Configurazione SMB per Microsoft Hyper-V e SQL Server

ONTAP 9

NetApp
January 08, 2026

Sommario

Configurazione SMB per Microsoft Hyper-V e SQL Server

Panoramica della configurazione SMB per Microsoft Hyper-V e SQL Server

Le funzionalità di ONTAP consentono di eseguire operazioni senza interruzioni per due applicazioni Microsoft tramite il protocollo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Utilizzare queste procedure se si desidera implementare operazioni SMB senza interruzioni nei seguenti casi:

- È stato configurato l'accesso al file del protocollo SMB di base.
- Si desidera abilitare le condivisioni di file SMB 3.0 o versioni successive che risiedono in SVM per memorizzare i seguenti oggetti:
  - File di macchine virtuali Hyper-V.
  - Database di sistema di SQL Server

Informazioni correlate

Per ulteriori informazioni sulla tecnologia ONTAP e sull'interazione con i servizi esterni, consultare i seguenti report tecnici (TR): "Report tecnico NetApp 4172: Best practice Microsoft Hyper-V su SMB 3.0 con ONTAP" "Report tecnico NetApp 4369: Best practice per Microsoft SQL Server e SnapManager 7.2 per SQL Server con Clustered Data ONTAP"

Configurare ONTAP per le soluzioni Microsoft Hyper-V e SQL Server su SMB

È possibile utilizzare le condivisioni di file SMB 3.0 e versioni successive disponibili in modo continuo per memorizzare i file delle macchine virtuali Hyper-V o i database di sistema SQL Server e i database degli utenti su volumi residenti in SVM, fornendo al contempo operazioni senza interruzioni (NDOS) per eventi pianificati e non pianificati.

Microsoft Hyper-V su SMB

Per creare una soluzione Hyper-V su SMB, devi prima configurare ONTAP per fornire servizi di storage per i server Microsoft Hyper-V. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster), i server Hyper-V, le connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS e, facoltativamente, i servizi di backup per proteggere i file delle macchine virtuali memorizzati nei volumi SVM.

I server Hyper-V devono essere configurati su Windows 2012 Server o versioni successive. Sono supportate le configurazioni dei server Hyper-V in cluster e standalone.

- Per informazioni sulla creazione di cluster Microsoft e server Hyper-V, visitare il sito Web Microsoft.
- SnapManager per Hyper-V è un'applicazione basata su host che facilita la creazione di servizi di backup rapidi e basati su snapshot, progettati per l'integrazione con le configurazioni Hyper-V su SMB.

Per informazioni sull'utilizzo di SnapManager con configurazioni Hyper-V su SMB, consultare la _Guida all'installazione e all'amministrazione di SnapManager per Hyper-V.

Microsoft SQL Server su SMB

Per creare una soluzione SQL Server su SMB, è necessario prima configurare ONTAP per fornire servizi di storage per l'applicazione Microsoft SQL Server. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster). Installare e configurare SQL Server sui server Windows e creare connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS. Facoltativamente, è possibile configurare i servizi di backup per proteggere i file di database memorizzati nei volumi SVM.

SQL Server deve essere installato e configurato su Windows 2012 Server o versione successiva. Sono supportate sia le configurazioni standalone che quelle in cluster.

- Per informazioni sulla creazione di cluster Microsoft e sull'installazione e configurazione di SQL Server, visitare il sito Web Microsoft.
- Il plug-in SnapCenter per Microsoft SQL Server è un'applicazione basata su host che facilita i servizi di backup rapidi e basati su snapshot, progettata per l'integrazione con le configurazioni SQL Server su SMB.

  Per informazioni sull'utilizzo del plug-in SnapCenter per Microsoft SQL Server, vedere "Plug-in SnapCenter per Microsoft SQL Server" documento.

Operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Che cosa significa operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB si riferiscono alla combinazione di funzionalità che consentono ai server di applicazioni e alle macchine virtuali o ai database contenuti di rimanere online e di garantire una disponibilità continua durante molte attività amministrative. Ciò include downtime pianificati e non pianificati dell'infrastruttura storage.

Le operazioni senza interruzioni supportate per i server di applicazioni su SMB includono:

- Acquisizione e giveback pianificati
- Takeover non pianificato
- Eseguire l'upgrade
- Delocalizzazione pianificata degli aggregati (ARL)
- Migrazione LIF e failover
- Spostamento pianificato del volume

Protocolli che consentono operazioni senza interruzioni su SMB

Insieme al rilascio di SMB 3.0, Microsoft ha rilasciato nuovi protocolli per fornire le funzionalità necessarie per supportare operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

ONTAP utilizza questi protocolli quando fornisce operazioni senza interruzioni per server di applicazioni su PMI:

- SMB 3.0
- Testimone

Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Prima di configurare la soluzione Hyper-V o SQL Server su SMB, è necessario comprendere alcuni concetti relativi alle operazioni senza interruzioni (NDOS).

- **Quota a disponibilità continua**

  Una condivisione SMB 3.0 con la proprietà di condivisione continuamente disponibile impostata. I client che si connettono attraverso condivisioni continuamente disponibili possono sopravvivere a eventi di interruzione come takeover, giveback e trasferimento aggregato.

- Nodo *

  Un singolo controller che è membro di un cluster. Per distinguere i due nodi di una coppia SFO, un nodo viene talvolta chiamato *nodo locale* e l'altro nodo viene talvolta chiamato *nodo partner* o *nodo remoto*. Il principale proprietario dello storage è il nodo locale. Il proprietario secondario, che assume il controllo dello storage in caso di guasto del proprietario primario, è il nodo partner. Ciascun nodo è il principale proprietario dello storage e il proprietario secondario dello storage del partner.

- **Trasferimento aggregato senza interruzioni**

  Possibilità di spostare un aggregato tra nodi partner all'interno di una coppia SFO in un cluster senza interrompere le applicazioni client.

- **Failover senza interruzioni**

  Vedi *Takeover*.

- **Migrazione LIF senza interruzioni**

  La possibilità di eseguire una migrazione LIF senza interrompere le applicazioni client connesse al cluster attraverso tale LIF. Per le connessioni SMB, ciò è possibile solo per i client che si connettono utilizzando SMB 2.0 o versioni successive.

- **Operazioni senza interruzioni**

  La capacità di eseguire importanti operazioni di gestione e aggiornamento di ONTAP e di resistere agli errori dei nodi senza interrompere le applicazioni client. Questo termine si riferisce alla raccolta di funzionalità di Takeover senza interruzioni, upgrade senza interruzioni e migrazione senza interruzioni nel loro complesso.

- **Upgrade senza interruzioni**

  Possibilità di aggiornare l'hardware o il software del nodo senza interruzioni dell'applicazione.

- **Spostamento del volume senza interruzioni**

Possibilità di spostare liberamente un volume nel cluster senza interrompere le applicazioni che utilizzano il volume. Per le connessioni SMB, tutte le versioni di SMB supportano spostamenti di volume senza interruzioni.

- **Handle persistenti**

  Proprietà di SMB 3.0 che consente alle connessioni continuamente disponibili di riconnettersi in modo trasparente al server CIFS in caso di disconnessione. In modo analogo ai gestori a lunga durata, i gestori persistenti vengono mantenuti dal server CIFS per un periodo di tempo successivo alla perdita della comunicazione con il client di connessione. Tuttavia, le maniglie persistenti hanno una maggiore resilienza rispetto alle maniglie resistenti. Oltre a dare al client la possibilità di recuperare l'handle in una finestra di 60 secondi dopo la riconnessione, il server CIFS nega l'accesso a tutti gli altri client che richiedono l'accesso al file durante la finestra di 60 secondi.

  Le informazioni sugli handle persistenti vengono mirrorate sullo storage persistente del partner SFO, che consente ai client con handle persistenti disconnessi di recuperare gli handle durevoli dopo un evento in cui il partner SFO assume la proprietà dello storage del nodo. Oltre a fornire operazioni senza interruzioni in caso di spostamenti LIF (che supportano la gestione durevole), le maniglie persistenti forniscono operazioni senza interruzioni per il takeover, il giveback e il trasferimento di aggregati.

- **Giveback SFO**

  Restituzione degli aggregati nelle sedi domestiche durante il ripristino da un evento di Takeover.

- **Coppia SFO**

  Coppia di nodi i cui controller sono configurati per fornire dati l'uno per l'altro se uno dei due nodi smette di funzionare. A seconda del modello di sistema, entrambi i controller possono trovarsi in un unico chassis o in uno chassis separato. Nota come coppia ha in un cluster a due nodi.

- **Takeover**

  Il processo mediante il quale il partner assume il controllo dello storage in caso di guasto del proprietario principale dello storage. Nel contesto di SFO, il failover e il takeover sono sinonimi.

In che modo la funzionalità SMB 3.0 supporta operazioni senza interruzioni sulle condivisioni SMB

SMB 3.0 offre funzionalità cruciali che consentono il supporto per operazioni senza interruzioni per Hyper-V e SQL Server su condivisioni SMB. Ciò include `continuously-available` Condividere la proprietà e un tipo di handle di file noto come *handle persistente* che consentono ai client SMB di recuperare lo stato di apertura del file e ristabilire in modo trasparente le connessioni SMB.

Gli handle persistenti possono essere concessi ai client SMB 3.0 che si connettono a una condivisione con il set di proprietà di condivisione continuamente disponibile. Se la sessione SMB viene disconnessa, il server CIFS conserva le informazioni sullo stato di handle persistente. Il server CIFS blocca le altre richieste client durante il periodo di 60 secondi in cui il client può riconnettersi, consentendo così al client con l'handle persistente di recuperare l'handle dopo una disconnessione dalla rete. I client con handle persistenti possono riconnettersi utilizzando una delle LIF di dati sulla macchina virtuale di storage (SVM), riconnettendosi attraverso lo stesso LIF o attraverso un LIF diverso.

Il trasferimento, il takeover e il giveback degli aggregati avvengono tra coppie SFO. Per gestire senza problemi

la disconnessione e la riconnessione delle sessioni con file con handle persistenti, il nodo partner conserva una copia di tutte le informazioni persistenti sul blocco degli handle. Sia che l'evento sia pianificato o non pianificato, il partner SFO può gestire senza interruzioni le riconnesse persistenti dell'handle. Con questa nuova funzionalità, le connessioni SMB 3.0 al server CIFS possono eseguire il failover trasparente e senza interruzioni su un altro LIF di dati assegnato a SVM in eventi che tradizionalmente hanno subito interruzioni.

