Configuration SMB pour Microsoft Hyper-V et SQL Server

ONTAP 9

NetApp
January 08, 2026

Sommaire

Configuration SMB pour Microsoft Hyper-V et SQL Server

Présentation de la configuration SMB pour Microsoft Hyper-V et SQL Server

Les fonctionnalités de ONTAP assurent la continuité de l'activité pour deux applications Microsoft sur le protocole SMB : Microsoft Hyper-V et Microsoft SQL Server.

Vous devez appliquer ces procédures pour implémenter une continuité de l'activité SMB dans les circonstances suivantes :

- L'accès de base aux fichiers du protocole SMB a été configuré.
- Vous souhaitez activer les partages de fichiers SMB 3.0 ou version ultérieure résidant sur les SVM pour stocker les objets suivants :
  - Fichiers de machines virtuelles Hyper-V.
  - Bases de données système SQL Server

Informations associées

Pour plus d'informations sur la technologie ONTAP et l'interaction avec les services externes, voir les rapports techniques (TR) : ** "Rapport technique de NetApp 4172 : Microsoft Hyper-V sur SMB 3.0 avec les meilleures pratiques de ONTAP" "Rapport technique NetApp 4369 : meilleures pratiques pour Microsoft SQL Server et SnapManager 7.2 for SQL Server avec clustered Data ONTAP"

Configuration de ONTAP pour Microsoft Hyper-V et SQL Server sur les solutions SMB

Vous pouvez utiliser les partages de fichiers SMB 3.0 et versions ultérieures disponibles en permanence pour stocker les fichiers des machines virtuelles Hyper-V ou les bases de données du système SQL Server et les bases de données des utilisateurs sur des volumes résidant dans des SVM, tout en assurant la continuité de l'activité à la fois pour les événements planifiés et non planifiés.

Microsoft Hyper-V sur SMB

Pour créer une solution Hyper-V sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage aux serveurs Microsoft Hyper-V. En outre, vous devez également configurer les clusters Microsoft (s'ils utilisent une configuration en cluster), les serveurs Hyper-V, les connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS, et, éventuellement, les services de sauvegarde pour protéger les fichiers de machines virtuelles stockés sur les volumes de SVM.

> Les serveurs Hyper-V doivent être configurés sur Windows 2012 Server ou version ultérieure. Les configurations de serveur Hyper-V autonomes et en cluster sont toutes deux prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et de serveurs Hyper-V, consultez le site Web de Microsoft.

- SnapManager for Hyper-V est une application basée sur hôte qui facilite des services de sauvegarde rapides basés sur des copies Snapshot. Elle est conçue pour s'intégrer aux configurations Hyper-V sur SMB.

  Pour plus d'informations sur l'utilisation de SnapManager avec les configurations Hyper-V sur SMB, voir le *SnapManager for Hyper-V installation and Administration Guide*.

Microsoft SQL Server sur SMB

Pour créer une solution SQL Server sur SMB, vous devez d'abord configurer ONTAP afin de fournir des services de stockage pour l'application Microsoft SQL Server. En outre, vous devez également configurer les clusters Microsoft (en cas d'utilisation d'une configuration en cluster). Vous devez ensuite installer et configurer SQL Server sur les serveurs Windows et créer des connexions SMB 3.0 disponibles en continu vers les partages hébergés par le serveur CIFS. Vous pouvez choisir de configurer les services de sauvegarde pour protéger les fichiers de base de données stockés sur des volumes SVM.

SQL Server doit être installé et configuré sur Windows 2012 Server ou version ultérieure. Les configurations autonomes et en cluster sont prises en charge.

- Pour plus d'informations sur la création de clusters Microsoft et l'installation et la configuration de SQL Server, consultez le site Web de Microsoft.
- Le plug-in SnapCenter pour Microsoft SQL Server est une application basée sur hôte qui facilite des services de sauvegarde rapides basés sur des snapshots, conçus pour s'intégrer aux configurations SQL Server sur SMB.

  Pour plus d'informations sur l'utilisation du plug-in SnapCenter pour Microsoft SQL Server, consultez le "Plug-in SnapCenter pour Microsoft SQL Server" documentation :

Continuité de l'activité pour Hyper-V et SQL Server over SMB

En termes de continuité de l'activité pour Hyper-V et SQL Server over SMB

La continuité de l'activité pour Hyper-V et SQL Server over SMB se réfère à la combinaison de fonctionnalités permettant aux serveurs d'application et aux machines virtuelles ou bases de données contenues de rester en ligne et d'assurer une disponibilité continue au cours de nombreuses tâches administratives. Cela inclut les temps d'indisponibilité planifiés et non planifiés de l'infrastructure de stockage.

