Configuração SMB para Microsoft Hyper-V e SQL Server

ONTAP 9

NetApp
January 17, 2025

Índice

Configuração SMB para Microsoft Hyper-V e SQL Server

Descrição geral da configuração SMB para Microsoft Hyper-V e SQL Server

Os recursos do ONTAP permitem que você ative operações ininterruptas para duas aplicações Microsoft através do protocolo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Use esses procedimentos se quiser implementar operações ininterruptas SMB nas seguintes circunstâncias:

- O acesso básico ao ficheiro de protocolo SMB foi configurado.
- Você deseja habilitar compartilhamentos de arquivo SMB 3,0 ou posteriores residentes em SVMs para armazenar os seguintes objetos:
  - Arquivos de máquina virtual Hyper-V.
  - Bancos de dados do sistema do SQL Server

Informações relacionadas

Para obter informações adicionais sobre a tecnologia ONTAP e a interação com serviços externos, consulte estes relatórios técnicos (TRs): "Relatório técnico da NetApp 4172: Microsoft Hyper-V sobre SMB 3,0 com práticas recomendadas da ONTAP" ** "Relatório técnico do NetApp 4369: Práticas recomendadas para Microsoft SQL Server e SnapManager 7,2 para SQL Server com Clustered Data ONTAP"

Configure o ONTAP para as soluções Microsoft Hyper-V e SQL Server em SMB

Você pode usar compartilhamentos de arquivos SMB 3,0 e posteriores disponíveis continuamente para armazenar arquivos de máquina virtual Hyper-V ou bancos de dados de sistema SQL Server e bancos de dados de usuários em volumes residentes em SVMs, ao mesmo tempo em que fornece operações ininterruptas (NDOs) para eventos planejados e não planejados.

Microsoft Hyper-V sobre SMB

Para criar uma solução Hyper-V sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de armazenamento para servidores Microsoft Hyper-V. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster), servidores Hyper-V, conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS e, opcionalmente, serviços de backup para proteger os arquivos de máquina virtual armazenados em volumes SVM.

> Os servidores Hyper-V devem ser configurados no Windows 2012 Server ou posterior. As configurações de servidor Hyper-V independentes e em cluster são suportadas.

- Para obter informações sobre como criar clusters da Microsoft e servidores Hyper-V, consulte o site da Microsoft.

- O SnapManager para Hyper-V é uma aplicação baseada em host que facilita os serviços de backup rápidos baseados em cópia Snapshot, projetados para se integrar às configurações do Hyper-V em SMB.

  Para obter informações sobre como usar o SnapManager com Hyper-V em configurações SMB, consulte *SnapManager para Guia de Instalação e Administração do Hyper-V*.

Microsoft SQL Server sobre SMB

Para criar uma solução SQL Server sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de storage para a aplicação Microsoft SQL Server. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster). Em seguida, você instalaria e configuraria o SQL Server nos servidores Windows e criaria conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS. Opcionalmente, você pode configurar serviços de backup para proteger os arquivos de banco de dados armazenados em volumes SVM.

> O SQL Server deve ser instalado e configurado no Windows 2012 Server ou posterior. Configurações autônomas e em cluster são compatíveis.

- Para obter informações sobre como criar clusters da Microsoft e instalar e configurar o SQL Server, consulte o site da Microsoft.
- O plug-in do SnapCenter para Microsoft SQL Server é uma aplicação baseada em host que facilita serviços de backup rápidos e baseados em cópias snapshot, projetados para serem integrados a configurações do SQL Server em SMB.

  Para obter informações sobre como usar o plug-in do SnapCenter para Microsoft SQL Server, consulte o "Plug-in do SnapCenter para Microsoft SQL Server" documento.

Operações ininterruptas para Hyper-V e SQL Server em SMB

O que significam operações ininterruptas para Hyper-V e SQL Server em SMB

Operações ininterruptas para Hyper-V e SQL Server sobre SMB referem-se à combinação de funcionalidades que permitem que os servidores de aplicações e as máquinas virtuais ou bancos de dados contidos permaneçam on-line e forneçam disponibilidade contínua durante muitas tarefas administrativas. Isso inclui tempo de inatividade planejado e não planejado da infraestrutura de storage.

Operações ininterruptas compatíveis para servidores de aplicações em SMB incluem o seguinte:

- Takeover planejado e giveback
- Takeover não planejado
- Atualização
- Realocação de agregados planejada (ARL)
- Migração de LIF e failover
- Movimentação de volume planejada

Protocolos que permitem operações ininterruptas em SMB

Juntamente com o lançamento do SMB 3,0, a Microsoft lançou novos protocolos para fornecer os recursos necessários para dar suporte a operações ininterruptas para Hyper-V e SQL Server sobre SMB.

A ONTAP usa esses protocolos ao fornecer operações ininterruptas para servidores de aplicações em SMB:

- SMB 3,0
- Testemunha

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Há certos conceitos sobre operações ininterruptas (NDOs) que você deve entender antes de configurar sua solução Hyper-V ou SQL Server sobre SMB.

- **Partilha continuamente disponível**

  Um compartilhamento SMB 3,0 que tem o conjunto de propriedades de compartilhamento continuamente disponível. Os clientes que se conetam por meio de compartilhamentos disponíveis continuamente podem sobreviver a eventos disruptivos, como aquisição, giveback e realocação agregada.

- **Nó**

  Um único controlador que é membro de um cluster. Para distinguir entre os dois nós em um par de SFO, um nó é às vezes chamado de *nó local* e o outro nó é às vezes chamado de *nó parceiro* ou *nó remoto*. O principal proprietário do storage é o nó local. O proprietário secundário, que controla o storage quando o proprietário principal falha, é o nó do parceiro. Cada nó é o principal proprietário do storage e o proprietário secundário do storage do parceiro.

- * Realocação de agregados sem interrupções*

  Capacidade de mover um agregado entre nós de parceiros dentro de um par de SFO em um cluster sem interromper as aplicações de clientes.

- **Failover sem interrupções**

  Veja *Takeover*.

- **Migração de LIF sem interrupções**

  A capacidade de realizar uma migração de LIF sem interromper aplicativos clientes conectados ao cluster por meio desse LIF. Para conexões SMB, isso só é possível para clientes que se conetam usando SMB 2,0 ou posterior.

- **Operações ininterruptas**

  Capacidade de executar grandes operações de gerenciamento e atualização do ONTAP, bem como resistir a falhas de nós sem interromper as aplicações dos clientes. Esse termo se refere à coleção de funcionalidades de aquisição sem interrupções, atualização sem interrupções e migração sem interrupções como um todo.

- **Atualização sem interrupções**

  Capacidade de atualizar o hardware ou o software do nó sem interrupção da aplicação.

- * Movimento de volume sem interrupções*

  Capacidade de mover um volume livremente pelo cluster sem interromper as aplicações que estão usando o volume. Para conexões SMB, todas as versões do SMB são compatíveis com movimentos de volume sem interrupções.

- * Alças persistentes*

  Uma propriedade do SMB 3,0 que permite que conexões continuamente disponíveis se reconetem de forma transparente ao servidor CIFS em caso de desconexão. Semelhante aos manipuladores duráveis, os manipuladores persistentes são mantidos pelo servidor CIFS por um período de tempo após a perda da comunicação com o cliente de conexão. No entanto, alças persistentes têm mais resiliência do que alças duráveis. Além de dar ao cliente a chance de recuperar o identificador dentro de uma janela de 60 segundos após a reconexão, o servidor CIFS nega acesso a quaisquer outros clientes que solicitem acesso ao arquivo durante essa janela de 60 segundos.

  As informações sobre alças persistentes são espelhadas no armazenamento persistente do parceiro SFO, o que permite que os clientes com alças persistentes desconetadas recuperem as alças duráveis após um evento em que o parceiro SFO assuma a propriedade do armazenamento do nó. Além de fornecer operações ininterruptas no caso de mudanças de LIF (que são duráveis lidar com o suporte), as alças persistentes fornecem operações ininterruptas para takeover, giveback e realocação de agregados.

- **SFO**

  Retorno de agregados para seus locais de origem ao se recuperar de um evento de aquisição.

- **Par SFO**

  Um par de nós cujos controladores estão configurados para servir dados entre si se um dos dois nós deixar de funcionar. Dependendo do modelo do sistema, ambos os controladores podem estar em um único chassi ou os controladores podem estar em um chassi separado. Conhecido como um par de HA em um cluster de dois nós.

- **Aquisição**

  O processo pelo qual o parceiro assume o controle do storage quando o proprietário principal desse storage falha. No contexto de SFO, failover e aquisição são sinônimos.

Como a funcionalidade SMB 3,0 dá suporte a operações ininterruptas por compartilhamentos SMB

O SMB 3,0 fornece funcionalidade crucial que permite o suporte a operações ininterruptas para compartilhamentos Hyper-V e SQL Server em SMB. Isso inclui a `continuously-available` propriedade compartilhar e um tipo de identificador de arquivo conhecido como *identificador persistente* que permite que os clientes SMB recuperem o estado aberto do arquivo e restabeleçam conexões SMB de forma transparente.