Sebbene l'utilizzo di handle persistenti consenta al server CIFS di eseguire il failover in modo trasparente sulle connessioni SMB 3.0, se un errore causa il failover dell'applicazione Hyper-V su un altro nodo nel cluster di Windows Server, il client non ha alcun modo per recuperare gli handle di file di questi handle disconnessi. In questo scenario, gli handle di file in stato disconnesso possono potenzialmente bloccare l'accesso all'applicazione Hyper-V se viene riavviata su un nodo diverso. "failover Clustering" fa parte di SMB 3.0 che risolve questo scenario fornendo un meccanismo per invalidare handle obsoleti e in conflitto. Grazie a questo meccanismo, un cluster Hyper-V può essere ripristinato rapidamente in caso di guasto dei nodi del cluster Hyper-V.

Cosa fa il protocollo Witness per migliorare il failover trasparente

Il protocollo Witness offre funzionalità di failover client avanzate per le condivisioni SMB 3.0 a disponibilità continua (condivisioni CA). La funzione Witness facilita un failover più rapido perché evita il periodo di failover di LIF. Notifica agli application server quando un nodo non è disponibile senza dover attendere il timeout della connessione SMB 3.0.

Il failover è perfetto, con le applicazioni in esecuzione sul client che non sono a conoscenza del failover. Se il server di controllo del mirroring non è disponibile, le operazioni di failover continuano a essere eseguite correttamente, ma il failover senza server di controllo del mirroring è meno efficiente.

Il failover avanzato di Witness è possibile quando vengono soddisfatti i seguenti requisiti:

- Può essere utilizzato solo con server CIFS con funzionalità SMB 3.0 e SMB 3.0 abilitati.
- Le condivisioni devono utilizzare SMB 3.0 con la proprietà di condivisione a disponibilità continua impostata.
- Il partner SFO del nodo a cui sono connessi i server applicazioni deve avere almeno una LIF di dati operativi assegnata alla macchina virtuale di storage (SVM) che ospita i dati per i server applicazioni.

> Il protocollo Witness opera tra coppie SFO. Poiché i LIF possono migrare a qualsiasi nodo all'interno del cluster, qualsiasi nodo potrebbe dover essere il testimone per il partner SFO. Il protocollo Witness non è in grado di fornire un failover rapido delle connessioni SMB su un dato nodo se la SVM che ospita i dati per gli application server non dispone di una LIF di dati attiva sul nodo partner. Pertanto, ogni nodo del cluster deve disporre di almeno una LIF di dati per ogni SVM che ospita una di queste configurazioni.

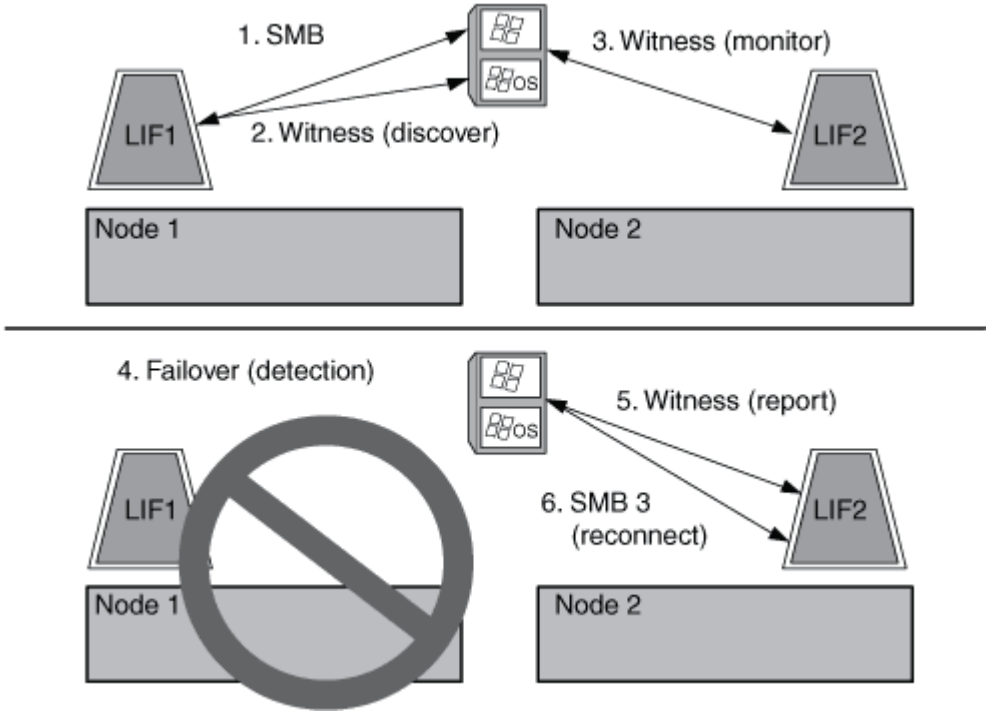
- I server applicazioni devono connettersi al server CIFS utilizzando il nome del server CIFS memorizzato in DNS invece di utilizzare singoli indirizzi IP LIF.

Funzionamento del protocollo Witness

ONTAP implementa il protocollo Witness utilizzando il partner SFO di un nodo come Witness. In caso di guasto, il partner rileva rapidamente il guasto e notifica il client SMB.

Il protocollo Witness offre un failover avanzato utilizzando il seguente processo:

1. Quando l'application server stabilisce una connessione SMB continuamente disponibile al Node1, il server CIFS informa l'application server che il server di controllo è disponibile.
2. Il server applicazioni richiede gli indirizzi IP del server di controllo del mirroring dal Node1 e riceve un elenco di indirizzi IP LIF dei dati Node2 (il partner SFO) assegnati alla macchina virtuale di storage (SVM).
3. Il server applicazioni sceglie uno degli indirizzi IP, crea una connessione testimone a Node2 e registra per ricevere una notifica se la connessione continuamente disponibile su Node1 deve spostarsi.
4. Se si verifica un evento di failover su Node1, Witness facilita gli eventi di failover, ma non è coinvolto nel giveback.
5. Il server di controllo del mirroring rileva l'evento di failover e notifica al server applicazioni tramite la connessione di controllo del mirroring che la connessione SMB deve spostarsi su Node2.
6. L'application server sposta la sessione SMB su Node2 e ripristina la connessione senza interrompere l'accesso al client.



Backup basati su condivisione con Remote VSS

Backup basati su condivisione con panoramica di Remote VSS

È possibile utilizzare Remote VSS per eseguire backup basati su condivisioni di file di macchine virtuali Hyper-V memorizzati su un server CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) è un'estensione dell'infrastruttura Microsoft VSS esistente. Con Remote VSS, Microsoft ha esteso l'infrastruttura VSS per supportare la copia shadow delle condivisioni SMB. Inoltre, le applicazioni server come Hyper-V possono memorizzare i file VHD nelle condivisioni di file SMB. Con queste estensioni, è possibile creare copie shadow coerenti con le applicazioni per le macchine virtuali che memorizzano i file di dati e di configurazione su condivisioni.

Concetti VSS remoti

È necessario conoscere alcuni concetti necessari per comprendere in che modo i servizi di backup con configurazioni Hyper-V su SMB utilizzano il servizio Remote VSS (Volume Shadow Copy Service).

- **VSS (Volume Shadow Copy Service)**

  Tecnologia Microsoft utilizzata per eseguire copie di backup o snapshot di dati su un volume specifico in un determinato momento. Il sistema VSS coordina tra server di dati, applicazioni di backup e software di gestione dello storage per supportare la creazione e la gestione di backup coerenti.

- **VSS remoto (Remote Volume Shadow Copy Service)**

  Tecnologia Microsoft utilizzata per eseguire copie di backup basate su condivisione dei dati in uno stato coerente con i dati in un momento specifico in cui si accede ai dati tramite le condivisioni SMB 3.0. Noto anche come *Volume Shadow Copy Service*.

- **Copia shadow**

  Un insieme duplicato di dati contenuti nella condivisione in un istante di tempo ben definito. Le copie shadow vengono utilizzate per creare backup point-in-time coerenti dei dati, consentendo al sistema o alle applicazioni di continuare ad aggiornare i dati sui volumi originali.

- **Set di copie shadow**

  Una raccolta di una o più copie shadow, con ciascuna copia shadow corrispondente a una condivisione. Le copie shadow all'interno di un set di copie shadow rappresentano tutte le condivisioni di cui è necessario eseguire il backup nella stessa operazione. Il client VSS nell'applicazione abilitata per VSS identifica le copie shadow da includere nel set.

- **Recupero automatico del set di copie shadow**

  Parte del processo di backup per le applicazioni di backup remote abilitate per VSS in cui la directory di replica contenente le copie shadow viene resa coerente point-in-time. All'inizio del backup, il client VSS sull'applicazione attiva l'applicazione per prendere punti di controllo software sui dati pianificati per il backup (i file della macchina virtuale nel caso di Hyper-V). Il client VSS consente quindi alle applicazioni di continuare. Una volta creato il set di copie shadow, Remote VSS rende il set di copie shadow scrivibile ed espone la copia scrivibile alle applicazioni. L'applicazione prepara il set di copie shadow per il backup eseguendo un ripristino automatico utilizzando il checkpoint del software preso in precedenza. Il ripristino automatico porta le copie shadow in uno stato coerente srotolando le modifiche apportate ai file e alle directory dalla creazione del checkpoint. Il ripristino automatico è un passaggio opzionale per i backup abilitati per VSS.

- **ID copia shadow**

  GUID che identifica in modo univoco una copia shadow.

- **ID set copia shadow**

  GUID che identifica in modo univoco una raccolta di ID di copia shadow sullo stesso server.

- **SnapManager per Hyper-V**

  Il software che automatizza e semplifica le operazioni di backup e ripristino per Microsoft Windows Server

2012 Hyper-V. SnapManager per Hyper-V utilizza VSS remoto con recovery automatico per eseguire il backup dei file Hyper-V sulle condivisioni SMB.

Informazioni correlate

Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Backup basati su condivisione con Remote VSS

Esempio di struttura di directory utilizzata da Remote VSS

Il VSS remoto attraversa la struttura di directory che memorizza i file delle macchine virtuali Hyper-V durante la creazione di copie shadow. È importante capire quale sia la struttura di directory appropriata, in modo da poter creare correttamente i backup dei file delle macchine virtuali.

