale, senza impatto sul carico di lavoro con RPO e RTO pari a zero.

Errore di archiviazione su un sito

- Arrestare una SVM sul sito primario Azione: arrestare la SVM iSCSI Risultati previsti: il cluster primario Hyper-V si è già connesso al sito mirrorato e con SnapMirror ActiveSync simmetrico attivo/attivo nessun impatto sul carico di lavoro con RPO e RTO pari a zero.

Criteri di successo

Durante i test, osservare quanto segue:

- Osservare il comportamento del cluster e assicurarsi che i servizi vengano trasferiti ai nodi rimanenti.
- Verificare eventuali errori o interruzioni del servizio.
- Assicurarsi che il cluster sia in grado di gestire i guasti di archiviazione e di continuare a funzionare.
- Verificare che i dati del database rimangano accessibili e che i servizi continuino a funzionare.
- Verificare che l'integrità dei dati del database venga mantenuta.
- Verificare che applicazioni specifiche possano eseguire il failover su un altro nodo senza alcun impatto sull'utente.
- Verificare che il cluster sia in grado di bilanciare il carico e mantenere le prestazioni durante e dopo un failover.

Riepilogo

La sincronizzazione attiva SnapMirror può aiutare i dati delle applicazioni multi-sito, ad esempio MSSQL e Oracle, a essere attivamente accessibili e sincronizzati su entrambi i siti. In caso di errore, le applicazioni vengono immediatamente reindirizzate al sito attivo rimanente, senza perdita di dati né di accesso.

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.