Identificadores persistentes podem ser concedidos a clientes compatíveis com SMB 3,0 que se conetam a um

compartilhamento com o conjunto de propriedades de compartilhamento continuamente disponível. Se a sessão SMB for desconetada, o servidor CIFS retém informações sobre o estado de identificador persistente. O servidor CIFS bloqueia outras solicitações de cliente durante o período de 60 segundos em que o cliente pode se reconetar, permitindo assim que o cliente com o identificador persistente recupere o identificador após uma desconexão da rede. Os clientes com alças persistentes podem se reconetar usando uma das LIFs de dados na máquina virtual de storage (SVM), seja reconetando pelo mesmo LIF ou por meio de um LIF diferente.

A realocação agregada, a aquisição e a giveback ocorrem entre pares de SFO. Para gerenciar de forma otimizada a desconexão e a reconexão de sessões com arquivos com alças persistentes, o nó do parceiro mantém uma cópia de todas as informações de bloqueio de identificador persistente. Independentemente de o evento ser planejado ou não planejado, o parceiro SFO pode gerenciar as reconexões de identificador persistente sem interrupções. Com essa nova funcionalidade, as conexões SMB 3,0 ao servidor CIFS podem fazer failover de forma transparente e sem interrupções para outro LIF de dados atribuído à SVM em eventos que tradicionalmente têm sido disruptivos.

Embora o uso de alças persistentes permita que o servidor CIFS faça failover transparente em conexões SMB 3,0, se uma falha fizer com que o aplicativo Hyper-V faça failover para outro nó no cluster do Windows Server, o cliente não terá como recuperar as alças de arquivo dessas alças desconetadas. Nesse cenário, os manipuladores de arquivos no estado desconetado podem potencialmente bloquear o acesso do aplicativo Hyper-V se ele for reiniciado em um nó diferente. "'Cluster de failover'" é uma parte do SMB 3,0 que aborda esse cenário fornecendo um mecanismo para invalidar manipulações obsoletas e conflitantes. Usando esse mecanismo, um cluster Hyper-V pode se recuperar rapidamente quando os nós de cluster Hyper-V falham.

O que o protocolo Witness faz para melhorar o failover transparente

O protocolo Witness fornece recursos aprimorados de failover de cliente para compartilhamentos continuamente disponíveis (compartilhamentos CA) SMB 3,0. O Witness facilita o failover mais rápido porque ignora o período de recuperação de failover de LIF. Ele notifica os servidores de aplicativos quando um nó não está disponível sem a necessidade de esperar que a conexão SMB 3,0 expire.

O failover é contínuo, com as aplicações em execução no cliente não cientes de que ocorreu um failover. Se a testemunha não estiver disponível, as operações de failover ainda ocorrem com sucesso, mas o failover sem testemunha é menos eficiente.

O failover aprimorado de testemunhas é possível quando os seguintes requisitos são atendidos:

- Ele só pode ser usado com servidores CIFS compatíveis com SMB 3,0 que tenham SMB 3,0 habilitado.
- Os compartilhamentos devem usar o SMB 3,0 com o conjunto de propriedades de compartilhamento de disponibilidade contínua.
- O parceiro SFO do nó ao qual os servidores de aplicativos estão conetados deve ter pelo menos um LIF de dados operacional atribuído à máquina virtual de armazenamento (SVM) que hospeda dados para os servidores de aplicativos.

O protocolo testemunha opera entre pares SFO. Como os LIFs podem migrar para qualquer nó dentro do cluster, qualquer nó pode precisar ser a testemunha de seu parceiro SFO. O protocolo Witness não pode fornecer failover rápido de conexões SMB em um determinado nó se os dados de hospedagem SVM para os servidores de aplicações não tiverem um LIF de dados ativo no nó de parceiro. Portanto, cada nó no cluster precisa ter pelo menos um data LIF para cada SVM que hospeda uma dessas configurações.

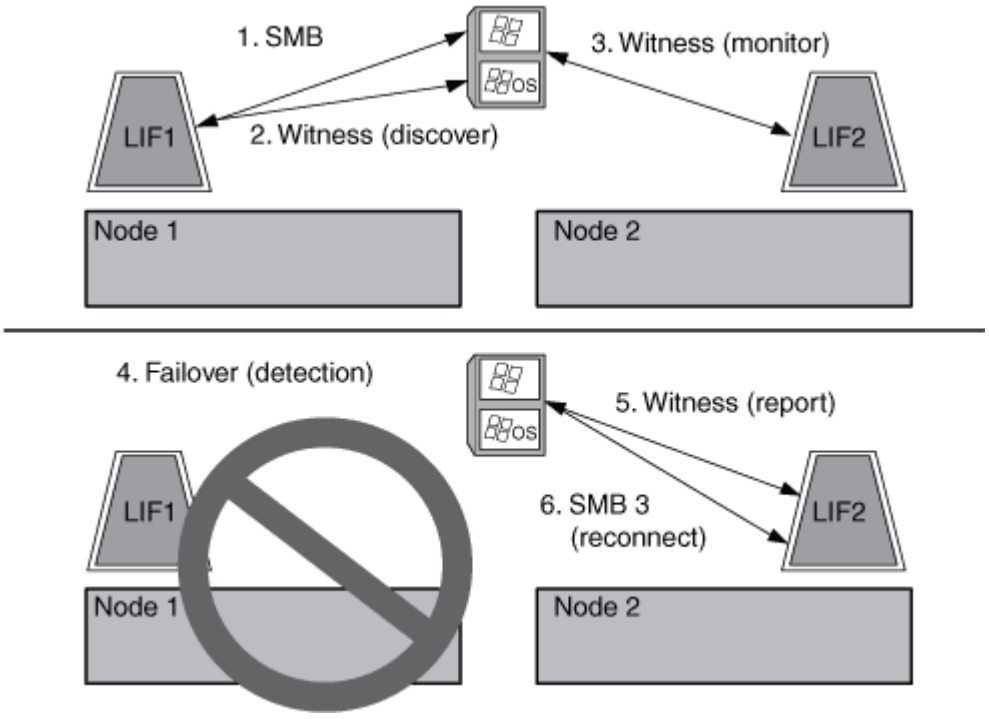
- Os servidores de aplicativos devem se conetar ao servidor CIFS usando o nome do servidor CIFS que é armazenado no DNS em vez de usando endereços IP de LIF individuais.

Como funciona o protocolo testemunha

O ONTAP implementa o protocolo Witness usando o parceiro SFO de um nó como testemunha. Em caso de falha, o parceiro deteta rapidamente a falha e notifica o cliente SMB.

O protocolo Witness fornece failover aprimorado usando o seguinte processo:

1. Quando o servidor de aplicativos estabelece uma conexão SMB continuamente disponível ao Node1, o servidor CIFS informa ao servidor de aplicativos que a testemunha está disponível.
2. O servidor do aplicativo solicita os endereços IP do servidor testemunha de Node1 e recebe uma lista de Node2 (o parceiro SFO) endereços IP de LIF de dados atribuídos à máquina virtual de armazenamento (SVM).
3. O servidor de aplicativos escolhe um dos endereços IP, cria uma conexão testemunha com o Node2 e se Registra para ser notificado se a conexão continuamente disponível no Node1 precisar se mover.
4. Se um evento de failover ocorrer no Node1, o Witness facilita os eventos de failover, mas não está envolvido com a giveback.
5. O Witness deteta o evento de failover e notifica o servidor de aplicativos por meio da conexão Witness que a conexão SMB deve ser movida para Node2.
6. O servidor de aplicativos move a sessão SMB para Node2 e recupera a conexão sem interrupção ao acesso do cliente.



Backups baseados em compartilhamento com VSS remoto

Backups baseados em compartilhamento com a visão geral do VSS remoto

Você pode usar o VSS remoto para executar backups baseados em compartilhamento de arquivos de máquina virtual Hyper-V armazenados em um servidor CIFS.

Microsoft Remote VSS (volume Shadow Copy Services) é uma extensão da infraestrutura Microsoft VSS existente. Com o VSS remoto, a Microsoft estendeu a infraestrutura VSS para dar suporte à cópia sombra de compartilhamentos SMB. Além disso, aplicativos de servidor, como o Hyper-V, podem armazenar arquivos VHD em compartilhamentos de arquivos SMB. Com essas extensões, é possível fazer cópias de sombra consistentes de aplicativos para máquinas virtuais que armazenam dados e arquivos de configuração em compartilhamentos.

Conceitos VSS remotos

Você deve estar ciente de certos conceitos que são necessários para entender como o VSS remoto (volume Shadow Copy Service) é usado por serviços de backup com configurações Hyper-V em SMB.

- **VSS (Serviço de cópia sombra de volume)**

  Uma tecnologia da Microsoft usada para fazer cópias de backup ou snapshots de dados em um volume específico em um determinado momento. O VSS coordena entre servidores de dados, aplicações de backup e software de gerenciamento de storage para dar suporte à criação e gerenciamento de backups consistentes.

- * VSS remoto (Serviço de cópia de sombra de volume remoto)*

  Uma tecnologia da Microsoft usada para fazer cópias de backup baseadas em compartilhamento de dados que estão em um estado consistente com dados em um momento específico em que os dados são acessados por compartilhamentos SMB 3,0. Também conhecido como *volume Shadow Copy Service*.