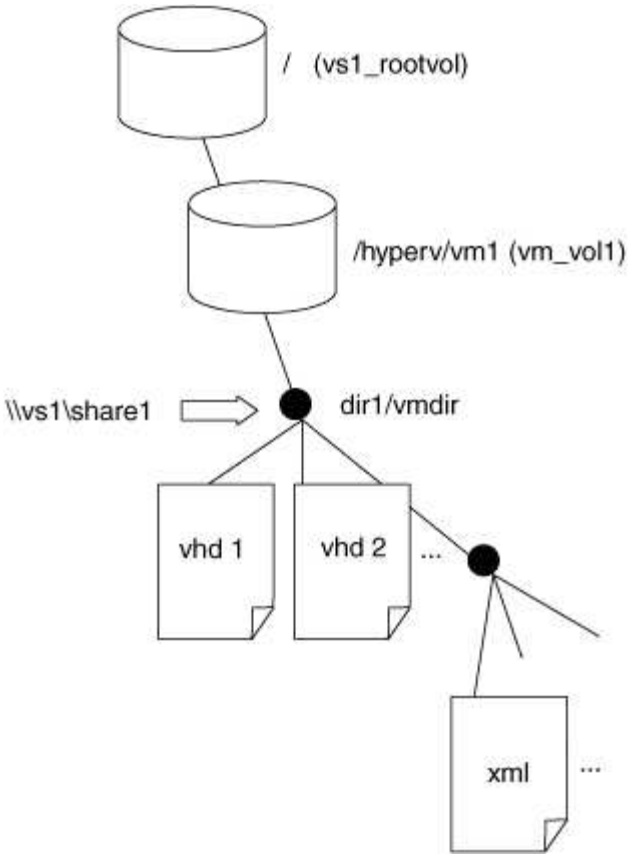
Una struttura di directory supportata per la creazione di copie shadow è conforme ai seguenti requisiti:

- Solo le directory e i file regolari sono presenti all'interno della struttura di directory utilizzata per memorizzare i file delle macchine virtuali.

  La struttura di directory non contiene giunzioni, collegamenti o file non regolari.

- Tutti i file di una macchina virtuale risiedono all'interno di una singola condivisione.
- La struttura di directory utilizzata per memorizzare i file delle macchine virtuali non supera la profondità configurata della directory di copia shadow.
- La directory principale della condivisione contiene solo i file o le directory delle macchine virtuali.

Nella seguente illustrazione, il volume denominato vm_vol1 viene creato con un punto di giunzione in `/hyperv/vm1` Su storage virtual machine (SVM) vs1. Le sottodirectory che contengono i file della macchina virtuale vengono create sotto il punto di giunzione. Ai file della macchina virtuale del server Hyper-V si accede tramite share1 che ha il percorso `/hyperv/vm1/dir1/vmdir`. Il servizio di copia shadow crea copie shadow di tutti i file della macchina virtuale contenuti nella struttura di directory sotto share1 (fino alla profondità configurata della directory di copia shadow).



In che modo SnapManager per Hyper-V gestisce backup remoti basati su VSS per Hyper-V su SMB

È possibile utilizzare SnapManager per Hyper-V per gestire i servizi di backup basati su VSS remoto. L'utilizzo del servizio di backup gestito di SnapManager per Hyper-V offre vantaggi per creare set di backup efficienti in termini di spazio.

Le ottimizzazioni di SnapManager per i backup gestiti da Hyper-V includono quanto segue:

- L'integrazione di SnapDrive con ONTAP offre l'ottimizzazione delle performance quando si scopre la posizione di condivisione delle PMI.

  ONTAP fornisce a SnapDrive il nome del volume in cui risiede la condivisione.

- SnapManager per Hyper-V specifica l'elenco dei file delle macchine virtuali nelle condivisioni SMB che il servizio di copia shadow deve copiare.

  Fornendo un elenco mirato di file di macchine virtuali, il servizio di copia shadow non deve creare copie shadow di tutti i file nella condivisione.

- La Storage Virtual Machine (SVM) conserva le snapshot per SnapManager per Hyper-V da utilizzare per i ripristini.

  Non esiste alcuna fase di backup. Il backup è l'istantanea efficiente in termini di spazio.

SnapManager per Hyper-V offre funzionalità di backup e ripristino per HyperV su SMB utilizzando il seguente processo:

1. Preparazione per l'operazione di copia shadow

   Il client VSS di SnapManager per l'applicazione Hyper-V imposta il set di copie shadow. Il client VSS raccoglie informazioni sulle condivisioni da includere nel set di copie shadow e fornisce queste informazioni a ONTAP. Un set potrebbe contenere una o più copie shadow e una copia shadow corrisponde a una condivisione.

2. Creazione del set di copie shadow (se viene utilizzato il ripristino automatico)

   Per ogni condivisione inclusa nel set di copie shadow, ONTAP crea una copia shadow e la rende scrivibile.

3. Esposizione del set di copie shadow

   Dopo che ONTAP ha creato le copie shadow, queste vengono esposte a SnapManager per Hyper-V in modo che i writer VSS dell'applicazione possano eseguire il ripristino automatico.

4. Ripristino automatico del set di copie shadow

   Durante la creazione del set di copie shadow, vi è un periodo di tempo in cui si verificano modifiche attive ai file inclusi nel set di backup. I writer VSS dell'applicazione devono aggiornare le copie shadow per assicurarsi che si trovino in uno stato completamente coerente prima del backup.

   > Il modo in cui viene eseguito il ripristino automatico è specifico dell'applicazione. Il VSS remoto non è coinvolto in questa fase.

5. Completamento e pulizia del set di copie shadow

   Il client VSS notifica a ONTAP una volta completato il ripristino automatico. Il set di copie shadow viene reso di sola lettura e quindi pronto per il backup. Quando si utilizza SnapManager per Hyper-V per il backup, i file di uno snapshot diventano il backup; pertanto, per la fase di backup, viene creata una snapshot per ogni volume contenente condivisioni nel set di backup. Una volta completato il backup, il set di copie shadow viene rimosso dal server CIFS.

Come viene utilizzato l'offload delle copie ODX con Hyper-V e SQL Server su condivisioni SMB

Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento diretto dei dati all'interno o tra dispositivi di storage compatibili senza trasferire i dati attraverso il computer host. L'offload delle copie ODX di ONTAP offre vantaggi in termini di performance quando si eseguono operazioni di copia sul server applicativo rispetto all'installazione SMB.

Nei trasferimenti di file non ODX, i dati vengono letti dal server CIFS di origine e trasferiti attraverso la rete al computer client. Il computer client trasferisce di nuovo i dati sulla rete al server CIFS di destinazione. In sintesi, il computer client legge i dati dall'origine e li scrive nella destinazione. Con i trasferimenti di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione.