La continuité de l'activité pour les serveurs applicatifs via SMB est prise en charge :

- Takeover et Giveback planifiées
- Basculement non planifié
- Mise à niveau
- Transfert d'agrégats planifié (ARL)
- Migration et basculement de LIF
- Déplacement de volume planifié

Protocoles qui garantissent la continuité de l'activité sur SMB

Outre la commercialisation de SMB 3.0, Microsoft a lancé de nouveaux protocoles qui fournissent les fonctionnalités nécessaires à la continuité de l'activité pour Hyper-V et SQL Server over SMB.

ONTAP utilise ces protocoles pour assurer la continuité de l'activité des serveurs applicatifs sur SMB :

- SMB 3.0
- Témoin

Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB

Avant de configurer la solution Hyper-V ou SQL Server sur SMB, certains concepts relatifs à la continuité de l'activité doivent être abordés.

- **Partage disponible en continu**

  Partage SMB 3.0 avec la propriété de partage disponible en continu. Les clients qui se connectent via des partages disponibles en permanence peuvent survivre aux événements perturbateur tels que le basculement, le rétablissement et le transfert d'agrégats.

- **Nœud**

  Un contrôleur unique membre d'un cluster. Pour faire la distinction entre les deux nœuds d'une paire SFO, un nœud est parfois appelé *local node* et l'autre nœud est parfois appelé *Partner node* ou *remote node*. Le propriétaire principal du stockage est le nœud local. Le propriétaire secondaire, qui prend le contrôle du stockage en cas de défaillance du propriétaire principal, est le nœud partenaire. Chaque nœud est le principal propriétaire de son stockage et du secondaire pour le stockage de son partenaire.

- **Transfert d'agrégats sans interruption**

  Capacité à déplacer un agrégat entre les nœuds partenaires au sein d'une paire SFO dans un cluster sans interrompre les applications client.

- **Basculement sans interruption**

  Voir *Takeover*.

- **Migration de LIF sans interruption**

  La possibilité d'effectuer une migration de LIF sans interrompre les applications client qui sont connectées au cluster via cette LIF. Pour les connexions SMB, cette opération est uniquement possible pour les clients qui se connectent via SMB 2.0 ou version ultérieure.

- * Continuité de l'activité*

  La possibilité d'effectuer les principales opérations de gestion et de mise à niveau ONTAP, et de résister aux défaillances de nœud sans interrompre les applications client. Ce terme fait référence à la collecte de fonctionnalités de basculement sans interruption, de mise à niveau sans interruption et de migration dans son ensemble.

- * Mise à niveau sans interruption*

Capacité à mettre à niveau le matériel ou les logiciels des nœuds sans perturber les applications.

- **Déplacement de volume sans interruption**

  La capacité de déplacer librement un volume au sein du cluster sans interrompre les applications qui utilisent ce volume. Pour les connexions SMB, toutes les versions de SMB prennent en charge le déplacement de volumes sans interruption.

- **Poignées permanentes**

  Propriété de SMB 3.0 qui permet aux connexions disponibles en continu de se reconnecter de façon transparente au serveur CIFS en cas de déconnexion. Tout comme les poignées durables, les poignées permanentes sont conservées par le serveur CIFS pendant un certain temps après la perte de la communication avec le client connecté. Toutefois, les pointeurs permanents bénéficient d'une résilience supérieure à celle des poignées durables. En plus de donner au client la possibilité de récupérer la poignée dans une fenêtre de 60 secondes après reconnexion, le serveur CIFS refuse l'accès à tout autre client demandant l'accès au fichier pendant cette fenêtre de 60 secondes.

  Des informations relatives aux pointeurs permanents sont mises en miroir sur le stockage persistant du partenaire SFO, qui permet aux clients disposant de pointeurs permanents déconnectés de récupérer les pointeurs durables après un événement où le partenaire SFO est propriétaire du stockage du nœud. En plus d'assurer la continuité de l'activité en cas de déplacement de LIF (dont la prise en charge est durable), des pointeurs permanents assurent la continuité de l'activité pendant le basculement, le rétablissement et le transfert d'agrégats.

- **OFS-retour**

  Retour d'agrégats à leurs locaux lors d'une récupération après un événement de basculement.

- **Paire SFO**

  Si l'un des deux nœuds cesse de fonctionner, une paire de nœuds dont les contrôleurs sont configurés pour transmettre des données les uns aux autres. Selon le modèle du système, les deux contrôleurs peuvent se trouver dans un seul châssis ou les contrôleurs peuvent se trouver dans un châssis distinct. Appelé paire HA dans un cluster à deux nœuds.

- * Prise de contrôle*

  Processus par lequel le partenaire prend le contrôle du stockage en cas de défaillance du propriétaire principal de ce stockage. Dans le cadre du SFO, le basculement et le basculement sont synonymes.

La fonctionnalité SMB 3.0 prend en charge la continuité de l'activité sur les partages SMB

SMB 3.0 apporte une fonctionnalité essentielle qui permet la continuité de l'activité pour les partages Hyper-V et SQL Server sur SMB. Cela inclut le `continuously-available` Partagez la propriété et un type de descripteur de fichier appelé *persistent handle* qui permettent aux clients SMB de récupérer l'état ouvert du fichier et de rétablir de façon transparente les connexions SMB.