- **Cópia sombra**

  Um conjunto duplicado de dados contidos no compartilhamento em um instante bem definido no tempo. As cópias de sombra são usadas para criar backups consistentes de dados pontuais, permitindo que o sistema ou as aplicações continuem atualizando os dados nos volumes originais.

- * Conjunto de cópias de sombra*

  Uma coleção de uma ou mais cópias de sombra, com cada cópia de sombra correspondente a um compartilhamento. As cópias de sombra dentro de um conjunto de cópias de sombra representam todos os compartilhamentos que precisam ser copiados na mesma operação. O cliente VSS no aplicativo habilitado para VSS identifica quais cópias de sombra incluir no conjunto.

- * Recuperação automática do conjunto de cópias sombra*

  A parte do processo de backup para aplicativos de backup remotos habilitados para VSS, em que o diretório de réplica que contém as cópias sombra é consistente ponto no tempo. No início do backup, o cliente VSS no aplicativo aciona o aplicativo para fazer pontos de verificação de software sobre os dados programados para backup (os arquivos de máquina virtual no caso do Hyper-V). Em seguida, o cliente VSS permite que os aplicativos continuem. Depois que o conjunto de cópias de sombra é criado, o VSS remoto torna o conjunto de cópias de sombra gravável e expõe a cópia gravável para os aplicativos. O aplicativo prepara o conjunto de cópias de sombra para backup executando uma recuperação automática usando o ponto de verificação de software feito anteriormente. A recuperação automática traz as cópias

de sombra para um estado consistente, desrolando as alterações feitas nos arquivos e diretórios desde que o ponto de verificação foi criado. A recuperação automática é uma etapa opcional para backups habilitados para VSS.

- **ID de cópia sombra**

  Um GUID que identifica exclusivamente uma cópia de sombra.

- **ID do conjunto de cópias sombra**

  Um GUID que identifica exclusivamente uma coleção de IDs de cópia de sombra para o mesmo servidor.

- **SnapManager para Hyper-V**

  O software que automatiza e simplifica as operações de backup e restauração para o Microsoft Windows Server 2012 Hyper-V. o SnapManager para Hyper-V usa o VSS remoto com recuperação automática para fazer backup de arquivos Hyper-V em compartilhamentos SMB.

Informações relacionadas

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Backups baseados em compartilhamento com VSS remoto

Exemplo de uma estrutura de diretório usada pelo VSS remoto

O VSS remoto percorre a estrutura de diretórios que armazena arquivos de máquina virtual Hyper-V enquanto cria cópias de sombra. É importante entender o que é uma estrutura de diretório apropriada, para que você possa criar com sucesso backups de arquivos de máquina virtual.

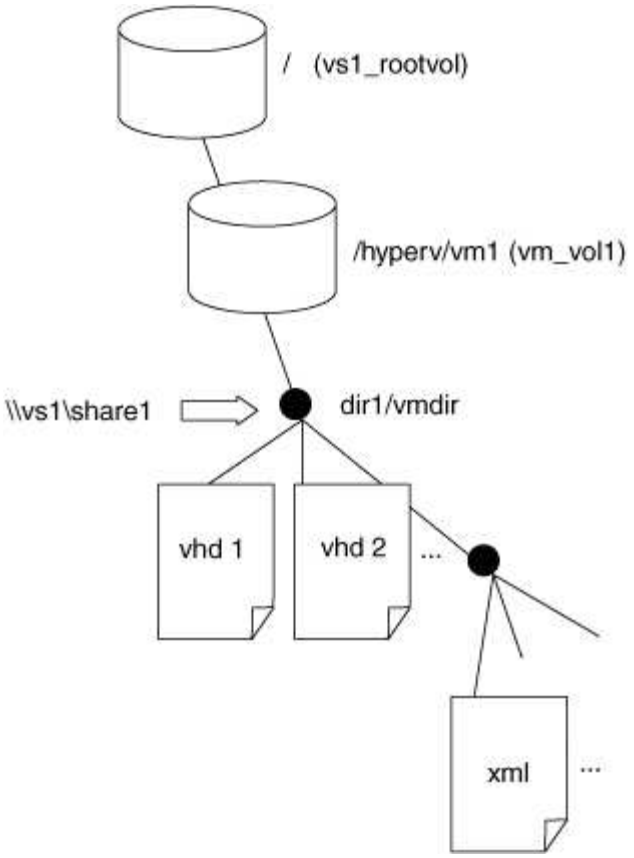
Uma estrutura de diretório suportada para a criação bem-sucedida de cópias sombra está em conformidade com os seguintes requisitos:

- Somente diretórios e arquivos regulares estão presentes dentro da estrutura de diretórios que é usada para armazenar arquivos de máquina virtual.

  A estrutura de diretórios não contém junções, links ou arquivos não regulares.

- Todos os arquivos de uma máquina virtual residem em um único compartilhamento.
- A estrutura de diretórios que é usada para armazenar arquivos de máquina virtual não excede a profundidade configurada do diretório de cópia de sombra.
- O diretório raiz do compartilhamento contém apenas arquivos ou diretórios de máquina virtual.

Na ilustração a seguir, o volume chamado VM_vol1 é criado com um ponto de junção em `/hyperv/vm1` na máquina virtual de armazenamento (SVM) VS1. Subdiretórios para conter os arquivos da máquina virtual são criados sob o ponto de junção. Os arquivos de máquina virtual do servidor Hyper-V são acessados em share1 que tem o `/hyperv/vm1/dir1/vmdir` caminho . O serviço de cópia de sombra cria cópias de sombra de todos os arquivos de máquina virtual que estão contidos na estrutura de diretórios sob share1 (até a profundidade configurada do diretório de cópia de sombra).



Como o SnapManager para Hyper-V gerencia backups remotos baseados em VSS para Hyper-V em SMB

Você pode usar o SnapManager para Hyper-V para gerenciar serviços de backup baseados em VSS remoto. Há benefícios de usar o serviço de backup gerenciado do SnapManager para Hyper-V para criar conjuntos de backup com uso eficiente de espaço.

As otimizações para o SnapManager para backups gerenciados do Hyper-V incluem o seguinte:

- A integração do SnapDrive com o ONTAP oferece otimização de performance ao descobrir o local de compartilhamento SMB.

  O ONTAP fornece ao SnapDrive o nome do volume em que o compartilhamento reside.

- O SnapManager para Hyper-V especifica a lista de arquivos de máquina virtual nos compartilhamentos SMB que o serviço de cópia sombra precisa copiar.

  Ao fornecer uma lista segmentada de arquivos de máquina virtual, o serviço de cópia de sombra não precisa criar cópias de sombra de todos os arquivos no compartilhamento.

- A máquina virtual de storage (SVM) retém as cópias Snapshot do SnapManager para Hyper-V a serem usadas para restaurações.

  Não há fase de backup. O backup é a cópia Snapshot com uso eficiente de espaço.

O SnapManager para Hyper-V fornece recursos de backup e restauração para o HyperV em SMB usando o

seguinte processo:

1. Preparação para a operação de cópia de sombra

   O cliente VSS do aplicativo SnapManager para Hyper-V configura o conjunto de cópias de sombra. O cliente VSS reúne informações sobre quais compartilhamentos incluir no conjunto de cópias de sombra e fornece essas informações ao ONTAP. Um conjunto pode conter uma ou mais cópias de sombra, e uma cópia de sombra corresponde a um compartilhamento.

2. Criando o conjunto de cópias de sombra (se a recuperação automática for usada)

   Para cada compartilhamento incluído no conjunto de cópias de sombra, o ONTAP cria uma cópia de sombra e torna a cópia de sombra gravável.

3. Expondo o conjunto de cópias de sombra

   Depois que o ONTAP cria as cópias de sombra, elas são expostas ao SnapManager para Hyper-V para que os escritores VSS do aplicativo possam executar a recuperação automática.

4. Recuperar automaticamente o conjunto de cópias de sombra

   Durante a criação do conjunto de cópias de sombra, há um período de tempo em que as alterações ativas estão ocorrendo nos arquivos incluídos no conjunto de backup. Os escritores VSS do aplicativo devem atualizar as cópias sombra para garantir que estejam em um estado completamente consistente antes do backup.

   > A forma como a recuperação automática é feita é específica da aplicação. VSS remoto não está envolvido nesta fase.

5. Completar e limpar o conjunto de cópias de sombra

   O cliente VSS notifica o ONTAP após concluir a recuperação automática. O conjunto de cópias de sombra é feito somente leitura e, em seguida, está pronto para backup. Ao usar o SnapManager para Hyper-V para backup, os arquivos em uma cópia Snapshot tornam-se o backup; portanto, para a fase de backup, uma cópia Snapshot é criada para cada volume que contém compartilhamentos no conjunto de backup. Após a conclusão do backup, o conjunto de cópias de sombra é removido do servidor CIFS.

Como a descarga de cópia ODX é usada com Hyper-V e SQL Server em compartilhamentos SMB

A transferência de dados descarregados (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host. A descarga de cópia ODX da ONTAP fornece benefícios de desempenho ao executar operações de cópia no servidor de aplicações através da instalação SMB.