Poiché le copie ODX offloaded vengono eseguite direttamente tra lo storage di origine e di destinazione, le performance sono notevolmente migliorate. I benefici delle performance ottenuti includono tempi di copia più rapidi tra origine e destinazione, utilizzo ridotto delle risorse (CPU, memoria) sul client e utilizzo ridotto della larghezza di banda i/o di rete.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti
ODX:
```

- Intra-volume

  I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Tra volumi, stesso nodo, stessa SVM (Storage Virtual Machine)

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

  I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni Hyper-V includono:

- È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

  Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

- Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
- L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.

> Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni SQL Server includono:

- È possibile utilizzare l'offload delle copie di ODX per esportare e importare i database SQL Server tra le condivisioni SMB mappate o tra le condivisioni SMB e le LUN iSCSI connesse all'interno dello stesso cluster.

- L'offload delle copie ODX viene utilizzato per le esportazioni e le importazioni dei database se lo storage di origine e di destinazione si trova nello stesso cluster.

Requisiti di configurazione e considerazioni

ONTAP e requisiti di licenza

Quando si creano soluzioni SQL Server o Hyper-V su PMI, è necessario conoscere alcuni requisiti di licenza e ONTAP per operazioni senza interruzioni su SVM.

Requisiti di versione di ONTAP

- Hyper-V su SMB

  ONTAP supporta operazioni senza interruzioni sulle condivisioni SMB per Hyper-V in esecuzione su Windows 2012 o versioni successive.

- SQL Server su SMB

  ONTAP supporta operazioni senza interruzioni su condivisioni SMB per SQL Server 2012 o versioni successive in esecuzione su Windows 2012 o versioni successive.

Per informazioni aggiornate sulle versioni supportate di ONTAP, Windows Server e SQL Server per operazioni senza interruzioni sulle condivisioni SMB, consulta la matrice di interoperabilità.

"Tool di matrice di interoperabilità NetApp"

Requisiti di licenza

Sono necessarie le seguenti licenze:

- CIFS
- FlexClone (solo per Hyper-V su SMB)

  Questa licenza è necessaria se si utilizza VSS remoto per i backup. Il servizio di copia shadow utilizza FlexClone per creare copie point-in-time dei file che vengono poi utilizzate durante la creazione di un backup.

  Una licenza FlexClone è opzionale se si utilizza un metodo di backup che non utilizza Remote VSS.

La licenza FlexClone è inclusa in "ONTAP uno". Se non si dispone di ONTAP ONE, è necessario "verificare che le licenze richieste siano installate", e, se necessario, "installarli".

Requisiti LIF di rete e dati

Quando si creano configurazioni SQL Server o Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti LIF di rete e dati).

Requisiti del protocollo di rete

- Sono supportate le reti IPv4 e IPv6.

- È richiesto SMB 3.0 o versione successiva.

  SMB 3.0 offre le funzionalità necessarie per creare le connessioni SMB continuamente disponibili necessarie per offrire operazioni senza interruzioni.

- I server DNS devono contenere voci che associano il nome del server CIFS agli indirizzi IP assegnati ai file LIF dei dati sulla macchina virtuale di storage (SVM).

  I server applicativi Hyper-V o SQL Server in genere effettuano più connessioni su più file di dati LIF quando accedono a macchine virtuali o file di database. Per una corretta funzionalità, i server applicazioni devono stabilire connessioni SMB multiple utilizzando il nome del server CIFS invece di effettuare connessioni multiple a più indirizzi IP univoci.

  Il server Witness richiede inoltre l'utilizzo del nome DNS del server CIFS invece di singoli indirizzi IP LIF.

  A partire da ONTAP 9.4, è possibile migliorare il throughput e la tolleranza agli errori per Hyper-V e SQL Server sulle configurazioni SMB attivando SMB multicanale. A tale scopo, è necessario implementare più NIC 1G, 10G o superiori nel cluster e nei client.

Requisiti Data LIF

- La SVM che ospita l'application server sulla soluzione SMB deve avere almeno un LIF di dati operativi su ogni nodo del cluster.

  Le LIF dei dati SVM possono eseguire il failover su altre porte dati all'interno del cluster, inclusi i nodi che attualmente non ospitano dati a cui accedono i server applicazioni. Inoltre, poiché il nodo di controllo è sempre il partner SFO di un nodo a cui è connesso l'application server, ogni nodo del cluster è un potenziale nodo di controllo.

- I file LIF dei dati non devono essere configurati per il ripristino automatico.

  Dopo un takeover o un evento di giveback, è necessario ripristinare manualmente le LIF dei dati alle porte home.

- Tutti gli indirizzi IP LIF dei dati devono avere una voce nel DNS e tutte le voci devono essere risolte nel nome del server CIFS.

  I server applicazioni devono connettersi alle condivisioni SMB utilizzando il nome del server CIFS. Non configurare i server applicativi per effettuare connessioni usando gli indirizzi IP LIF.

- Se il nome del server CIFS è diverso dal nome SVM, le voci DNS devono essere risolte nel nome del server CIFS.

Requisiti di volume e server SMB per Hyper-V su SMB

Quando si creano configurazioni Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti di volume e server SMB.

Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

  Questa opzione è attivata per impostazione predefinita.

- L’opzione predefinita del server CIFS dell’utente UNIX deve essere configurata con un account utente UNIX valido.

  I server applicazioni utilizzano l’account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l’utente Windows si meda correttamente a un account utente UNIX o all’account utente UNIX predefinito, ONTAP deve essere in grado di mappare l’account del computer dell’application server all’account utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

  Se si desidera utilizzare riferimenti automatici ai nodi per l’accesso a dati diversi dai file macchina Hyper-V, è necessario creare una SVM separata per tali dati.

- L’autenticazione Kerberos e NTLM deve essere consentita nel dominio a cui appartiene il server SMB.

  ONTAP non annuncia il servizio Kerberos per il VSS remoto; pertanto, il dominio deve essere impostato su Consenti NTLM.

- La funzionalità di copia shadow deve essere attivata.

  Questa funzionalità è attivata per impostazione predefinita.

- L’account di dominio Windows utilizzato dal servizio di copia shadow per la creazione delle copie shadow deve essere membro del gruppo BUILTIN/Administrators locale del server SMB o del gruppo BUILTIN/Backup Operators.

Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

  Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume.

  Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo requisito si applica solo alle copie shadow con ripristino automatico.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti di volume e server SMB per SQL Server su SMB

Quando si creano configurazioni SQL Server su SMB per operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti di volume e server SMB.

Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

  Questa opzione è attivata per impostazione predefinita.

- L'opzione predefinita del server CIFS dell'utente UNIX deve essere configurata con un account utente UNIX valido.

  I server applicazioni utilizzano l'account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l'utente Windows si meda correttamente a un account utente UNIX o all'account utente UNIX predefinito, ONTAP deve essere in grado di mappare l'account del computer dell'application server all'account utente UNIX predefinito.

  Inoltre, SQL Server utilizza un utente di dominio come account del servizio SQL Server. L'account di servizio deve anche essere associato all'utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

  Se si desidera utilizzare riferimenti automatici ai nodi per l'accesso a dati diversi dai file di database di SQL Server, è necessario creare una SVM separata per tali dati.

- All'account utente Windows utilizzato per l'installazione di SQL Server su ONTAP deve essere assegnato il privilegio SeSecurityPrivilege.

  Questo privilegio viene assegnato al gruppo BUILTIN/Administrators locale del server SMB.

Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

  Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni di backup del plug-in SnapCenter per SQL Server, è necessario disporre di spazio disponibile sufficiente sul volume.

Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

Informazioni correlate

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisiti e considerazioni di condivisione continuamente disponibili per Hyper-V su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni Hyper-V su SMB che supportano operazioni senza interruzioni, è necessario essere consapevoli di determinati requisiti e considerazioni.

Condividere i requisiti

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà Continuously Available (disponibilità continua).

  Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS, non è possibile inserire i file Hyper-V in condivisioni che contengono giunzioni.

  In caso di ripristino automatico, la creazione della copia shadow non riesce se viene rilevata una giunzione durante l'attraversamento della condivisione. In caso di non ripristino automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS con il ripristino automatico, non è possibile inserire i file Hyper-V in condivisioni contenenti quanto segue:
  - Symlink, hardlink o widelink
  - File non regolari

    La creazione della copia shadow non riesce se nella copia shadow sono presenti collegamenti o file non regolari. Questo requisito si applica solo alle copie shadow con ripristino automatico.

  - Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume (solo per Hyper-V su SMB).

    Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo requisito si applica solo alle copie shadow con ripristino automatico.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
  - Home directory
  - Caching degli attributi
  - BranchCache

Considerazioni

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni Hyper-V su SMB:
  - Controllo
  - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` parametro impostato su `Yes`.

Requisiti e considerazioni di condivisione continuamente disponibili per SQL Server su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni SQL Server su SMB che supportano operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti e considerazioni.

Condividere i requisiti

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

  Per fornire operazioni senza interruzioni per i server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per operazioni senza interruzioni sulle condivisioni SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per operazioni senza interruzioni sulle condivisioni SMB, è necessario posizionare manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà Continuously Available (disponibilità continua).

  Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni del plug-in SnapCenter per SQL Server, è necessario disporre di spazio disponibile sufficiente sul volume.

  Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
  - Home directory

- Caching degli attributi
- BranchCache

Condividere le considerazioni

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni SQL Server su SMB:
  - Controllo
  - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` condividere il set di proprietà.

Considerazioni sul VSS remoto per le configurazioni Hyper-V su SMB

Quando si utilizzano soluzioni di backup abilitate per VSS remoto per configurazioni Hyper-V su SMB, è necessario tenere presenti alcune considerazioni.

Considerazioni generali su Remote VSS

- È possibile configurare un massimo di 64 condivisioni per server applicazioni Microsoft.

  L'operazione di copia shadow non riesce se sono presenti più di 64 condivisioni in un set di copie shadow. Si tratta di un requisito Microsoft.

- È consentito un solo set di copie shadow attive per server CIFS.

  Un'operazione di copia shadow non riesce se è in corso un'operazione di copia shadow sullo stesso server CIFS. Si tratta di un requisito Microsoft.

- Non sono consentite giunzioni all'interno della struttura di directory in cui Remote VSS crea una copia shadow.
  - In caso di ripristino automatico, la creazione della copia shadow non riesce se si incontra una giunzione durante l'attraversamento della condivisione.
  - Nel caso di recovery non automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

Considerazioni sul VSS remoto valide solo per le copie shadow con ripristino automatico

Alcuni limiti si applicano solo alle copie shadow con ripristino automatico.

- Per la creazione delle copie shadow è consentita una profondità massima di directory di cinque sottodirectory.

  Questa è la profondità della directory in cui il servizio di copia shadow crea un set di backup delle copie shadow. La creazione della copia shadow non riesce se le directory contenenti il file della macchina virtuale sono nidificate più in profondità di cinque livelli. Questa opzione consente di limitare l'attraversamento della directory durante la clonazione della condivisione. È possibile modificare la profondità massima della directory utilizzando un'opzione del server CIFS.

- La quantità di spazio disponibile sul volume deve essere adeguata.

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow.

- Non sono consentiti collegamenti o file non regolari all'interno della struttura di directory in cui Remote VSS crea una copia shadow.

  La creazione della copia shadow non riesce se nella condivisione sono presenti collegamenti o file non regolari alla copia shadow. Il processo di clonazione non li supporta.

- Non sono consentiti ACL NFSv4 nelle directory.

  Sebbene la creazione delle copie shadow conservi gli ACL NFSv4 nei file, gli ACL NFSv4 nelle directory vengono persi.

- È consentito creare un set di copie shadow per un massimo di 60 secondi.

  Le specifiche Microsoft consentono di creare il set di copie shadow per un massimo di 60 secondi. Se il client VSS non riesce a creare il set di copie shadow entro questo intervallo di tempo, l'operazione di copia shadow non riesce; pertanto, questo limita il numero di file in un set di copie shadow. Il numero effettivo di file o macchine virtuali che possono essere inclusi in un set di backup varia; tale numero dipende da molti fattori e deve essere determinato per ogni ambiente del cliente.

Requisiti di offload delle copie ODX per SQL Server e Hyper-V su SMB

L'offload delle copie ODX deve essere attivato se si desidera migrare i file delle macchine virtuali o esportare e importare i file di database direttamente dall'origine alla posizione di storage di destinazione senza inviare dati attraverso i server applicazioni. È necessario comprendere alcuni requisiti sull'utilizzo dell'offload delle copie ODX con SQL Server e Hyper-V su soluzioni SMB.

L'utilizzo dell'offload delle copie di ODX offre un significativo vantaggio in termini di performance. Questa opzione del server CIFS è attivata per impostazione predefinita.