Des pointeurs permanents peuvent être accordés aux clients compatibles SMB 3.0 qui se connectent à un partage avec l'ensemble de propriétés de partage disponible en continu. Si la session SMB est déconnectée, le serveur CIFS conserve les informations relatives à l'état de descripteur permanent. Le serveur CIFS bloque

les autres requêtes client pendant la période de 60 secondes pendant laquelle le client est autorisé à se reconnecter, ce qui permet au client avec le descripteur permanent de récupérer le descripteur après une déconnexion du réseau. Les clients avec pointeurs permanents peuvent se reconnecter en utilisant l'une des LIF de données sur la machine virtuelle de stockage (SVM), en reconnectant via la même LIF ou via une autre LIF.

Le transfert, le basculement et le rétablissement d'agrégats s'effectuent tous entre les paires SFO. Pour gérer de manière transparente la déconnexion et la reconnexion des sessions avec des fichiers dotés de pointeurs permanents, le nœud partenaire conserve une copie de toutes les informations de verrouillage de descripteur permanent. Que l'événement soit planifié ou non, le partenaire SFO peut gérer les reconnexions de la poignée persistante sans interruption. Grâce à cette nouvelle fonctionnalité, les connexions SMB 3.0 au serveur CIFS peuvent basculer en toute transparence vers une autre LIF de données affectée à la SVM, selon les temps d'événements perturbateurs.

Bien que l'utilisation de pointeurs permanents permette au serveur CIFS de basculer en toute transparence sur des connexions SMB 3.0, en cas de défaillance, l'application Hyper-V bascule vers un autre nœud du cluster Windows Server, le client n'a aucun moyen de récupérer les descripteurs de fichiers de ces pointeurs déconnectés. Dans ce scénario, les descripteurs de fichier à l'état déconnecté peuvent potentiellement bloquer l'accès à l'application Hyper-V s'il est redémarré sur un autre nœud. « Failover Clustering » fait partie de SMB 3.0 qui répond à ce scénario en fournissant un mécanisme permettant d'invalider des pointeurs obsolètes en conflit. Grâce à ce mécanisme, un cluster Hyper-V peut restaurer rapidement les données en cas de panne des nœuds de cluster Hyper-V.

Comment le protocole Witness traite l'amélioration du basculement transparent

Le protocole Witness propose des fonctionnalités de basculement client améliorées pour les partages SMB 3.0 disponibles en continu (partages CA). Témoin facilite le basculement plus rapide car il évite toute période de restauration de basculement LIF. Cette notification avertit les serveurs d'applications lorsqu'un nœud est indisponible sans nécessiter l'attente de la connexion SMB 3.0.

Le basculement est transparent, car les applications s'exécutant sur le client ne savent pas qu'un basculement a eu lieu. Si Witness n'est pas disponible, le basculement s'effectue toujours avec succès, mais le basculement sans Witness s'avère moins efficace.

Le basculement amélioré par témoin est possible lorsque les conditions suivantes sont respectées :

- Il ne peut être utilisé qu'avec des serveurs CIFS compatibles SMB 3.0 sur lesquels SMB 3.0 est activé.
- Les partages doivent utiliser SMB 3.0 avec l'ensemble de propriétés de partage de disponibilité continue.
- Le partenaire SFO du nœud sur lequel les serveurs d'applications sont connectés doit disposer d'au moins une LIF de données opérationnelles attribuée au SVM (Storage Virtual machine) qui héberge les données des serveurs applicatifs.

> Le protocole Witness fonctionne entre les paires SFO. Étant donné que les LIF peuvent migrer vers n'importe quel nœud du cluster, n'importe quel nœud peut avoir besoin d'être le témoin de son partenaire SFO. Le protocole Witness ne peut pas permettre le basculement rapide des connexions SMB sur un nœud donné si le SVM hébergeant les données des serveurs d'applications ne dispose pas d'une LIF de données active sur le nœud partenaire. Par conséquent, chaque nœud du cluster doit disposer d'au moins une LIF de données pour chaque SVM hébergeant l'une de ces configurations.