Em transferências de arquivos não ODX, os dados são lidos do servidor CIFS de origem e são transferidos através da rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o servidor CIFS de destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e

destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:
```

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e mesma máquina virtual de storage (SVM)

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

Casos de uso específicos para descarga de cópia ODX com soluções Hyper-V incluem o seguinte:

- Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

  Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

> ⓘ Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Casos de uso específicos para descarga de cópia ODX com soluções SQL Server incluem o seguinte:

- Você pode usar a descarga de cópia ODX para exportar e importar bancos de dados SQL Server entre compartilhamentos SMB mapeados ou entre compartilhamentos SMB e LUNs iSCSI conetados no mesmo cluster.
- A descarga de cópia ODX é usada para exportações e importações de banco de dados se o armazenamento de origem e destino estiver no mesmo cluster.

Requisitos e considerações de configuração

Requisitos de ONTAP e licenciamento

Você precisa estar ciente de certos requisitos de licenciamento e ONTAP ao criar soluções SQL Server ou Hyper-V em SMB para operações ininterruptas em SVMs.

Requisitos de versão do ONTAP

- Hyper-V em SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para Hyper-V executados no Windows 2012 ou posterior.

- SQL Server sobre SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para SQL Server 2012 ou posterior executados no Windows 2012 ou posterior.

Para obter as informações mais recentes sobre versões com suporte do ONTAP, Windows Server e SQL Server para operações ininterruptas em compartilhamentos SMB, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de licenciamento

São necessárias as seguintes licenças:

- CIFS
- FlexClone (somente para Hyper-V em SMB)

  Esta licença é necessária se o VSS remoto for usado para backups. O serviço de cópia de sombra usa o FlexClone para criar cópias pontuais de arquivos que são então usados ao criar um backup.

  Uma licença do FlexClone é opcional se você usar um método de backup que não use o VSS remoto.

A licença FlexClone está incluída no "ONTAP One". Se não tiver o ONTAP One, deverá "verifique se as licenças necessárias estão instaladas", e, se necessário"instale-os", .

Requisitos de LIF de rede e dados

Você precisa estar ciente de certos requisitos de rede e de LIF de dados ao criar configurações do SQL Server ou Hyper-V em SMB para operações ininterruptas).

Requisitos de protocolo de rede

- São suportadas redes IPv4G e IPv6G.
- SMB 3,0 ou posterior é necessário.

  O SMB 3,0 fornece a funcionalidade necessária para criar as conexões SMB continuamente disponíveis necessárias para oferecer operações ininterruptas.

- Os servidores DNS devem conter entradas que mapeiam o nome do servidor CIFS para os endereços IP atribuídos aos LIFs de dados na máquina virtual de armazenamento (SVM).

  Os servidores de aplicativos Hyper-V ou SQL Server normalmente fazem várias conexões em várias LIFs de dados ao acessar arquivos de máquina virtual ou banco de dados. Para uma funcionalidade adequada, os servidores de aplicativos devem fazer essas várias conexões SMB usando o nome do servidor CIFS em vez de fazer várias conexões com vários endereços IP exclusivos.

  Witness também requer o uso do nome DNS do servidor CIFS em vez de endereços IP LIF individuais.

  A partir do ONTAP 9.4, você pode melhorar a taxa de transferência e a tolerância a falhas para as configurações Hyper-V e SQL Server em SMB, ativando o Multichannel SMB. Para fazer isso, você deve ter várias NICs de 1G, 10G ou maiores implantados no cluster e nos clientes.

Requisitos de LIF de dados

- O SVM que hospeda a solução de servidor de aplicações em SMB precisa ter pelo menos um LIF de dados operacionais em cada nó do cluster.

  Os LIFs de dados do SVM podem fazer failover para outras portas de dados no cluster, incluindo nós que não estão hospedando dados acessados pelos servidores de aplicações. Além disso, como o nó testemunha é sempre o parceiro SFO de um nó ao qual o servidor de aplicativos está conetado, cada nó no cluster é um nó de testemunha potencial.

- Os LIFs de dados não devem ser configurados para reverter automaticamente.

  Após um evento de aquisição ou giveback, você deve reverter manualmente os LIFs de dados para suas portas domésticas.

- Todos os endereços IP de LIF de dados devem ter uma entrada no DNS e todas as entradas devem ser resolvidas para o nome do servidor CIFS.

  Os servidores de aplicativos devem se conetar a compartilhamentos SMB usando o nome do servidor CIFS. Não configure os servidores de aplicativos para fazer conexões usando os endereços IP LIF.

- Se o nome do servidor CIFS for diferente do nome SVM, as entradas DNS deverão ser resolvidas para o nome do servidor CIFS.

Requisitos de volume e servidor SMB para Hyper-V em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações Hyper-V em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de máquina do Hyper-V, crie um SVM separado para esses dados.

- A autenticação Kerberos e NTLM devem ser permitidas no domínio ao qual o servidor SMB pertence.

  O ONTAP não anuncia o serviço Kerberos para VSS remoto; portanto, o domínio deve ser definido para permitir NTLM.

- A funcionalidade de cópia sombra deve estar ativada.

  Esta funcionalidade está ativada por predefinição.

- A conta de domínio do Windows que o serviço de cópia de sombra usa ao criar cópias de sombra deve ser membro do grupo de administradores locais do servidor SMB ou operadores de backup.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Para que as operações de cópia de sombra sejam bem-sucedidas, você precisa ter espaço disponível suficiente no volume.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

Informações relacionadas

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

Requisitos de volume e servidor SMB para SQL Server em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações do SQL Server em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

  Além disso, o SQL Server usa um usuário de domínio como a conta de serviço do SQL Server. A conta de serviço também deve ser mapeada para o usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de banco de dados do SQL Server, você deve criar um SVM separado para esses dados.

- A conta de usuário do Windows usada para instalar o SQL Server no ONTAP deve ser atribuída ao privilégio SeSecurityPrivilege.

  Este privilégio é atribuído ao grupo de administradores/BUILTIN local do servidor SMB.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que as operações de backup do SnapCenter Plug-in para Microsoft SQL Server sejam bem-sucedidas, você deve ter espaço disponível suficiente no volume.

  O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

Informações relacionadas

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

Requisitos e considerações de compartilhamento continuamente disponíveis para Hyper-V sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos disponíveis continuamente para configurações do Hyper-V em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Se você quiser usar serviços de backup habilitados para VSS remoto, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham junções.

  No caso de recuperação automática, a criação de cópia sombra falha se uma junção for encontrada ao atravessar o compartilhamento. No caso não auto-recuperação, a criação de cópia sombra não falha, mas a junção não aponta para nada.

- Se você quiser usar serviços de backup habilitados para VSS remoto com recuperação automática, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham o seguinte:
  - Links simbólicos, hardlinks ou widelinks
  - Arquivos não regulares

    A criação de cópia sombra falha se houver links ou arquivos não regulares na cópia compartilhar para sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

  - Para que as operações de cópia sombra tenham sucesso, você deve ter espaço disponível suficiente no volume (somente para Hyper-V sobre SMB).

    O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos

continuamente disponíveis usados pelos servidores de aplicativos:

- Diretório base
- Armazenamento em cache de atributos
- BranchCache

Considerações

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações Hyper-V em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` parâmetro definido como `Yes`.

Requisitos e considerações de compartilhamento continuamente disponíveis para SQL Server sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos continuamente disponíveis para configurações do SQL Server em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer operações ininterruptas para servidores de aplicações que usam conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Você não pode alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para operações ininterruptas em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para operações ininterruptas em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que o plug-in do SnapCenter para operações do Microsoft SQL Server seja bem-sucedido, você

deve ter espaço disponível suficiente no volume.

O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos continuamente disponíveis usados pelos servidores de aplicativos:
  - Diretório base
  - Armazenamento em cache de atributos
  - BranchCache

Considerações sobre compartilhamento

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações do SQL Server em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` conjunto de propriedades de compartilhamento.

Considerações sobre VSS remoto para configurações Hyper-V em SMB

Você precisa estar ciente de certas considerações ao usar soluções de backup habilitadas para VSS remotas para configurações Hyper-V sobre SMB.

Considerações gerais sobre o VSS remoto

- Um máximo de 64 compartilhamentos pode ser configurado por servidor de aplicativos da Microsoft.

  A operação de cópia de sombra falha se houver mais de 64 compartilhamentos em um conjunto de cópias de sombra. Este é um requisito da Microsoft.

- Apenas é permitido um conjunto de cópias de sombra ativo por servidor CIFS.

  Uma operação de cópia sombra falhará se houver uma operação de cópia sombra contínua no mesmo servidor CIFS. Este é um requisito da Microsoft.

- Nenhuma junção é permitida dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.
  - No caso de recuperação automática, a criação de cópia de sombra falhará se uma junção for encontrada ao atravessar o compartilhamento.
  - No caso de recuperação não automática, a criação de cópia sombra não falha, mas a junção não aponta para nada.

Considerações do VSS remoto que se aplicam somente a cópias de sombra com recuperação automática

Certos limites se aplicam apenas a cópias sombra com recuperação automática.

- Uma profundidade máxima de diretório de cinco subdiretórios é permitida para a criação de cópias de sombra.

  Esta é a profundidade do diretório sobre a qual o serviço de cópia sombra cria um conjunto de backup de cópia sombra. A criação de cópia de sombra falhará se os diretórios que contêm arquivo de máquina virtual estiverem aninhados mais profundamente do que cinco níveis. Isto destina-se a limitar a travessia de diretório ao clonar o compartilhamento. A profundidade máxima do diretório pode ser alterada usando uma opção de servidor CIFS.

- A quantidade de espaço disponível no volume deve ser adequada.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra.

- Não são permitidos links ou arquivos não regulares dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.

  A criação de cópia sombra falha se houver links ou arquivos não regulares no compartilhamento para a cópia sombra. O processo de clone não os suporta.

- Não são permitidas ACLs NFSv4 nos diretórios.

  Embora a criação de cópia sombra retenha NFSv4 ACLs em arquivos, as ACLs NFSv4 nos diretórios são perdidas.

- Um máximo de 60 segundos é permitido criar um conjunto de cópias de sombra.

  As especificações da Microsoft permitem um máximo de 60 segundos para criar o conjunto de cópias de sombra. Se o cliente VSS não puder criar o conjunto de cópias de sombra dentro desse tempo, a operação de cópia de sombra falhará; portanto, isso limita o número de arquivos em um conjunto de cópias de sombra. O número real de arquivos ou máquinas virtuais que podem ser incluídos em um conjunto de backup varia; esse número depende de muitos fatores e deve ser determinado para cada ambiente de cliente.

Requisitos de descarga de cópia ODX para SQL Server e Hyper-V sobre SMB

A descarga de cópia ODX deve ser ativada se você quiser migrar arquivos de máquina virtual ou exportar e importar arquivos de banco de dados diretamente da origem para o local de armazenamento de destino sem enviar dados através dos servidores de aplicativos. Há certos requisitos que você deve entender sobre o uso de descarga de cópia ODX com soluções SQL Server e Hyper-V sobre SMB.

O uso de descarga de cópia ODX proporciona um benefício significativo de desempenho. Esta opção de servidor CIFS está ativada por predefinição.

- O SMB 3,0 deve estar habilitado para usar a descarga de cópia ODX.
- Os volumes de origem devem ter no mínimo 1,25 GB.
- A deduplicação deve ser habilitada em volumes usados com descarga de cópia.
- Se você usar volumes compatados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

O tipo de compressão secundária não é suportado

- Para usar a descarga de cópia ODX para migrar convidados Hyper-V dentro e entre discos, os servidores Hyper-V devem ser configurados para usar discos SCSI.

  O padrão é configurar discos IDE, mas a descarga de cópia ODX não funciona quando os convidados são migrados se os discos são criados usando discos IDE.

Recomendações para configurações do SQL Server e Hyper-V em SMB

Para ter certeza de que as configurações do SQL Server e do Hyper-V sobre SMB são robustas e operacionais, você precisa estar familiarizado com as práticas recomendadas ao configurar as soluções.

Recomendações gerais

- Separe os arquivos do servidor de aplicativos dos dados gerais do usuário.

  Se possível, dedique uma máquina virtual de storage inteira (SVM) e seu armazenamento aos dados do servidor de aplicativos.

- Para obter o melhor desempenho, não ative a assinatura SMB em SVMs que são usadas para armazenar os dados do servidor de aplicativos.
- Para melhor desempenho e melhor tolerância a falhas, ative o multicanal SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB.
- Não crie compartilhamentos continuamente disponíveis em compartilhamentos diferentes daqueles usados na configuração Hyper-V ou SQL Server sobre SMB.
- Desative o Change Notify em compartilhamentos usados para disponibilidade contínua.
- Não realize uma movimentação de volume ao mesmo tempo que o ARL (Aggregate Relocation) porque o ARL tem fases que pausam algumas operações.
- Para soluções Hyper-V sobre SMB, use unidades iSCSI convidadas ao criar máquinas virtuais em cluster. Os arquivos compartilhados `.VHDX` não são compatíveis com Hyper-V em SMB em compartilhamentos SMB do ONTAP.

Planeje a configuração Hyper-V ou SQL Server em SMB

Conclua a Planilha de configuração de volume

A Planilha fornece uma maneira fácil de Registrar os valores de que você precisa ao criar volumes para configurações do SQL Server e do Hyper-V em SMB.

Para cada volume, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

  O nome do SVM é o mesmo para todos os volumes.

- Nome do volume
- Nome agregado

  É possível criar volumes em agregados localizados em qualquer nó do cluster.

- Tamanho
- Caminho de junção

Você deve ter em mente o seguinte ao criar volumes usados para armazenar dados do servidor de aplicativos:

- Se o volume raiz não tiver um estilo de segurança NTFS, deve especificar o estilo de segurança como NTFS quando criar o volume.

  Por padrão, os volumes herdam o estilo de segurança do volume raiz da SVM.

- Os volumes devem ser configurados com a garantia de espaço de volume padrão.
- Opcionalmente, você pode configurar a configuração de gerenciamento de espaço de dimensionamento automático.
- Você deve definir a opção que determina a reserva de espaço de cópia Snapshot como `0`.
- A política Snapshot aplicada ao volume deve ser desativada.

  Se a política SVM Snapshot estiver desativada, você não precisará especificar uma política de Snapshot para os volumes. Os volumes herdam a política Snapshot da SVM. Se a política Snapshot do SVM não estiver desativada e estiver configurada para criar cópias Snapshot, você precisará especificar uma política de Snapshot no nível de volume e essa política deverá ser desativada. Os backups habilitados para o serviço de cópia sombra e os backups do SQL Server gerenciam a criação e exclusão de cópias Snapshot.

- Não é possível configurar espelhos de compartilhamento de carga para os volumes.

Os caminhos de junção nos quais você planeja criar compartilhamentos que os servidores de aplicativos usam devem ser escolhidos para que não haja volumes juntados abaixo do ponto de entrada de compartilhamento.

Por exemplo, se você quiser armazenar arquivos de máquina virtual em quatro volumes denominados "'vol1"", "'vol2", "'vol3" e "'vol4"", você pode criar o namespace mostrado no exemplo. Em seguida, é possível criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/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
```