- SMB 3.0 deve essere abilitato per utilizzare l'offload delle copie ODX.
- I volumi di origine devono essere di almeno 1.25 GB.
- La deduplica deve essere attivata sui volumi utilizzati con l'offload delle copie.
- Se si utilizzano volumi compressi, il tipo di compressione deve essere adattivo e sono supportate solo le dimensioni del gruppo di compressione 8K.

  Il tipo di compressione secondario non è supportato

- Per utilizzare l'offload delle copie di ODX per migrare i guest Hyper-V all'interno e tra i dischi, i server Hyper-V devono essere configurati per l'utilizzo di dischi SCSI.

  L'impostazione predefinita prevede la configurazione dei dischi IDE, ma l'offload delle copie ODX non funziona quando i guest vengono migrati se i dischi vengono creati utilizzando dischi IDE.

Raccomandazioni per le configurazioni SQL Server e Hyper-V su SMB

Per essere sicuri che le configurazioni di SQL Server e Hyper-V su SMB siano solide e operative, è necessario conoscere le Best practice consigliate per la configurazione delle soluzioni.

Raccomandazioni generali

- Separare i file del server applicazioni dai dati generali dell'utente.

  Se possibile, dedicare un'intera macchina virtuale di storage (SVM) e il relativo storage ai dati dell'application server.

- Per ottenere performance ottimali, non abilitare la firma SMB sulle SVM utilizzate per memorizzare i dati dell'application server.
- Per ottenere le migliori performance e una maggiore tolleranza agli errori, abilitare SMB multicanale per fornire più connessioni tra ONTAP e client in una singola sessione SMB.
- Non creare condivisioni continuamente disponibili su condivisioni diverse da quelle utilizzate nella configurazione Hyper-V o SQL Server su SMB.
- Disattiva la notifica delle modifiche sulle condivisioni utilizzate per la disponibilità continua.
- Non eseguire uno spostamento del volume contemporaneamente al trasferimento dell'aggregato (ARL) perché ARL ha fasi che interrompono alcune operazioni.
- Per le soluzioni Hyper-V su SMB, utilizzare dischi iSCSI in-guest durante la creazione di macchine virtuali in cluster. Condiviso `.VHDX` I file non sono supportati per Hyper-V su SMB nelle condivisioni SMB ONTAP.

Pianificare la configurazione di Hyper-V o SQL Server su SMB

Completare il foglio di lavoro per la configurazione del volume

Il foglio di lavoro offre un modo semplice per registrare i valori necessari per la creazione di volumi per le configurazioni SQL Server e Hyper-V su SMB.

Per ciascun volume, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

  Il nome SVM è lo stesso per tutti i volumi.

- Nome del volume
- Nome dell'aggregato

  È possibile creare volumi su aggregati situati su qualsiasi nodo del cluster.

- Dimensione
- Percorso di giunzione

Quando si creano volumi utilizzati per memorizzare i dati dell'application server, tenere presente quanto segue:

- Se il volume root non dispone di uno stile di protezione NTFS, è necessario specificare lo stile di protezione come NTFS quando si crea il volume.

  Per impostazione predefinita, i volumi ereditano lo stile di sicurezza del volume root SVM.

- I volumi devono essere configurati con la garanzia di spazio del volume predefinita.
- Facoltativamente, è possibile configurare l'impostazione di gestione automatica dello spazio.
- È necessario impostare l'opzione che determina la riserva di spazio dell'istantanea su `0`.
- Il criterio snapshot applicato al volume deve essere disattivato.

  Se la policy di snapshot della SVM è disabilitata, non dovrai specificare una policy di Snapshot per i volumi. I volumi ereditano la policy di snapshot per la SVM. Se la policy di Snapshot per la SVM non è disabilitata ed è configurata per creare snapshot, devi specificare una policy di Snapshot a livello di volume e tale policy deve essere disabilitata. I backup abilitati al servizio di copia shadow e i backup di SQL Server gestiscono la creazione e l'eliminazione di snapshot.

- Non è possibile configurare i mirror di condivisione del carico per i volumi.

I percorsi di giunzione su cui si intende creare le condivisioni utilizzate dai server applicazioni devono essere scelti in modo che non vi siano volumi congiunti al di sotto del punto di ingresso della condivisione.

Ad esempio, se si desidera memorizzare i file delle macchine virtuali su quattro volumi denominati "vol1", "vol2", "vol3" e "vol4", è possibile creare lo spazio dei nomi mostrato nell'esempio. È quindi possibile creare condivisioni per i server applicazioni nei seguenti percorsi: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, e. `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Tipi di informazioni	Valori
Volume 1: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 2: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 3: Nome del volume, aggregato, dimensione, percorso di giunzione	

Tipi di informazioni	Valori
Volume 4: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 5: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volume 6: Nome del volume, aggregato, dimensione, percorso di giunzione	
Volumi aggiuntivi: Nome del volume, aggregato, dimensione, percorso di giunzione	

Completare il foglio di lavoro per la configurazione della condivisione SMB

Utilizzare questo foglio di lavoro per registrare i valori necessari per la creazione di condivisioni SMB continuamente disponibili per le configurazioni SQL Server e Hyper-V su SMB.

Informazioni sulle proprietà delle condivisioni SMB e sulle impostazioni di configurazione

Per ciascuna condivisione, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

  Il nome SVM è lo stesso per tutte le condivisioni

- Nome di condivisione
- Percorso
- Condividere le proprietà

  È necessario configurare le seguenti due proprietà di condivisione:

  - `oplocks`
  - `continuously-available`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - I collegamenti simbolici devono essere disattivati (il valore per `-symlink-properties` il parametro deve essere nullo [""]).

Informazioni sui percorsi di condivisione

Se si utilizza il VSS remoto per eseguire il backup dei file Hyper-V, è importante scegliere i percorsi di

condivisione da utilizzare per le connessioni SMB dai server Hyper-V alle posizioni di storage in cui sono memorizzati i file delle macchine virtuali. Sebbene sia possibile creare condivisioni in qualsiasi punto dello spazio dei nomi, i percorsi per le condivisioni utilizzati dai server Hyper-V non devono contenere volumi congiunti. Le operazioni di copia shadow non possono essere eseguite su percorsi di condivisione che contengono punti di giunzione.

SQL Server non è in grado di incrociare le giunzioni durante la creazione della struttura di directory del database. Non creare percorsi di condivisione per SQL Server che contengono punti di giunzione.

Ad esempio, dato lo spazio dei nomi mostrato, se si desidera memorizzare i file di macchine virtuali o i file di database sui volumi "vol1", "vol2", "vol3" e "vol4", è necessario creare condivisioni per i server applicazioni nei seguenti percorsi: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, e. `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Sebbene sia possibile creare condivisioni su `/data1` e `/data2` percorsi per la gestione amministrativa, non configurare i server applicazioni in modo che utilizzino tali condivisioni per archiviare i dati.

Foglio di lavoro per la pianificazione

Tipi di informazioni	Valori
Volume 1: Nome e percorso della condivisione SMB	
Volume 2: Nome e percorso della condivisione SMB	
Volume 3: Nome e percorso della condivisione SMB	
Volume 4: Nome e percorso della condivisione SMB	
Volume 5: Nome e percorso della condivisione SMB	
Volume 6: Nome e percorso della condivisione SMB	
Volume 7: Nome e percorso della condivisione SMB	
Volumi aggiuntivi: Nomi e percorsi di condivisione SMB	

Creazione di configurazioni ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB

Crea configurazioni ONTAP per operazioni senza interruzioni con la panoramica di Hyper-V e SQL Server su SMB

Per preparare le installazioni di ONTAP e Hyper-V, è necessario eseguire diverse operazioni di configurazione di SQL Server che forniscono operazioni senza interruzioni su SMB.

Prima di creare la configurazione ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB, è necessario completare le seguenti attività:

- I servizi Time devono essere impostati sul cluster.
- È necessario configurare la rete per SVM.
- È necessario creare la SVM.
- Le interfacce Data LIF devono essere configurate su SVM.
- Il DNS deve essere configurato sulla SVM.
- I servizi Names desiderati devono essere impostati per la SVM.
- È necessario creare il server SMB.

Informazioni correlate

Pianificare la configurazione di Hyper-V o SQL Server su SMB

Requisiti di configurazione e considerazioni

Verificare che sia consentita l'autenticazione Kerberos e NTLMv2 (Hyper-V su condivisioni SMB)

Le operazioni senza interruzioni per Hyper-V su SMB richiedono che il server CIFS su una SVM dati e il server Hyper-V consentano l'autenticazione Kerberos e NTLMv2. È necessario verificare le impostazioni sul server CIFS e sui server Hyper-V che controllano i metodi di autenticazione consentiti.

A proposito di questa attività

L'autenticazione Kerberos è necessaria quando si effettua una connessione di condivisione continuamente disponibile. Parte del processo VSS remoto utilizza l'autenticazione NTLMv2. Pertanto, le connessioni che utilizzano entrambi i metodi di autenticazione devono essere supportate per le configurazioni Hyper-V su SMB.

È necessario configurare le seguenti impostazioni per consentire l'autenticazione Kerberos e NTLMv2:

- I criteri di esportazione per SMB devono essere disattivati sulla macchina virtuale di storage (SVM).

L'autenticazione Kerberos e NTLMv2 è sempre abilitata sulle SVM, ma è possibile utilizzare i criteri di esportazione per limitare l'accesso in base al metodo di autenticazione.

I criteri di esportazione per SMB sono opzionali e sono disattivati per impostazione predefinita. Se i criteri di esportazione sono disattivati, l'autenticazione Kerberos e NTLMv2 è consentita per impostazione predefinita

su un server CIFS.

- Il dominio a cui appartengono il server CIFS e i server Hyper-V deve consentire l'autenticazione Kerberos e NTLMv2.

L'autenticazione Kerberos è attivata per impostazione predefinita nei domini Active Directory. Tuttavia, l'autenticazione NTLMv2 può essere non consentita, utilizzando le impostazioni dei criteri di protezione o i criteri di gruppo.

Fasi

1. Eseguire le seguenti operazioni per verificare che i criteri di esportazione siano disattivati su SVM:
   a. Impostare il livello di privilegio su Advanced (avanzato):

      `set -privilege advanced`

   b. Verificare che il `-is-exportpolicy-enabled` L'opzione del server CIFS è impostata su `false`:

      `vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled`

   c. Tornare al livello di privilegio admin:

      `set -privilege admin`

2. Se i criteri di esportazione per SMB non sono disattivati, disabilitarli:

   `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`

3. Verificare che l'autenticazione NTLMv2 e Kerberos sia consentita nel dominio.

   Per informazioni sulla determinazione dei metodi di autenticazione consentiti nel dominio, consultare la Microsoft TechNet Library.

4. Se il dominio non consente l'autenticazione NTMLv2, attivare l'autenticazione NTLMv2 utilizzando uno dei metodi descritti nella documentazione Microsoft.

Esempio

I seguenti comandi verificano che i criteri di esportazione per SMB siano disattivati su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

Verificare che gli account di dominio corrispondano all'utente UNIX predefinito in ONTAP

Hyper-V e SQL Server utilizzano gli account di dominio per creare connessioni SMB alle condivisioni continuamente disponibili. Per creare correttamente la connessione, l'account del computer deve essere mappato correttamente a un utente UNIX. Il modo più conveniente per eseguire questa operazione consiste nel mappare l'account del computer all'utente UNIX predefinito.

A proposito di questa attività

Hyper-V e SQL Server utilizzano gli account dei computer di dominio per creare connessioni SMB. Inoltre, SQL Server utilizza un account utente di dominio come account di servizio che effettua anche connessioni SMB.

Quando si crea una macchina virtuale di archiviazione (SVM), ONTAP crea automaticamente l'utente predefinito denominato `pcuser` (con un UID di `65534`) e il gruppo denominato `pcuser` (con un GID di `65534`), e aggiunge l'utente predefinito al `pcuser` gruppo. Se si configura una soluzione Hyper-V su SMB su una SVM esistente prima dell'aggiornamento del cluster a Data ONTAP 8.2, l'utente e il gruppo predefiniti potrebbero non esistere. In caso contrario, è necessario crearli prima di configurare l'utente UNIX predefinito del server CIFS.

Fasi

1. Determinare se esiste un utente UNIX predefinito:

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

2. Se l'opzione utente predefinita non è impostata, determinare se esiste un utente UNIX che può essere designato come utente UNIX predefinito:

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

3. Se l'opzione utente predefinito non è impostata e non esiste un utente UNIX che può essere designato come utente UNIX predefinito, creare il gruppo predefinito e l'utente UNIX predefinito, quindi aggiungere l'utente predefinito al gruppo.

   , al gruppo predefinito viene assegnato il nome "pcuser". Il GID assegnato al gruppo deve essere `65534`.

   a. Crea il gruppo predefinito:

   ```
   vserver services unix-group create -vserver <vserver_name> -name
   pcuser -id 65534
   ```

   b. Crea l'utente predefinito e aggiungilo al gruppo predefinito:

   ```
   vserver services unix-user create -vserver <vserver_name> -user
   pcuser -id 65534 -primary-gid 65534
   ```

   c. Verificare che l'utente e il gruppo predefiniti siano configurati correttamente:

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

   ```
   vserver services unix-group show -vserver <vserver_name> -members
   ```

4. Se l'utente predefinito del server CIFS non è configurato, eseguire le seguenti operazioni:

   a. Configurare l'utente predefinito:

   ```
   vserver cifs options modify -vserver <vserver_name> -default-unix
   -user pcuser
   ```

   b. Verificare che l'utente UNIX predefinito sia configurato correttamente:

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

5. Per verificare che l'account del computer del server applicazioni sia associato correttamente all'utente predefinito, mappare un'unità a una condivisione che risiede sulla SVM e confermare l'associazione dell'utente Windows all'utente UNIX utilizzando `vserver cifs session show` comando.

   Ulteriori informazioni su `vserver cifs options` nella "Riferimento al comando ONTAP".

Esempio

I seguenti comandi determinano che l'utente predefinito del server CIFS non è impostato, ma determina che `pcuser` utente e `pcuser` gruppo esiste. Il `pcuser` l'utente è assegnato come utente predefinito del server CIFS su SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
```

```
  WINS Servers            : -
```