- Les serveurs d'applications doivent se connecter au serveur CIFS en utilisant le nom du serveur CIFS

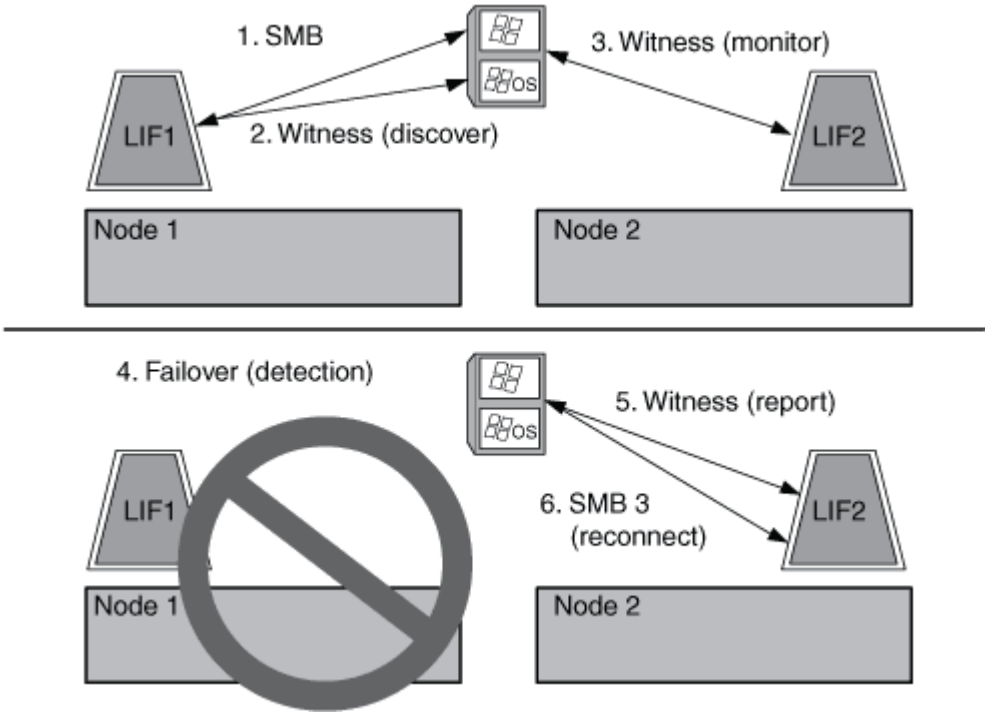
stocké dans DNS au lieu d'utiliser des adresses IP LIF individuelles.

Fonctionnement du protocole Witness

ONTAP implémente le protocole Witness en utilisant le partenaire SFO d'un nœud comme témoin. En cas de défaillance, le partenaire détecte rapidement la panne et en informe le client SMB.

Le protocole Witness fournit un basculement amélioré à l'aide du processus suivant :

1. Lorsque le serveur d'applications établit une connexion SMB disponible en continu pour Node1, le serveur CIFS informe le serveur d'applications que Witness est disponible.
2. Le serveur d'application demande les adresses IP du serveur Witness à partir du nœud 1 et reçoit une liste des adresses IP LIF de données Node2 (le partenaire SFO) attribuées à la machine virtuelle de stockage (SVM).
3. Le serveur d'application choisit l'une des adresses IP, crée une connexion témoin à Node2 et s'enregistre pour être averti si la connexion disponible en continu sur Node1 doit être déplacé.
4. Si un événement de basculement se produit sur le nœud 1, Witness simplifie les événements de basculement, mais n'est pas impliqué dans le rétablissement.
5. Témoin détecte l'événement de basculement et informe le serveur d'application via la connexion Witness que la connexion SMB doit passer à Node2.
6. Le serveur d'application déplace la session SMB sur Node2 et restaure la connexion sans interruption de l'accès client.



Partage de sauvegardes avec VSS distant

Présentation de VSS distant pour les sauvegardes basées sur le partage

Vous pouvez utiliser VSS distant pour effectuer des sauvegardes basées sur les partages des fichiers de machines virtuelles Hyper-V stockés sur un serveur CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) est une extension de l'infrastructure Microsoft VSS existante. Avec Remote VSS, Microsoft a étendu l'infrastructure VSS pour prendre en charge la copie Shadow des partages SMB. De plus, des applications serveur telles qu'Hyper-V peuvent stocker des fichiers VHD sur des partages de fichiers SMB. Avec ces extensions, il est possible d'effectuer des clichés instantanés cohérents avec les applications pour les machines virtuelles qui stockent des données et des fichiers de configuration sur des partages.

Concepts de VSS distant

Vous devez connaître certains concepts requis pour comprendre l'utilisation de VSS distant (Volume Shadow Copy Service) par les services de sauvegarde avec des configurations Hyper-V sur SMB.

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

  Technologie Microsoft utilisée pour effectuer des copies de sauvegarde ou des snapshots de données sur un volume spécifique à un point dans le temps spécifique. VSS coordonne entre les serveurs de données, les applications de sauvegarde et les logiciels de gestion du stockage afin d'assurer la création et la gestion de sauvegardes cohérentes.

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

  Technologie Microsoft utilisée pour créer des copies de sauvegarde basées sur les partages de données qui sont cohérentes avec les données à un point spécifique dans le temps où les données sont accessibles via les partages SMB 3.0. Également connu sous le nom *Volume Shadow Copy Service*.