Tipos de informação	Valores
Volume 1: Nome do volume, agregado, tamanho, caminho de junção	
Volume 2: Nome do volume, agregado, tamanho, caminho de junção	
Volume 3: Nome do volume, agregado, tamanho, caminho de junção	
Volume 4: Nome do volume, agregado, tamanho, caminho de junção	
Volume 5: Nome do volume, agregado, tamanho, caminho de junção	
Volume 6: Nome do volume, agregado, tamanho, caminho de junção	
Volumes adicionais: Nome do volume, agregado, tamanho, caminho de junção	

Conclua a Planilha de configuração do compartilhamento SMB

Use esta Planilha para Registrar os valores de que você precisa ao criar compartilhamentos SMB continuamente disponíveis para configurações do SQL Server e do Hyper-V sobre SMB.

Informações sobre as propriedades de compartilhamentos SMB e configurações

Para cada compartilhamento, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

  O nome do SVM é o mesmo para todos os compartilhamentos

- Nome da partilha
- Caminho
- Compartilhar propriedades

  Você deve configurar as duas propriedades de compartilhamento a seguir:

  - `oplocks`
  - `continuously-available`

As seguintes propriedades de compartilhamento não devem ser definidas:

- `homedirectory attributecache`

- `branchcache`
- `access-based-enumeration`
  - Links simbólicos devem ser desativados (o valor para o `-symlink-properties` parâmetro deve ser nulo ["]).

Informações sobre caminhos de compartilhamento

Se você estiver usando o VSS remoto para fazer backup de arquivos Hyper-V, a escolha de caminhos de compartilhamento a serem usados ao fazer conexões SMB dos servidores Hyper-V para os locais de armazenamento onde os arquivos da máquina virtual são armazenados é importante. Embora os compartilhamentos possam ser criados em qualquer ponto do namespace, os caminhos para compartilhamentos que os servidores Hyper-V usam não devem conter volumes juntados. As operações de cópia sombra não podem ser executadas em caminhos de partilha que contenham pontos de junção.

O SQL Server não pode cruzar junções ao criar a estrutura do diretório do banco de dados. Você não deve criar caminhos de compartilhamento para o servidor SQL que contenham pontos de junção.