Verificare che lo stile di protezione del volume root SVM sia impostato su NTFS

Per garantire il successo delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB, i volumi devono essere creati con lo stile di sicurezza NTFS. Poiché lo stile di sicurezza del volume root viene applicato per impostazione predefinita ai volumi creati sulla macchina virtuale di storage (SVM), lo stile di sicurezza del volume root deve essere impostato su NTFS.

A proposito di questa attività

- È possibile specificare lo stile di sicurezza del volume root al momento della creazione di SVM.
- Se SVM non viene creato con il volume root impostato sullo stile di protezione NTFS, è possibile modificare lo stile di protezione in un secondo momento utilizzando `volume modify` comando.

Fasi

1. Determinare lo stile di sicurezza corrente del volume root SVM:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. Se il volume root non è un volume di sicurezza NTFS, impostare lo stile di protezione su NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Verificare che il volume root SVM sia impostato sullo stile di protezione NTFS:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Esempio

I seguenti comandi verificano che lo stile di protezione del volume root sia NTFS su SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verificare che le opzioni del server CIFS richieste siano configurate

È necessario verificare che le opzioni del server CIFS richieste siano attivate e configurate in base ai requisiti delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

A proposito di questa attività

- SMB 2.x e SMB 3.0 devono essere abilitati.
- L'offload delle copie di ODX deve essere abilitato per utilizzare l'offload delle copie che migliora le performance.
- I servizi di copia shadow di VSS devono essere attivati se la soluzione Hyper-V su SMB utilizza servizi di backup abilitati per VSS remoto (solo Hyper-V).

Fasi

1. Verificare che le opzioni del server CIFS richieste siano attivate sulla macchina virtuale di storage (SVM):
   a. Impostare il livello di privilegio su Advanced (avanzato):

      `set -privilege advanced`

   b. Immettere il seguente comando:

      `vserver cifs options show -vserver *vserver_name*`

      Le seguenti opzioni devono essere impostate su `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Solo Hyper-V)
2. Se una delle opzioni non è impostata su `true`, eseguire le seguenti operazioni:
   a. Impostarli su `true` utilizzando `vserver cifs options modify` comando.
   b. Verificare che le opzioni siano impostate su `true` utilizzando `vserver cifs options show` comando.
3. Tornare al livello di privilegio admin:

   `set -privilege admin`

Esempio

I seguenti comandi verificano che le opzioni richieste per la configurazione Hyper-V su SMB siano attivate su SVM vs1. Nell'esempio, l'offload delle copie ODX deve essere abilitato per soddisfare i requisiti delle opzioni.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configurare SMB multicanale per performance e ridondanza

A partire da ONTAP 9.4, è possibile configurare SMB multicanale in modo da fornire più connessioni tra ONTAP e client in una singola sessione SMB. In questo modo si migliora il throughput e la tolleranza agli errori per Hyper-V e SQL Server rispetto alle configurazioni SMB.

Prima di iniziare

È possibile utilizzare la funzionalità SMB multicanale solo quando i client negoziano con SMB 3.0 o versioni successive. SMB 3.0 e versioni successive sono attivate sul server SMB ONTAP per impostazione predefinita.

A proposito di questa attività

I client SMB rilevano e utilizzano automaticamente più connessioni di rete se viene identificata una configurazione corretta nel cluster ONTAP.

Il numero di connessioni simultanee in una sessione SMB dipende dalle schede NIC implementate:

- **NIC 1G su client e cluster ONTAP**

  Il client stabilisce una connessione per NIC e associa la sessione a tutte le connessioni.

- **NIC da 10 G e capacità superiore su cluster client e ONTAP**

  Il client stabilisce fino a quattro connessioni per NIC e associa la sessione a tutte le connessioni. Il client può stabilire connessioni su più NIC da 10 G e capacità maggiore.

È inoltre possibile modificare i seguenti parametri (privilegio avanzato):

- `-max-connections-per-session`

  Numero massimo di connessioni consentite per sessione multicanale. L'impostazione predefinita è 32 connessioni.

  Se si desidera attivare più connessioni rispetto a quelle predefinite, è necessario apportare modifiche simili alla configurazione del client, che ha anche un valore predefinito di 32 connessioni.

- `-max-lifs-per-session`

  Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. L'impostazione predefinita è 256 interfacce di rete.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Abilitare SMB Multichannel sul server SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verificare che ONTAP stia segnalando sessioni multicanale SMB:

```
vserver cifs session show
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutte le sessioni SMB, che mostrano più connessioni per una singola sessione:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate su una sessione SMB con id sessione 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Creare volumi di dati NTFS

È necessario creare volumi di dati NTFS sulla macchina virtuale di storage (SVM) prima di poter configurare condivisioni continuamente disponibili per l'utilizzo con Hyper-V o

SQL Server su server applicazioni SMB. Utilizzare il foglio di lavoro per la configurazione del volume per creare i volumi di dati.

A proposito di questa attività

Per personalizzare un volume di dati, è possibile utilizzare parametri opzionali. Per ulteriori informazioni sulla personalizzazione dei volumi, vedere "Gestione dello storage logico".

Durante la creazione dei volumi di dati, non è necessario creare punti di giunzione all'interno di un volume contenente quanto segue:

- File Hyper-V per i quali ONTAP crea copie shadow
- File di database di SQL Server di cui viene eseguito il backup mediante SQL Server

> Se si crea inavvertitamente un volume che utilizza uno stile di sicurezza misto o UNIX, non è possibile modificare il volume in un volume di sicurezza NTFS e utilizzarlo direttamente per creare condivisioni continuamente disponibili per operazioni senza interruzioni. Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB non funzionano correttamente, a meno che i volumi utilizzati nella configurazione non vengano creati come volumi di sicurezza NTFS.è necessario eliminare il volume e ricrearlo con lo stile di protezione NTFS, In alternativa, è possibile mappare il volume su un host Windows e applicare un ACL nella parte superiore del volume e propagare l'ACL a tutti i file e cartelle del volume.

Fasi

1. Creare il volume di dati immettendo il comando appropriato:

Se si desidera creare un volume in una SVM in cui lo stile di sicurezza del volume root è…	Immettere il comando…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Non NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Verificare che la configurazione del volume sia corretta:

```
volume show -vserver vserver_name -volume volume_name
```

Creare condivisioni SMB continuamente disponibili

Dopo aver creato i volumi di dati, è possibile creare le condivisioni continuamente disponibili utilizzate dai server applicazioni per accedere alla macchina virtuale Hyper-V, ai file di configurazione e ai file di database di SQL Server. È necessario utilizzare il foglio

di lavoro di configurazione della condivisione per creare le condivisioni SMB.

Fasi

1. Visualizzare informazioni sui volumi di dati esistenti e sui relativi percorsi di giunzione:

   volume show -vserver *vserver_name* -junction

2. Creare una condivisione SMB sempre disponibile:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - È possibile aggiungere un commento alla configurazione della condivisione.
   - Per impostazione predefinita, la proprietà di condivisione dei file offline è configurata sulla condivisione ed è impostata su `manual`.
   - ONTAP crea la condivisione con l'autorizzazione di condivisione predefinita di `Everyone` / `Full Control`.

3. Ripetere il passaggio precedente per tutte le condivisioni nel foglio di lavoro di configurazione della condivisione.
4. Verificare che la configurazione sia corretta utilizzando `vserver cifs share show` comando.
5. Configurare le autorizzazioni dei file NTFS sulle condivisioni continuamente disponibili mappando un disco a ciascuna condivisione e configurando le autorizzazioni dei file utilizzando la finestra **Proprietà di Windows**.

Esempio

I seguenti comandi creano una condivisione continuamente disponibile denominata "data2" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. I collegamenti simbolici vengono disattivati impostando `-symlink` parametro a. `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Aggiungere il privilegio SeSecurityPrivilege all'account utente (per SQL Server delle condivisioni SMB)

All'account utente di dominio utilizzato per l'installazione del server SQL deve essere assegnato il privilegio "SeSecurityPrivilege" per eseguire determinate azioni sul server CIFS che richiedono privilegi non assegnati per impostazione predefinita agli utenti di dominio.

Prima di iniziare

L'account di dominio utilizzato per l'installazione di SQL Server deve già esistere.

A proposito di questa attività

Quando si aggiunge il privilegio all'account del programma di installazione di SQL Server, ONTAP potrebbe validare l'account contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

Fasi

1. Aggiungere il privilegio “SeSecurityPrivilege”:

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   Il valore di `-user-or-group-name` Parameter è il nome dell’account utente di dominio utilizzato per l’installazione di SQL Server.

2. Verificare che il privilegio sia applicato all’account:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Esempio

Il seguente comando aggiunge il privilegio “SeSecurityPrivilege” all’account del programma di installazione di SQL Server nel dominio DI ESEMPIO per la macchina virtuale di storage (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- --------------------       ---------------
vs1       EXAMPLE\SQLinstaller       SeSecurityPrivilege
```