- **Copie fantôme**

  Un jeu de données dupliqué contenu dans le partage à un instant bien défini dans le temps. Des clichés instantanés sont utilisés pour créer des sauvegardes ponctuelles cohérentes des données, permettant ainsi au système ou aux applications de continuer à mettre à jour les données sur les volumes d'origine.

- **Ensemble de copies ombré**

  Collection d'une ou plusieurs clichés instantanés, chaque copie fantôme correspondant à un partage. Les clichés instantanés dans un jeu de clichés instantanés représentent tous les partages qui doivent être sauvegardés dans la même opération. Le client VSS de l'application VSS-enabled identifie les clichés instantanés à inclure dans l'ensemble.

- **Shadow Copy set Automatic Recovery**

  La partie du processus de sauvegarde pour les applications de sauvegarde VSS distantes dans lesquelles le répertoire de réplica contenant les clichés instantanés est cohérent à un point dans le temps. Au début de la sauvegarde, le client VSS de l'application déclenche l'application pour qu'elle prenne des points de contrôle logiciels sur les données planifiées pour la sauvegarde (les fichiers de la machine virtuelle dans le cas d'Hyper-V). Le client VSS autorise alors les applications à continuer. Une fois le jeu de clichés instantanés créé, Remote VSS rend le jeu de clichés instantanés inscriptible et expose la copie inscriptible aux applications. L'application prépare le jeu de clichés instantanés pour la sauvegarde en effectuant une restauration automatique à l'aide du point de contrôle du logiciel précédemment effectué. La récupération

automatique place les clichés instantanés dans un état cohérent en détournant les modifications apportées aux fichiers et répertoires depuis la création du point de contrôle. La restauration automatique est une étape facultative pour les sauvegardes VSS.

- **ID de copie fantôme**

  GUID qui identifie de manière unique une copie en double.

- **ID jeu de copies ombré**

  GUID qui identifie de manière unique une collection d'ID de copie en double sur le même serveur.

- **SnapManager pour Hyper-V**

  Logiciel qui automatise et simplifie les opérations de sauvegarde et de restauration pour Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V utilise VSS distant avec restauration automatique pour sauvegarder des fichiers Hyper-V sur des partages SMB.

Informations associées

Concepts clés de la continuité de l'activité pour Hyper-V et SQL Server sur SMB

Partage de sauvegardes avec VSS distant

Exemple de structure de répertoire utilisée par VSS distant

VSS distant traverse la structure de répertoire qui stocke les fichiers de machine virtuelle Hyper-V lorsqu'il crée des clichés instantanés. Il est important de comprendre la structure de répertoires appropriée afin de pouvoir créer des sauvegardes de fichiers de machines virtuelles.

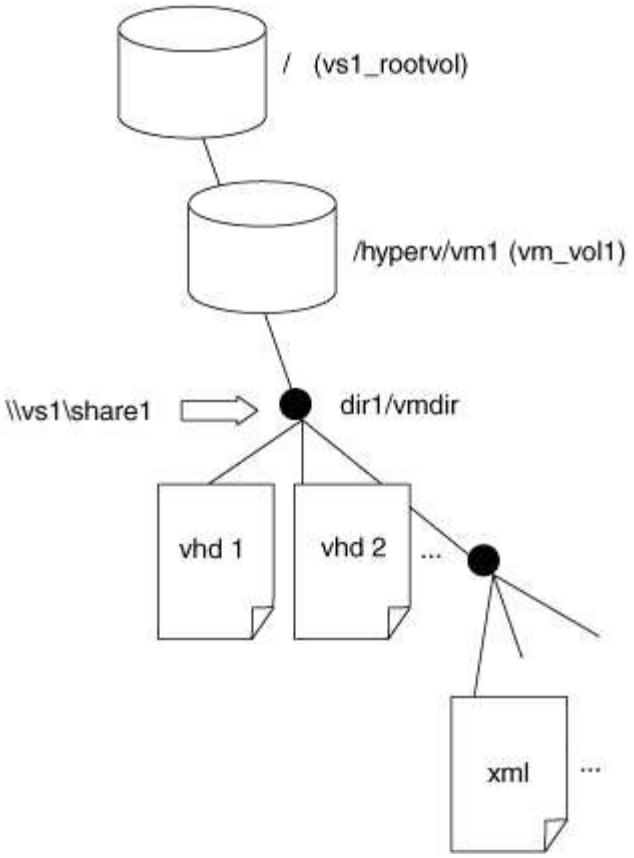
Une structure de répertoire prise en charge pour la création réussie de clichés instantanés est conforme aux exigences suivantes :

- Seuls les répertoires et les fichiers réguliers sont présents dans la structure de répertoires utilisée pour stocker les fichiers de la machine virtuelle.

  La structure du répertoire ne contient pas de jonctions, de liens ou de fichiers non réguliers.

- Tous les fichiers d'une machine virtuelle résident dans un même partage.
- La structure de répertoire utilisée pour stocker les fichiers de la machine virtuelle ne dépasse pas la profondeur configurée dans le répertoire de clichés instantanés.
- Le répertoire racine du partage contient uniquement des fichiers ou des répertoires de machine virtuelle.