Por exemplo, dado o namespace mostrado, se você quiser armazenar arquivos de máquina virtual ou arquivos de banco de dados nos volumes "'vol1", "'vol2", "'vol3"" e "'vol4", você deve criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/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
```

Embora seja possível criar compartilhamentos `/data1` nos caminhos e `/data2` para gerenciamento administrativo, não configure os servidores de aplicativos para usar esses compartilhamentos para armazenar dados.

Folha de trabalho de planeamento

Tipos de informação	Valores
Volume 1: Nome e caminho do compartilhamento SMB	
Volume 2: Nome e caminho do compartilhamento SMB	

Tipos de informação	Valores
Volume 3: Nome e caminho do compartilhamento SMB	
Volume 4: Nome e caminho do compartilhamento SMB	
Volume 5: Nome e caminho do compartilhamento SMB	
Volume 6: Nome e caminho do compartilhamento SMB	
Volume 7: Nome e caminho do compartilhamento SMB	
Volumes adicionais: Nomes e caminhos de compartilhamento SMB	

Crie configurações de ONTAP para operações ininterruptas com Hyper-V e SQL Server em SMB

Crie configurações do ONTAP para operações ininterruptas com a visão geral do Hyper-V e do SQL Server sobre SMB

Há várias etapas de configuração do ONTAP que você deve executar para se preparar para instalações do Hyper-V e SQL Server que fornecem operações ininterruptas em SMB.

Antes de criar a configuração do ONTAP para operações ininterruptas com o Hyper-V e o SQL Server em SMB, as seguintes tarefas devem ser concluídas:

- Os serviços de tempo devem ser configurados no cluster.
- É necessário configurar uma rede para o SVM.
- É necessário criar o SVM.
- As interfaces de LIF de dados devem ser configuradas na SVM.
- O DNS deve ser configurado na SVM.
- Os serviços de nomes desejados devem ser configurados para o SVM.
- O servidor SMB deve ser criado.

Informações relacionadas

Planeje a configuração Hyper-V ou SQL Server em SMB

Requisitos e considerações de configuração

Verifique se a autenticação Kerberos e NTLMv2 são permitidas (Hyper-V sobre compartilhamentos SMB)

Operações ininterruptas para Hyper-V em SMB exigem que o servidor CIFS em um SVM de dados e o servidor Hyper-V permitam a autenticação Kerberos e NTLMv2. Você deve verificar as configurações no servidor CIFS e nos servidores Hyper-V que controlam quais métodos de autenticação são permitidos.

Sobre esta tarefa

A autenticação Kerberos é necessária ao fazer uma conexão de compartilhamento continuamente disponível. Parte do processo VSS remoto usa autenticação NTLMv2.1X. Portanto, conexões usando ambos os métodos de autenticação devem ser suportadas para configurações Hyper-V em SMB.

As seguintes configurações devem ser configuradas para permitir a autenticação Kerberos e NTLMv2:

- As políticas de exportação para SMB devem ser desativadas na máquina virtual de storage (SVM).

A autenticação Kerberos e NTLMv2 estão sempre ativadas em SVMs, mas as políticas de exportação podem ser usadas para restringir o acesso com base no método de autenticação.

As políticas de exportação para SMB são opcionais e estão desativadas por padrão. Se as políticas de exportação estiverem desativadas, a autenticação Kerberos e NTLMv2 serão permitidas em um servidor CIFS por padrão.

- O domínio ao qual o servidor CIFS e os servidores Hyper-V pertencem deve permitir a autenticação Kerberos e NTLMv2.

A autenticação Kerberos é ativada por padrão em domínios do ative Directory. No entanto, a autenticação NTLMv2.1X pode ser desativada, utilizando as definições de Política de Segurança ou políticas de Grupo.

Passos

1. Execute o seguinte procedimento para verificar se as políticas de exportação estão desativadas no SVM:
   a. Defina o nível de privilégio como avançado:

      ```
      set -privilege advanced
      ```

   b. Verifique se a `-is-exportpolicy-enabled` opção de servidor CIFS está definida como `false`:

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

   c. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

2. Se as políticas de exportação para SMB não estiverem desativadas, desative-as:

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

3. Verifique se a autenticação NTLMv2 e Kerberos são permitidas no domínio.

   Para obter informações sobre como determinar quais métodos de autenticação são permitidos no domínio,

consulte a Biblioteca Microsoft TechNet.

4. Se o domínio não permitir a autenticação NTMLv2.1x, ative a autenticação NTLMv2.1x utilizando um dos métodos descritos na documentação da Microsoft.

Exemplo

Os comandos a seguir verificam se as políticas de exportação para SMB estão desativadas no 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
```

Verifique se as contas de domínio são mapeadas para o usuário UNIX padrão

Hyper-V e SQL Server usam contas de domínio para criar conexões SMB para compartilhamentos continuamente disponíveis. Para criar a conexão com êxito, a conta do computador deve mapear com êxito para um usuário UNIX. A maneira mais conveniente de fazer isso é mapear a conta do computador para o usuário UNIX padrão.

Sobre esta tarefa

Hyper-V e SQL Server usam as contas de computador de domínio para criar conexões SMB. Além disso, o SQL Server usa uma conta de usuário de domínio como a conta de serviço que também faz conexões SMB.

Quando você cria uma máquina virtual de armazenamento (SVM), o ONTAP cria automaticamente o usuário padrão chamado "'pcuser'" (com um UID do `65534`) e o grupo chamado "'pcuser'" (com um GID do `65534`) e adiciona o usuário padrão ao grupo "'pcuser'". Se você estiver configurando uma solução Hyper-V sobre SMB em um SVM que existia antes de atualizar o cluster para o Data ONTAP 8.2, o usuário e o grupo padrão podem não existir. Se não o fizerem, você deverá criá-los antes de configurar o usuário UNIX padrão do servidor CIFS.

Passos

1. Determine se há um usuário UNIX padrão:

   vserver cifs options show -vserver *vserver_name*

2. Se a opção de usuário padrão não estiver definida, determine se há um usuário UNIX que pode ser designado como o usuário UNIX padrão:

   vserver services unix-user show -vserver *vserver_name*

3. Se a opção de usuário padrão não estiver definida e não houver um usuário UNIX que possa ser designado como usuário UNIX padrão, crie o usuário UNIX padrão e o grupo padrão e adicione o usuário padrão ao grupo.

   Geralmente, o usuário padrão recebe o nome de usuário ""pcuser"" e deve ser atribuído o UID de `65534`. O grupo padrão geralmente recebe o nome do grupo ""pcuser"". O GID atribuído ao grupo deve ser `65534`.

   a. Criar o grupo padrão **vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534**
   b. Crie o usuário padrão e adicione o usuário padrão ao grupo padrão **vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534**
   c. Verifique se o usuário padrão e o grupo padrão estão configurados corretamente **vserver services unix-user show -vserver *vserver_name* vserver services unix-group show -vserver *vserver_name* -members**
4. Se o usuário padrão do servidor CIFS não estiver configurado, execute o seguinte procedimento:
   a. Configurar o utilizador predefinido:

      vserver cifs options modify -vserver *vserver_name* -default-unix-user pcuser*

   b. Verifique se o usuário UNIX padrão está configurado corretamente:

      vserver cifs options show -vserver *vserver_name*

5. Para verificar se a conta do computador do servidor de aplicativos mapeia corretamente para o usuário padrão, mapeie uma unidade para um compartilhamento residente no SVM e confirme o mapeamento do usuário do Windows para o UNIX usando o `vserver cifs session show` comando.

   Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Exemplo

Os comandos a seguir determinam que o usuário padrão do servidor CIFS não está definido, mas determina que o usuário "'pcuser'" e o grupo "'pcuser'" existem. O usuário "'pcuser'" é atribuído como o usuário padrão do servidor CIFS na 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           : -
```

Verifique se o estilo de segurança do volume raiz SVM está definido como NTFS

Para garantir que as operações ininterruptas para Hyper-V e SQL Server sobre SMB sejam bem-sucedidas, os volumes devem ser criados com o estilo de segurança NTFS. Como o estilo de segurança do volume raiz é aplicado por padrão aos volumes criados na máquina virtual de armazenamento (SVM), o estilo de segurança do volume raiz deve ser definido como NTFS.

Sobre esta tarefa

- Você pode especificar o estilo de segurança do volume raiz no momento em que você criar o SVM.

- Se o SVM não for criado com o volume raiz definido como estilo de segurança NTFS, você poderá alterar o estilo de segurança mais tarde usando o `volume modify` comando.

Passos

1. Determine o estilo de segurança atual do volume raiz da SVM:

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

2. Se o volume raiz não for um volume de estilo de segurança NTFS, altere o estilo de segurança para NTFS:

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

3. Verifique se o volume raiz SVM está definido como estilo de segurança NTFS:

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

Exemplo

Os comandos a seguir verificam se o estilo de segurança do volume raiz é NTFS no 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
```

Verifique se as opções de servidor CIFS necessárias estão configuradas

Você deve verificar se as opções de servidor CIFS necessárias estão habilitadas e configuradas de acordo com os requisitos para operações ininterruptas para Hyper-V e SQL Server sobre SMB.

Sobre esta tarefa

- O SMB 2.x e o SMB 3,0 devem estar ativados.
- A descarga de cópia ODX deve ser habilitada para usar a descarga de cópia que melhora o desempenho.
- Os serviços VSS Shadow Copy devem estar ativados se a solução Hyper-V over SMB utilizar serviços de cópia de segurança ativados por VSS remoto (apenas Hyper-V).