Configurare la profondità della directory della copia shadow VSS (per Hyper-V su condivisioni SMB)

Facoltativamente, è possibile configurare la profondità massima delle directory all’interno delle condivisioni SMB su cui creare le copie shadow. Questo parametro è utile se si desidera controllare manualmente il livello massimo di sottodirectory in cui ONTAP deve creare copie shadow.

Prima di iniziare

La funzione di copia shadow del VSS deve essere attivata.

A proposito di questa attività

L’impostazione predefinita prevede la creazione di copie shadow per un massimo di cinque sottodirectory. Se il valore è impostato su `0`, ONTAP crea copie shadow per tutte le sottodirectory.

> Sebbene sia possibile specificare che la profondità della directory shadow set copy includa più di cinque sottodirectory o tutte le sottodirectory, Microsoft richiede che la creazione del set di copie shadow venga completata entro 60 secondi. La creazione del set di copie shadow non riesce se non può essere completata entro questo intervallo di tempo. La profondità della directory di copia shadow scelta non deve far superare il tempo di creazione.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Impostare la profondità della directory della copia shadow del VSS al livello desiderato:

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Gestire le configurazioni Hyper-V e SQL Server su SMB

Configurare le condivisioni esistenti per la disponibilità continua

È possibile modificare le condivisioni esistenti per diventare condivisioni continuamente disponibili utilizzate dai server applicativi Hyper-V e SQL Server per accedere senza interruzioni ai file di configurazione e alla macchina virtuale Hyper-V e ai file di database SQL Server.

A proposito di questa attività

Non è possibile utilizzare una condivisione esistente come condivisione continuamente disponibile per operazioni senza interruzioni con server applicazioni su SMB se la condivisione ha le seguenti caratteristiche:

- Se il `homedirectory` la proprietà share viene impostata su tale condivisione
- Se la condivisione contiene link simbolici o widelink abilitati
- Se la condivisione contiene volumi congiundati al di sotto della radice della condivisione

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:

- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

È necessario configurare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate. Se sono presenti nell'elenco delle proprietà di condivisione correnti, devono essere rimosse dalla condivisione continuamente disponibile:

- `attributecache`
- `branchcache`

Fasi

1. Visualizza le impostazioni correnti dei parametri di condivisione e l'elenco corrente delle proprietà di condivisione configurate:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Se necessario, modificare i parametri di condivisione per disabilitare i collegamenti simbolici e impostare i file offline su manuale utilizzando il `vserver cifs share modify` comando.
   - È possibile disattivare i collegamenti simbolici impostando il valore di `-symlink` parametro a. `""`.
   - È possibile impostare `-offline-files` impostare correttamente il parametro specificando `manual`.
3. Aggiungere la `continuously-available` proprietà di condivisione e, se necessario, la `oplocks` proprietà di condivisione:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Se il `oplocks` la proprietà di condivisione non è già impostata, è necessario aggiungerla con `continuously-available` condividere la proprietà.

4. Rimuovere eventuali proprietà di condivisione non supportate nelle condivisioni a disponibilità continua:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   È possibile rimuovere una o più proprietà di condivisione specificando le proprietà di condivisione con un elenco delimitato da virgole.

5. Verificare che il `-symlink` e. `-offline-files` i parametri sono impostati correttamente:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Verificare che l'elenco delle proprietà di condivisione configurate sia corretto:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Esempi

Il seguente esempio mostra come configurare una condivisione esistente, denominata "share1" su una Storage Virtual Machine (SVM) "VS1" per NDOS con un application server su SMB:

- I collegamenti simbolici vengono disattivati nella condivisione impostando il `-symlink` parametro su `""`.

- Il `-offline-file` il parametro viene modificato e impostato su `manual`.
- Il `continuously-available` la proprietà share viene aggiunta alla condivisione.
- Il `oplocks` la proprietà di condivisione è già presente nell'elenco delle proprietà di condivisione, pertanto non è necessario aggiungerla.
- Il `attributecache` la proprietà share viene rimossa dalla condivisione.
- Il `browsable` La proprietà Share è opzionale per una condivisione a disponibilità continua utilizzata per NDOS con server applicazioni su SMB e viene conservata come una delle proprietà di condivisione.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Abilitare o disabilitare le copie shadow VSS per i backup Hyper-V su SMB

Se si utilizza un'applicazione di backup VSS-aware per eseguire il backup dei file di macchine virtuali Hyper-V memorizzati nelle condivisioni SMB, è necessario attivare la copia shadow VSS. Se non si utilizzano applicazioni di backup compatibili con VSS, è possibile disattivare la copia shadow del VSS. L'impostazione predefinita prevede l'attivazione della copia shadow del VSS.

A proposito di questa attività

È possibile attivare o disattivare le copie shadow VSS in qualsiasi momento.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   `set -privilege advanced`

2. Eseguire una delle seguenti operazioni:

Se si desidera che le copie shadow di VSS siano…	Immettere il comando…
Attivato	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true`**
Disattivato	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false`**

3. Tornare al livello di privilegio admin:

   `set -privilege admin`

Esempio

I seguenti comandi abilitano le copie shadow VSS su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Utilizza le statistiche per monitorare l'attività di Hyper-V e SQL Server su SMB

Determinare quali oggetti e contatori di statistiche sono disponibili in ONTAP

Prima di ottenere informazioni su CIFS, SMB, audit e statistiche hash BranchCache e monitorare le performance, è necessario sapere quali oggetti e contatori sono disponibili per ottenere i dati.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera determinare…	Inserisci…
Quali oggetti sono disponibili	`statistics catalog object show`
Oggetti specifici disponibili	`statistics catalog object show -object` *`object_name`*
Quali contatori sono disponibili	`statistics catalog counter show -object` *`object_name`*

   Scopri di più su `statistics catalog object show` E `statistics catalog counter show` nel "Riferimento al comando ONTAP" .

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Esempi

Il seguente comando visualizza le descrizioni degli oggetti statistici selezionati relativi all'accesso CIFS e SMB nel cluster, come si vede al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

Il seguente comando visualizza informazioni su alcuni contatori di `cifs` oggetto visto a livello di privilegi avanzati:

> In questo esempio non vengono visualizzati tutti i contatori disponibili per `cifs` oggetto; l'output è troncato.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Ulteriori informazioni su `statistics start` nella "Riferimento al comando ONTAP".

Visualizza le statistiche SMB in ONTAP

È possibile visualizzare varie statistiche SMB per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati.
2. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le statistiche per…	Immettere il seguente comando…
Tutte le versioni di SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x e SMB 3.0	**`statistics show -object smb2`**
Sottosistema SMB del nodo	**`statistics show -object nblade_cifs`**

Informazioni correlate

- "le statistiche mostrano"
- "inizio delle statistiche"
- "le statistiche si fermano"

Verificare che la configurazione sia in grado di eseguire operazioni senza interruzioni

Utilizzare il monitoraggio dello stato di salute per determinare se lo stato delle operazioni senza interruzioni è integro

Il monitoraggio dello stato di salute fornisce informazioni sullo stato di salute del sistema nel cluster. Il monitor dello stato di salute monitora le configurazioni di Hyper-V e SQL Server su SMB per garantire operazioni senza interruzioni (NDOS) per gli application server. Se lo stato è degradato, è possibile visualizzare i dettagli del problema, incluse la probabile causa e le azioni di ripristino consigliate.

Sono disponibili diversi monitor di stato. ONTAP monitora sia lo stato generale del sistema che lo stato di salute dei singoli monitor. Il monitor di stato della connettività del nodo contiene il sottosistema CIFS-NDO. Il monitor dispone di una serie di policy di salute che attivano avvisi se determinate condizioni fisiche possono causare interruzioni e, se esiste una condizione di interruzione, genera avvisi e fornisce informazioni sulle azioni correttive. Per le configurazioni NDO su SMB, vengono generati avvisi per le due seguenti condizioni:

ID avviso	Severità	Condizione
HaNotReadyCifsNdo_Alert	Maggiore	Uno o più file ospitati da un volume in un aggregato sul nodo sono stati aperti attraverso una condivisione SMB continuamente disponibile con la promessa di persistenza in caso di guasto; tuttavia, la relazione ha con il partner non è configurata o non è integro.
NoStandbyLifCifsNdo_Alert	Minore	La macchina virtuale di storage (SVM) sta fornendo attivamente i dati tramite SMB attraverso un nodo e ci sono file SMB aperti in modo persistente su condivisioni continuamente disponibili; tuttavia, il nodo partner non sta esponendo alcun LIF di dati attivo per SVM.

Visualizzazione dello stato delle operazioni senza interruzioni mediante il monitoraggio dello stato di salute del sistema

È possibile utilizzare `system health` Comandi per visualizzare informazioni sullo stato generale del sistema del cluster e sullo stato del sottosistema CIFS-NDO, per rispondere agli avvisi, per configurare gli avvisi futuri e per visualizzare informazioni sulla configurazione del monitoraggio dello stato di salute.