Dans l'illustration suivante, le volume nommé vm_vol1 est créé avec un point de jonction à `/hyperv/vm1` Sur la machine virtuelle de stockage (SVM) vs1. Les sous-répertoires contenant les fichiers de la machine virtuelle sont créés sous le point de jonction. Les fichiers de machine virtuelle du serveur Hyper-V sont accessibles sur share1 qui a le chemin `/hyperv/vm1/dir1/vmdir`. Le service Shadow Copy crée des clichés instantanés de tous les fichiers de la machine virtuelle qui sont contenus dans la structure de répertoires sous share1 (jusqu'à la profondeur configurée dans le répertoire Shadow Copy).



Comment SnapManager for Hyper-V gère les sauvegardes VSS distantes pour Hyper-V sur SMB

Vous pouvez utiliser SnapManager for Hyper-V pour gérer les services de sauvegarde VSS distants. Les avantages du service géré de sauvegarde SnapManager for Hyper-V sont nombreux, car il permet de créer des ensembles de sauvegarde peu gourmands en espace.

Les optimisations vers SnapManager pour les sauvegardes gérées Hyper-V sont les suivantes :

- L'intégration de SnapDrive avec ONTAP permet d'optimiser les performances lors de la détection de l'emplacement de partage SMB.

  ONTAP fournit à SnapDrive le nom du volume où réside le partage.

- SnapManager for Hyper-V spécifie la liste des fichiers de machine virtuelle dans les partages SMB que le service Shadow Copy doit copier.

  En fournissant une liste ciblée de fichiers de machine virtuelle, le service de clichés instantanés n'a pas besoin de créer de clichés instantanés de tous les fichiers du partage.

- La machine virtuelle de stockage (SVM) conserve les snapshots de SnapManager pour Hyper-V à utiliser pour les restaurations.

  Il n'y a pas de phase de sauvegarde. La sauvegarde est le snapshot compact.

SnapManager for Hyper-V fournit des fonctionnalités de sauvegarde et de restauration pour HyperV sur SMB,

en utilisant le processus suivant :

1. Préparation de l'opération de copie en double

   Le client VSS de l'application SnapManager pour Hyper-V configure le jeu de clichés instantanés. Le client VSS collecte des informations sur les partages à inclure dans le jeu de clichés instantanés et fournit ces informations à ONTAP. Un ensemble peut contenir une ou plusieurs clichés instantanés et une copie en double correspond à un partage.

2. Création du jeu de clichés instantanés (si la restauration automatique est utilisée)

   Pour chaque partage inclus dans le jeu de clichés instantanés, ONTAP crée une copie « shadow » et rend la copie « shadow Copy » accessible en écriture.

3. Exposition du jeu de clichés instantanés

   Une fois que ONTAP a créé les clichés instantanés, ils sont exposés à SnapManager for Hyper-V de sorte que les enregistreurs VSS de l'application peuvent effectuer une restauration automatique.

4. Restauration automatique du jeu de clichés instantanés

   Au cours de la création du jeu de clichés instantanés, il y a une période pendant laquelle des modifications actives sont apportées aux fichiers inclus dans le jeu de sauvegardes. Les VSS writer de l'application doivent mettre à jour les clichés instantanés pour s'assurer qu'ils sont dans un état complètement cohérent avant la sauvegarde.

   > La méthode d'exécution de la restauration automatique est spécifique à l'application. VSS distant n'est pas impliqué dans cette phase.

5. Finalisation et nettoyage du jeu de clichés instantanés

   Le client VSS informe ONTAP après la fin de la restauration automatique. Le jeu de copies « shadow » est en lecture seule, puis prêt pour la sauvegarde. Lors de l'utilisation de SnapManager pour Hyper-V pour la sauvegarde, les fichiers d'un snapshot deviennent la sauvegarde. Par conséquent, pour la phase de sauvegarde, un snapshot est créé pour chaque volume contenant des partages dans le jeu de sauvegarde. Une fois la sauvegarde terminée, le jeu de clichés instantanés est supprimé du serveur CIFS.

Comment l'allègement de la charge des copies d'ODX est utilisé avec Hyper-V et SQL Server sur des partages SMB

Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage compatible ou entre ces périphériques, sans transférer les données via l'ordinateur hôte. Le allègement de la charge des copies ONTAP ODX présente des avantages en termes de performances lors des opérations de copie sur votre serveur applicatif plutôt que sur une installation SMB.