Passos

1. Verifique se as opções de servidor CIFS necessárias estão ativadas na máquina virtual de armazenamento (SVM):
   a. Defina o nível de privilégio como avançado:

      `set -privilege advanced`

   b. Introduza o seguinte comando:

      `vserver cifs options show -vserver *vserver_name*`

      As seguintes opções devem ser definidas como `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Apenas Hyper-V)
2. Se alguma das opções não estiver definida como `true`, execute o seguinte procedimento:
   a. Defina-os como `true` utilizando o `vserver cifs options modify` comando.
   b. Verifique se as opções estão definidas `true` usando o `vserver cifs options show` comando.
3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Exemplo

Os comandos a seguir verificam se as opções necessárias para a configuração Hyper-V sobre SMB estão habilitadas no SVM VS1. No exemplo, a descarga de cópia ODX deve estar habilitada para atender aos requisitos de opção.

```
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
```

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas para configurações Hyper-V e SQL Server em SMB.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

  O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

  Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Ative SMB Multichannel no servidor SMB:

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

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

   ```
   vserver cifs session show
   ```

4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
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
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 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: -
```

Criar volumes de dados NTFS

Você deve criar volumes de dados NTFS na máquina virtual de armazenamento (SVM) antes de poder configurar compartilhamentos continuamente disponíveis para uso com

Hyper-V ou SQL Server em servidores de aplicativos SMB. Use a Planilha de configuração de volume para criar seus volumes de dados.

Sobre esta tarefa

Há parâmetros opcionais que você pode usar para personalizar um volume de dados. Para obter mais informações sobre a personalização de volumes, consulte "Gerenciamento de storage lógico".

À medida que você cria seus volumes de dados, você não deve criar pontos de junção dentro de um volume que contenha o seguinte:

- Arquivos Hyper-V para os quais o ONTAP faz cópias de sombra
- Arquivos de banco de dados do SQL Server que são copiados usando o SQL Server

> Se você inadvertidamente criar um volume que usa estilo de segurança misto ou UNIX, não poderá alterar o volume para um volume de estilo de segurança NTFS e usá-lo diretamente para criar compartilhamentos continuamente disponíveis para operações ininterruptas. Operações ininterruptas para Hyper-V e SQL Server em SMB não funcionam corretamente, a menos que os volumes usados na configuração sejam criados como volumes de estilo de segurança NTFS. Você deve excluir o volume e recriar o volume com estilo de segurança NTFS, ou pode mapear o volume em um host Windows e aplicar uma ACL na parte superior do volume e propagar a ACL para todos os arquivos e pastas no volume.

Passos

1. Crie o volume de dados inserindo o comando apropriado:

Se você quiser criar um volume em um SVM onde o estilo de segurança do volume raiz é…	Digite o comando…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Não 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. Verifique se a configuração do volume está correta:

   `volume show -vserver vserver_name -volume volume_name`

Crie compartilhamentos SMB continuamente disponíveis

Depois de criar seus volumes de dados, você pode criar os compartilhamentos continuamente disponíveis que os servidores de aplicativos usam para acessar a máquina virtual Hyper-V e os arquivos de configuração e os arquivos de banco de dados

do SQL Server. Você deve usar a Planilha de configuração de compartilhamento ao criar compartilhamentos SMB.

Passos

1. Apresenta informações sobre os volumes de dados existentes e os respetivos caminhos de junção:

   volume show -vserver *vserver_name* -junction

2. Crie um compartilhamento SMB continuamente disponível:

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

   - Opcionalmente, você pode adicionar um comentário à configuração de compartilhamento.
   - Por padrão, a propriedade de compartilhamento de arquivos off-line é configurada no compartilhamento e está definida como `manual`.
   - O ONTAP cria o compartilhamento com a permissão de compartilhamento padrão do Windows de `Everyone` / `Full Control`.

3. Repita a etapa anterior para todos os compartilhamentos na Planilha de configuração de compartilhamento.
4. Verifique se sua configuração está correta usando o `vserver cifs share show` comando.
5. Configure permissões de arquivo NTFS nos compartilhamentos continuamente disponíveis mapeando uma unidade para cada compartilhamento e configurando permissões de arquivo usando a janela **Propriedades do Windows**.

Exemplo

Os comandos a seguir criam um compartilhamento continuamente disponível chamado "ata2" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os links simbólicos são desativados definindo o `-symlink` parâmetro para `""`:

```
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
```

Adicionar o privilégio SeSecurityPrivilege à conta de usuário (para SQL Server de compartilhamentos SMB)

A conta de usuário do domínio usada para instalar o servidor SQL deve ser atribuída ao privilégio ""SeSecurityPrivilege"" para executar determinadas ações no servidor CIFS que exigem Privileges não atribuído por padrão aos usuários do domínio.

O que você vai precisar

A conta de domínio usada para instalar o SQL Server já deve existir.

Sobre esta tarefa

Ao adicionar o privilégio à conta do instalador do SQL Server, o ONTAP pode validar a conta entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Adicione o privilégio "SeSecurityPrivilege":

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

   O valor para o `-user-or-group-name` parâmetro é o nome da conta de usuário do domínio usada para instalar o SQL Server.

2. Verifique se o privilégio é aplicado à conta:

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

Exemplo

O comando a seguir adiciona o privilégio "'SeSecurityPrivilege" à conta do instalador do SQL Server no domínio DE EXEMPLO para máquina virtual de armazenamento (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
```

Configurar a profundidade do diretório de cópia de sombra VSS (para compartilhamentos Hyper-V sobre SMB)

Opcionalmente, você pode configurar a profundidade máxima de diretórios em compartilhamentos SMB nos quais criar cópias sombra. Este parâmetro é útil se você quiser controlar manualmente o nível máximo de subdiretórios nos quais o ONTAP deve criar cópias de sombra.

O que você vai precisar

O recurso de cópia de sombra VSS deve estar ativado.

Sobre esta tarefa

O padrão é criar cópias de sombra para um máximo de cinco subdiretórios. Se o valor estiver definido como `0`, o ONTAP criará cópias de sombra para todos os subdiretórios.

> Embora você possa especificar que a profundidade do diretório do conjunto de cópias de sombra inclua mais de cinco subdiretórios ou todos os subdiretórios, há um requisito da Microsoft de que a criação do conjunto de cópias de sombra deve ser concluída em 60 segundos. A criação do conjunto de cópias de sombra falhará se não puder ser concluída dentro deste período de tempo. A profundidade do diretório de cópia sombra escolhida não deve fazer com que o tempo de criação exceda o limite de tempo.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Defina a profundidade do diretório de cópia de sombra VSS para o nível desejado:

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

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

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar configurações do Hyper-V e do SQL Server em SMB

Configurar compartilhamentos existentes para disponibilidade contínua

Você pode modificar compartilhamentos existentes para se tornarem compartilhamentos continuamente disponíveis que os servidores de aplicativos Hyper-V e SQL Server usam para acessar arquivos de configuração e máquina virtual Hyper-V sem interrupções e arquivos de banco de dados do SQL Server.

Sobre esta tarefa

Você não pode usar um compartilhamento existente como um compartilhamento continuamente disponível para operações ininterruptas com servidores de aplicações em SMB se o compartilhamento tiver as seguintes características:

- Se a `homedirectory` propriedade share estiver definida nesse compartilhamento
- Se o compartilhamento contiver links simbólicos ou widelinks habilitados
- Se o compartilhamento contiver volumes juntados abaixo da raiz do compartilhamento

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

As seguintes propriedades de compartilhamento devem ser configuradas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas. Se eles estiverem presentes na lista de propriedades de compartilhamento atuais, eles precisam ser removidos do compartilhamento continuamente disponível:

- `attributecache`
- `branchcache`

Passos

1. Exiba as configurações atuais de parâmetros de compartilhamento e a lista atual de propriedades de compartilhamento configuradas:

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

2. Se necessário, modifique os parâmetros de compartilhamento para desativar links simbólicos e defina arquivos off-line para manual usando o `vserver cifs share modify` comando.
   - Pode desativar os links simbólicos definindo o valor do `-symlink` parâmetro para `""`.
   - Pode definir o `-offline-files` parâmetro para a definição correta especificando `manual`.
3. Adicione a `continuously-available` propriedade da ação e, se necessário, a `oplocks` propriedade da ação:

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

   Se a `oplocks` propriedade share ainda não estiver definida, você deve adicioná-la juntamente com a `continuously-available` propriedade share.

4. Remova quaisquer propriedades de compartilhamento que não sejam suportadas em compartilhamentos disponíveis continuamente:

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

   Você pode remover uma ou mais propriedades de compartilhamento especificando as propriedades de compartilhamento com uma lista delimitada por vírgulas.

5. Verifique se `-symlink` os parâmetros e `-offline-files` estão definidos corretamente:

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

6. Verifique se a lista de propriedades de compartilhamento configuradas está correta:

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

Exemplos

O exemplo a seguir mostra como configurar um compartilhamento existente chamado "share1" na máquina virtual de armazenamento (SVM) "VS1" para NDOs com um servidor de aplicativos sobre SMB:

- Os links simbólicos são desativados no compartilhamento definindo o `-symlink` parâmetro como `""`.
- O `-offline-file` parâmetro é modificado e definido para `manual`.
- A `continuously-available` propriedade share é adicionada à ação.
- A `oplocks` propriedade da ação já está na lista de propriedades da ação; portanto, ela não precisa ser adicionada.
- A `attributecache` propriedade share é removida da ação.
- A `browsable` propriedade de compartilhamento é opcional para um compartilhamento continuamente disponível usado para NDOs com servidores de aplicativos em SMB e é mantido como uma das propriedades de compartilhamento.

```
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
```

Ative ou desative cópias de sombra VSS para backups Hyper-V em SMB

Se você usar um aplicativo de backup com reconhecimento VSS para fazer backup de arquivos de máquina virtual Hyper-V armazenados em compartilhamentos SMB, a cópia de sombra VSS deve estar habilitada. Você pode desativar a cópia de sombra do VSS se não usar aplicativos de backup com reconhecimento VSS. O padrão é ativar a cópia de sombra VSS.