Fasi

1. Monitorare lo stato di salute eseguendo l'azione appropriata:

Se si desidera visualizzare…	Immettere il comando…
Lo stato di salute del sistema, che riflette lo stato generale dei singoli monitor di salute	**system health status show**
Informazioni sullo stato di salute del sottosistema CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Visualizzare le informazioni sulla configurazione del monitoraggio degli avvisi CIFS-NDO eseguendo le azioni appropriate:

Se si desidera visualizzare informazioni su…	Immettere il comando…
La configurazione e lo stato del monitor di stato per il sottosistema CIFS-NDO, ad esempio i nodi monitorati, lo stato di inizializzazione e lo stato	**system health config show -subsystem CIFS-NDO**

Se si desidera visualizzare informazioni su…	Immettere il comando…
CIFS-NDO avvisa che un monitor di stato può potenzialmente generare	**system health alert definition show -subsystem CIFS-NDO**
Criteri di monitoraggio dello stato CIFS-NDO, che determinano quando vengono generati gli avvisi	**system health policy definition show -monitor node-connect**

Utilizzare `-instance` per visualizzare informazioni dettagliate.

Esempi

Il seguente output mostra informazioni sullo stato di salute generale del cluster e del sottosistema CIFS-NDO:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

Il seguente output mostra informazioni dettagliate sulla configurazione e lo stato del monitor di stato del sottosistema CIFS-NDO:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
            Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verificare la configurazione della condivisione SMB continuamente disponibile

Per supportare operazioni senza interruzioni, le condivisioni SMB di Hyper-V e SQL Server devono essere configurate come condivisioni a disponibilità continua. Inoltre, è necessario controllare alcune altre impostazioni di condivisione. È necessario verificare che le condivisioni siano configurate correttamente per fornire operazioni senza interruzioni per i server di applicazioni in caso di eventi di interruzione pianificati o non pianificati.

A proposito di questa attività

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:

- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

Per operazioni corrette senza interruzioni, è necessario impostare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Fasi

1. Verificare che i file offline siano impostati su `manual` oppure `disabled` e che i link simbolici sono disabilitati:

   vserver cifs shares show -vserver *vserver_name*

2. Verificare che le condivisioni SMB siano configurate per la disponibilità continua:

   vserver cifs shares properties show -vserver *vserver_name*

Esempi

Nell'esempio seguente viene visualizzata l'impostazione di condivisione per una condivisione denominata "share1" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. I file offline sono impostati su `manual` i collegamenti simbolici e sono disattivati (indicati da un trattino in `Symlink Properties` output di campo):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Nell'esempio seguente vengono visualizzate le proprietà di condivisione di una condivisione denominata "share1" su SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Verificare lo stato LIF

Anche se si configurano le macchine virtuali di storage (SVM) con configurazioni Hyper-V e SQL Server su SMB in modo che dispongano di LIF su ciascun nodo di un cluster, durante le operazioni quotidiane, alcune LIF potrebbero spostarsi sulle porte di un altro nodo. È necessario verificare lo stato LIF e intraprendere le azioni correttive necessarie.

A proposito di questa attività

Per fornire un supporto operativo senza interruzioni, ciascun nodo di un cluster deve disporre di almeno una LIF per la SVM e tutte le LIF devono essere associate a una porta home. Se alcune delle LIF configurate non sono attualmente associate alla porta home, è necessario risolvere eventuali problemi di porta e ripristinare le LIF alla porta home.

Fasi

1. Visualizzare le informazioni sui LIF configurati per SVM:

   network interface show -vserver *vserver_name*

   In questo esempio, "lif1" non si trova sulla porta home.

`network interface show -vserver vs1`

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Ulteriori informazioni su `network interface show` nella "Riferimento al comando ONTAP".

2. Se alcune delle LIF non si trovano sulle porte home, attenersi alla seguente procedura:

   a. Per ogni LIF, determinare quale sia la porta home di LIF:

   network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

   network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

   ```
   vserver lif  home-node  home-port
   ------- ---- ---------- ---------
   vs1     lif1 node1      e0d
   ```

   b. Per ciascun LIF, determinare se la porta home del LIF è attiva:

   network port show -node *node_name* -port *port* -fields port,link

   `network port show -node node1 -port e0d -fields port,link`

   ```
   node       port link
   ---------- ---- ----
   node1      e0d  up
   ```

   In questo esempio, “lif1” deve essere nuovamente migrato alla porta home, `node1:e0d`.

   Ulteriori informazioni su `network port show` nella "Riferimento al comando ONTAP".

3. Se una delle interfacce di rete della porta home a cui devono essere associate le LIF non è nello `up` stato, risolvere il problema in modo che siano attive. Ulteriori informazioni su `up` nella "Riferimento al comando ONTAP".

4. Se necessario, ripristinare le LIF alle porte home:

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Ulteriori informazioni su `network interface revert` nella "Riferimento al comando ONTAP".

5. Verificare che ciascun nodo del cluster disponga di una LIF attiva per SVM:

   network interface show -vserver *vserver_name*

   network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determinare se le sessioni SMB sono continuamente disponibili

Visualizzare le informazioni sulla sessione SMB

È possibile visualizzare informazioni sulle sessioni SMB stabilite, tra cui la connessione SMB, l'ID della sessione e l'indirizzo IP della workstation che utilizza la sessione. È possibile visualizzare informazioni sulla versione del protocollo SMB della sessione e sul livello di protezione continuamente disponibile, per identificare se la sessione supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare le informazioni relative a tutte le sessioni della SVM in forma di riepilogo. Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali:

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output relativo ai campi scelti.

  È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sulle sessioni SMB stabilite.
- È possibile utilizzare `-fields` o il `-instance` parametro da solo o in combinazione con altri parametri opzionali.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le informazioni sulla sessione SMB…	**Immettere il seguente comando…**
Per tutte le sessioni su SVM in forma di riepilogo	**vserver cifs session show -vserver *vserver_name***
Su un ID di connessione specificato	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
Da un indirizzo IP della workstation specificato	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Su un indirizzo IP LIF specificato	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Su un nodo specificato	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	Da un utente Windows specificato
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Il formato per `user_name` è `[domain]\user`.	Con un meccanismo di autenticazione specificato

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
`vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism` Il valore per `-auth -mechanism` può essere uno dei seguenti: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Con una versione del protocollo specificata

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` Il valore per `-protocol-version` può essere uno dei seguenti: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Con un livello specifico di protezione a disponibilità continua

Se si desidera visualizzare le informazioni sulla sessione SMB…	Immettere il seguente comando…
`vserver cifs session show -vserver` ***`vserver_name`*** **`-continuously -available`** ***`continuously_available_protection_level`*** Il valore per `-continuously -available` può essere uno dei seguenti: • `No` • `Yes` • `Partial`	Con uno stato di sessione SMB Signing specificato

Esempi

Il seguente comando visualizza le informazioni sulla sessione per le sessioni su SVM vs1 stabilite da una workstation con indirizzo IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

almeno un file aperto a disponibilit

Il seguente comando visualizza informazioni dettagliate sulla sessione per le sessioni con protezione continuamente disponibile su SVM vs1. La connessione è stata effettuata utilizzando l'account di dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

aperti con una protezione continuam ente disponibile .

Il seguente comando visualizza le informazioni di sessione su una sessione che utilizza SMB 3.0 e SMB Multichannel su SVM vs1. Nell'esempio, l'utente si è connesso a questa condivisione da un client SMB 3.0 utilizzando l'indirizzo IP LIF; pertanto, il meccanismo di autenticazione è stato impostato su NTLMv2 per impostazione predefinita. La connessione deve essere effettuata utilizzando l'autenticazione Kerberos per

connettersi con la protezione continuamente disponibile.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
           Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Visualizza le informazioni sui file SMB aperti in ONTAP

È possibile visualizzare informazioni sui file SMB aperti, tra cui la connessione SMB e l'ID sessione, il volume di hosting, il nome della condivisione e il percorso di condivisione. È inoltre possibile visualizzare informazioni sul livello di protezione continuamente disponibile di un file, utile per determinare se un file aperto si trova in uno stato che supporta operazioni senza interruzioni.

A proposito di questa attività

È possibile visualizzare informazioni sui file aperti in una sessione SMB stabilita. Le informazioni visualizzate sono utili quando è necessario determinare le informazioni della sessione SMB per determinati file all'interno di una sessione SMB.

Ad esempio, se si dispone di una sessione SMB in cui alcuni dei file aperti sono aperti con una protezione continuamente disponibile e alcuni non sono aperti con una protezione continuamente disponibile (il valore per `-continuously-available` campo in `vserver cifs session show` l'output del comando è `Partial`), è possibile determinare quali file non sono continuamente disponibili utilizzando questo comando.

È possibile visualizzare le informazioni relative a tutti i file aperti nelle sessioni SMB stabilite sulle macchine virtuali di storage (SVM) in forma riepilogativa utilizzando `vserver cifs session file show` senza parametri opzionali.

Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Ciò può essere utile quando si desidera visualizzare informazioni solo per un piccolo sottoinsieme di file aperti.

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output nei campi scelti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sui file SMB aperti.

  È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
Sul modulo SVM in forma di riepilogo	**vserver cifs session file show -vserver *vserver_name***
Su un nodo specificato	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Su un ID file specificato
vserver cifs session file show -vserver *vserver_name* -file-id integer	Su un ID connessione SMB specificato
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Su un ID sessione SMB specificato
vserver cifs session file show -vserver *vserver_name* -session-id integer	Sull'aggregato di hosting specificato
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Sul volume specificato
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	Sulla condivisione SMB specificata
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Sul percorso SMB specificato

Se si desidera visualizzare i file SMB aperti…	Immettere il seguente comando…
vserver cifs session file show -vserver *vserver_name* -path *path*	Con il livello specificato di protezione a disponibilità continua
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* Il valore per `-continuously-available` può essere uno dei seguenti: • `No` • `Yes` Se lo stato di disponibilità continua è `No`, questo significa che questi file aperti non sono in grado di eseguire il ripristino senza interruzioni dal takeover e dal giveback. Inoltre, non possono essere ripristinati dal trasferimento generale di aggregati tra partner in una relazione ad alta disponibilità.	Con lo stato di riconnessione specificato

Sono disponibili ulteriori parametri opzionali che è possibile utilizzare per perfezionare i risultati di output. Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "Riferimento al comando ONTAP".

Esempi

Nell'esempio seguente vengono visualizzate informazioni sui file aperti su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sui file SMB aperti con ID file 82 su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informazioni sul copyright

Informazioni sul marchio commerciale