Dans les transferts de fichiers non ODX, les données sont lues à partir du serveur CIFS source et sont transférées sur le réseau vers l'ordinateur client. L'ordinateur client transfère les données via le réseau vers le serveur CIFS de destination. En résumé, l'ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d'ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l'accélération du délai de copie entre la source et la destination, la réduction de l'utilisation des ressources (CPU, mémoire) sur le client et la réduction de l'utilisation de la bande passante E/S du réseau.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Les cas d'utilisation suivants prennent en charge l'utilisation de copies
et de déplacements d'ODX :
```

- Intra-volume

  Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volumes, même nœud, même machine virtuelle de stockage (SVM)

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

  Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

Les cas d'utilisation spécifiques pour l'allègement de la charge des copies d'ODX avec les solutions Hyper-V sont les suivants :

- Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

  Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
- L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.

Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Voici quelques cas d'utilisation spécifiques des copies ODX utilisées par les solutions SQL Server :

- Vous pouvez utiliser l'allègement de la charge des copies d'ODX pour exporter et importer des bases de données SQL Server entre des partages SMB mappés ou entre des partages SMB et des LUN iSCSI connectés au sein du même cluster.
- L'allègement de la charge de copies (ODX) est utilisé pour les exportations et les importations de bases de données si le stockage source et cible est situé sur le même cluster.

Configuration requise et considérations

Conditions requises pour le ONTAP et les licences

Vous devez connaître certaines exigences en matière de licences et de ONTAP lors de la création de solutions SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité sur les SVM.

Configuration requise pour la version ONTAP

- Hyper-V sur SMB

  ONTAP prend en charge la continuité de l'activité sur les partages SMB pour Hyper-V exécutés sous Windows 2012 ou version ultérieure.

- SQL Server sur SMB

  ONTAP prend en charge la continuité de l'activité sur les partages SMB pour SQL Server 2012 ou une version ultérieure fonctionnant sous Windows 2012 ou version ultérieure.

Pour obtenir les dernières informations sur les versions prises en charge de ONTAP, Windows Server et SQL Server pour assurer la continuité de l'activité sur les partages SMB, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Licences requises

Les licences suivantes sont requises :

- CIFS
- FlexClone (pour Hyper-V sur SMB uniquement)

  Cette licence est requise si Remote VSS est utilisé pour les sauvegardes. Le service Shadow Copy utilise FlexClone pour créer des copies instantanées de fichiers qui sont ensuite utilisés lors de la création d'une sauvegarde.

  Une licence FlexClone est facultative si vous utilisez une méthode de sauvegarde qui n'utilise pas VSS

distant.

La licence FlexClone est incluse dans "ONTAP One". Si vous n'avez pas ONTAP One, vous devez "vérifiez que les licences requises sont installées", et, si nécessaire, "installez-les".

Exigences LIF relatives au réseau et aux données

Vous devez connaître certaines exigences LIF de réseau et de données lors de la création de configurations SQL Server ou Hyper-V sur SMB afin de garantir la continuité de l'activité).

Exigences en matière de protocoles réseau

- Les réseaux IPv4 et IPv6 sont pris en charge.
- SMB 3.0 ou version ultérieure requis.

  SMB 3.0 apporte les fonctionnalités nécessaires pour créer les connexions SMB disponibles en continu nécessaires à la continuité de l'activité.

- Les serveurs DNS doivent contenir des entrées qui mappent le nom du serveur CIFS aux adresses IP attribuées aux LIF de données sur la machine virtuelle de stockage (SVM).

  Les serveurs d'applications Hyper-V ou SQL Server font en général plusieurs connexions sur plusieurs LIF de données lors de l'accès aux fichiers de machines virtuelles ou de bases de données. Pour garantir la fonctionnalité appropriée, les serveurs d'applications doivent établir ces connexions SMB en utilisant le nom du serveur CIFS au lieu de créer plusieurs connexions à plusieurs adresses IP uniques.

  Témoin exige également l'utilisation du nom DNS du serveur CIFS au lieu d'adresses IP LIF individuelles.

  Depuis ONTAP 9.4, SMB Multichannel permet d'améliorer le débit et la tolérance aux pannes des configurations Hyper-V et SQL Server sur SMB. Pour ce faire, vous devez avoir plusieurs cartes réseau 1G, 10G ou plus grandes déployées sur le cluster et les clients.

Configuration requise pour Data LIF

- La SVM hébergeant le serveur d'application sur la solution SMB doit disposer d'au moins une LIF de données opérationnelles sur chaque nœud du cluster.

  Les LIFs de données SVM peuvent basculer vers d'autres ports de données du cluster, y compris les nœuds qui n'hébergent pas actuellement les données accessibles par les serveurs applicatifs. De plus, comme le nœud Witness est toujours le partenaire SFO d'un nœud sur lequel le serveur d'applications est connecté, chaque nœud du cluster est un nœud potentiel Witness.

- Les LIF de données ne doivent pas être configurées pour rétablir automatiquement ces données.

  Après un événement de basculement ou de rétablissement, vous devez rétablir manuellement les LIF de données sur leurs ports de rattachement.

- Toutes les adresses IP de la LIF de données doivent disposer d'une entrée dans DNS et toutes les entrées doivent se résoudre au nom du serveur CIFS.

  Les serveurs d'applications doivent se connecter aux partages SMB à l'aide du nom du serveur CIFS. Ne configurez pas les serveurs d'application pour établir des connexions en utilisant les adresses IP de LIF.