Sobre esta tarefa

Você pode ativar ou desativar cópias de sombra VSS a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Execute uma das seguintes ações:

Se você quiser que cópias de sombra VSS sejam…	Digite o comando…
Ativado	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true`**
Desativado	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false`**

3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Exemplo

Os comandos a seguir habilitam cópias de sombra do VSS no 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
```

Use estatísticas para monitorar a atividade do Hyper-V e do SQL Server em SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object` *`object_name`*
Quais contadores estão disponíveis	`statistics catalog counter show object` *`object_name`*

   Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
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
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível de privilégio avançado:

> Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
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


[...]
```

Exibir estatísticas SMB no ONTAP

Você pode exibir várias estatísticas SMB para monitorar o desempenho e diagnosticar

problemas.

Passos

1. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados.
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite o seguinte comando…
Todas as versões do SMB	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x e SMB 3,0	**`statistics show -object smb2`**
Subsistema SMB do nó	**`statistics show -object nblade_cifs`**

Saiba mais sobre os comandos link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-show.html[`statistics show`(em inglês), link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-start.html[`statistics start`(em inglês) e link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-stop.html[`statistics stop`(em inglês) na referência de comando ONTAP.

Verifique se a configuração é capaz de operações ininterruptas

Use o monitoramento de integridade para determinar se o status de operação sem interrupções está íntegro

O monitoramento de integridade fornece informações sobre o status de integridade do sistema em todo o cluster. O monitor de integridade monitora as configurações Hyper-V e SQL Server em SMB para garantir operações ininterruptas (NDOs) para os servidores de aplicações. Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas.

Existem vários monitores de saúde. O ONTAP monitora a integridade e a integridade geral do sistema para monitores de integridade individuais. O monitor de integridade da conetividade do nó contém o subsistema CIFS-NDO. O monitor tem um conjunto de políticas de integridade que acionam alertas se certas condições físicas podem causar interrupções e, se houver uma condição disruptiva, gera alertas e fornece informações sobre ações corretivas. Para configurações NDO sobre SMB, alertas são gerados para as duas condições a seguir:

ID de alerta	Gravidade	Condição
HaNotReadyCifsNdo_Alert	Maior	Um ou mais arquivos hospedados por um volume em um agregado no nó foram abertos por meio de um compartilhamento SMB continuamente disponível com a promessa de persistência em caso de falha. No entanto, o relacionamento de HA com o parceiro não está configurado ou não está íntegro.
NoStandbyLifCifsNdo_Alert	Menor	A máquina virtual de storage (SVM) está fornecendo dados ativamente sobre SMB por meio de um nó e há arquivos SMB abertos persistentemente por compartilhamentos disponíveis continuamente. No entanto, seu nó de parceiro não expõe LIFs de dados ativos para o SVM.

Exibir o status de operação sem interrupções usando o monitoramento de integridade do sistema

Você pode usar os `system health` comandos para exibir informações sobre a integridade geral do sistema do cluster e a integridade do subsistema CIFS-NDO, responder a alertas, configurar alertas futuros e exibir informações sobre como o monitoramento de integridade está configurado.

Passos

1. Monitore o status de integridade executando a ação apropriada:

Se você quiser exibir…	Digite o comando…
O estado de saúde do sistema, que reflete o estado geral dos monitores de saúde individuais	**system health status show**
Informações sobre o estado de funcionamento do subsistema CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Exiba informações sobre como o monitoramento de alerta CIFS-NDO é configurado executando as ações apropriadas:

Se você quiser exibir informações sobre…	Digite o comando…
A configuração e o status do monitor de integridade do subsistema CIFS-NDO, como nós monitorados, estado de inicialização e status	**system health config show -subsystem CIFS-NDO**
O CIFS-NDO alerta que um monitor de integridade pode gerar	**system health alert definition show -subsystem CIFS-NDO**
Políticas do monitor de integridade CIFS-NDO, que determinam quando os alertas são gerados	**system health policy definition show -monitor node-connect**

Use o `-instance` parâmetro para exibir informações detalhadas.

Exemplos

A saída a seguir mostra informações sobre o status geral de integridade do cluster e do subsistema 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
```

A saída a seguir mostra informações detalhadas sobre a configuração e o status do monitor de integridade do subsistema 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
```

Verifique a configuração de compartilhamento SMB continuamente disponível

Para dar suporte a operações ininterruptas, os compartilhamentos SMB do Hyper-V e do SQL Server devem ser configurados como compartilhamentos disponíveis continuamente. Além disso, existem certas outras configurações de compartilhamento que você deve verificar. Você deve verificar se os compartilhamentos estão configurados corretamente para fornecer operações ininterruptas contínuas para os servidores de aplicações, se houver eventos disruptivos planejados ou não planejados.

Sobre esta tarefa

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

Para operações ininterruptas adequadas, as seguintes propriedades de compartilhamento devem ser definidas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas:

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

Passos

1. Verifique se os arquivos off-line estão definidos como `manual` ou `disabled` e se os links simbólicos estão desativados:

   vserver cifs shares show -vserver *vserver_name*

2. Verifique se os compartilhamentos SMB estão configurados para disponibilidade contínua:

   vserver cifs shares properties show -vserver *vserver_name*

Exemplos

O exemplo a seguir exibe a configuração de compartilhamento para um compartilhamento chamado "hare1" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os arquivos offline são definidos como `manual` e os links simbólicos são desativados (designados por um hífen na `Symlink Properties` saída do 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
```

O exemplo a seguir exibe as propriedades de compartilhamento de um compartilhamento chamado "hare1" no SVM VS1:

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

Verifique o status do LIF

Mesmo que você configure máquinas virtuais de armazenamento (SVMs) com configurações Hyper-V e SQL Server sobre SMB para ter LIFs em cada nó em um cluster, durante operações diárias, alguns LIFs podem se mover para portas em outro nó. Você deve verificar o status do LIF e tomar todas as ações corretivas necessárias.

Sobre esta tarefa

Para oferecer suporte contínuo a operações ininterruptas e sem interrupções, cada nó em um cluster precisa ter pelo menos um LIF para a SVM e todos os LIFs precisam estar associados a uma porta inicial. Se algumas LIFs configuradas não estiverem associadas atualmente à porta inicial, você deverá corrigir quaisquer problemas de porta e reverter os LIFs para a porta inicial.

Passos

1. Exibir informações sobre LIFs configuradas para o SVM:

   network interface show -vserver *vserver_name*

   Neste exemplo, "'lif1'" não está localizado na porta inicial.

```
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
```

2. Se alguns dos LIFs não estiverem em suas portas residenciais, execute as seguintes etapas:

   a. Para cada LIF, determine qual é a porta inicial do 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. Para cada LIF, determine se a porta inicial do LIF está ativa:

   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
   ```

   + Neste exemplo, "'lif1" deve ser migrado de volta para sua porta de origem, `node1:e0d`.

3. Se qualquer uma das interfaces de rede de porta inicial às quais os LIFs devem estar associados não estiver no `up` estado, resolva o problema para que essas interfaces estejam ativas.
4. Se necessário, reverta os LIFs para suas portas residenciais:

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

   network interface revert -vserver vs1 -lif lif1

5. Verifique se cada nó no cluster tem um LIF ativo para o 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
```

Determine se as sessões SMB estão continuamente disponíveis

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
Para todas as sessões no SVM de forma resumida	**vserver cifs session show -vserver *vserver_name***
Em um ID de conexão especificado	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
A partir de um endereço IP de estação de trabalho especificado	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Em um endereço IP de LIF especificado	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Em um nó especificado	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	De um usuário do Windows especificado
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* O formato para `user_name` é `[domain]\user`.	Com um mecanismo de autenticação especificado

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism O valor para `-auth -mechanism` pode ser um dos seguintes: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Com uma versão de protocolo especificada

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version O valor para `-protocol-version` pode ser um dos seguintes: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Com um nível especificado de proteção continuamente disponível

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
`vserver cifs session show -vserver vserver_name -continuously -available continuously_available_protection_level` O valor para `-continuously -available` pode ser um dos seguintes: • `No` • `Yes` • `Partial` Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode	Com um status de sessão de assinatura SMB especificado

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço 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
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
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
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
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
```

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você também pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show` comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais

informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	**vserver cifs session file show -vserver *vserver_name***
Em um nó especificado	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Em um ID de arquivo especificado
vserver cifs session file show -vserver *vserver_name* -file-id integer	Em uma ID de conexão SMB especificada
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Em um SMB Session ID especificado
vserver cifs session file show -vserver *vserver_name* -session-id integer	No agregado de hospedagem especificado
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	No volume especificado
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	No compartilhamento SMB especificado
vserver cifs session file show -vserver *vserver_name* -share *share_name*	No caminho SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
vserver cifs session file show -vserver *vserver_name* -path *path*	Com o nível especificado de proteção continuamente disponível
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* O valor para `-continuously-available` pode ser um dos seguintes: • `No` • `Yes` Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade.	Com o estado de reconexão especificado

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no 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
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no 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
```

Informações sobre direitos autorais

Informações sobre marcas comerciais