- Si le nom du serveur CIFS est différent du nom du SVM, les entrées DNS doivent être résolus sur le nom du serveur CIFS.

Exigences en termes de volumes et de serveurs SMB pour Hyper-V sur SMB

Vous devez tenir compte de certaines exigences en matière de volume et de serveur SMB lors de la création de configurations Hyper-V sur SMB afin de garantir la continuité de l'activité.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

  Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

  Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

  Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres que les fichiers des machines Hyper-V, vous devez créer un SVM distinct pour ces données.

- L'authentification Kerberos et NTLM doit être autorisée dans le domaine auquel le serveur SMB appartient.

  ONTAP ne fait pas la promotion du service Kerberos pour VSS distant ; par conséquent, le domaine doit être défini pour autoriser NTLM.

- La fonctionnalité Shadow Copy doit être activée.

  Cette fonctionnalité est activée par défaut.

- Le compte de domaine Windows utilisé par le service de copie instantanée lors de la création de copies en double doit être membre du groupe local BULILTIN\Administrators ou BULILTIN\Backup Operators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

  Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les

migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Pour que les opérations de copie en mode « shadow » aient réussi, vous devez disposer de suffisamment d'espace disponible sur le volume.

  L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

Informations associées

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

Besoins en volume et serveur SMB pour SQL Server sur SMB

Pour assurer la continuité de l'activité, vous devez tenir compte des exigences en matière de volumes et de serveurs SMB lors de la création de configurations SQL Server sur SMB.

Configuration requise pour les serveurs SMB

- SMB 3.0 doit être activé.

  Cette option est activée par défaut.

- L'option de serveur CIFS utilisateur UNIX par défaut doit être configurée avec un compte utilisateur UNIX valide.

  Les serveurs d'applications utilisent le compte machine lors de la création d'une connexion SMB. Comme tout accès SMB nécessite que l'utilisateur Windows soit correctement mappé à un compte d'utilisateur UNIX ou au compte d'utilisateur UNIX par défaut, ONTAP doit pouvoir mapper le compte machine du serveur d'applications sur le compte d'utilisateur UNIX par défaut.

  En outre, SQL Server utilise un utilisateur de domaine comme compte de service SQL Server. Le compte de service doit également être mappé à l'utilisateur UNIX par défaut.

- Les référencements de nœuds automatiques doivent être désactivés (cette fonctionnalité est désactivée par défaut).

  Si vous souhaitez utiliser les référencements de nœuds automatiques pour l'accès aux données autres que les fichiers de bases de données SQL Server, vous devez créer un SVM distinct pour ces données.

- Le privilège SeSecurityPrivilege doit être attribué au compte utilisateur Windows utilisé pour installer SQL Server sur ONTAP.

  Ce privilège est attribué au groupe local BULTILTIN\Administrators du serveur SMB.

Besoins en termes de volume

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

Pour fournir des NDO aux serveurs d'applications utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume de type sécurité NTFS et l'utiliser directement pour les NDO sur des partages SMB. Si vous modifiez un volume de style de sécurité mixte en volume de style de sécurité NTFS et que vous envisagez de l'utiliser pour les NDO sur des partages SMB, vous devez placer manuellement une ACL en haut du volume et propager cette ACL à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations de sauvegarde du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

  Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

Informations associées

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

Exigences de partage constamment disponibles et considérations pour Hyper-V sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations Hyper-V sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

  Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled, vous ne pouvez pas placer de fichiers Hyper-V dans des partages contenant des jonctions.

  Dans le cas de la récupération automatique, la création de clichés instantanés échoue si une jonction est détectée lors du déplacement du partage. Dans le cas non auto-Recovery, la création de la copie en double ne échoue pas, mais la jonction ne pointe en rien.

- Si vous souhaitez utiliser les services de sauvegarde Remote VSS-enabled avec auto-Recovery, vous ne pouvez pas placer les fichiers Hyper-V dans des partages contenant les éléments suivants :
  - Symlinks, liens rigides ou widelinks

- Fichiers non standard

  La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers copie en double. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

- Pour que les opérations de clichés instantanés réussisse, vous devez disposer d'un espace disponible suffisant sur le volume (pour Hyper-V sur SMB uniquement).

  L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy. Cette exigence s'applique uniquement aux clichés instantanés avec la restauration automatique.

- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
  - Répertoire de base
  - Mise en cache des attributs
  - BranchCache

Considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge pour les configurations Hyper-V sur SMB :
  - Audit
  - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` paramètre défini sur `Yes`.

Exigences en matière de partages disponibles en permanence et considérations pour SQL Server sur SMB

Vous devez connaître certaines exigences et considérations relatives à la configuration de partages disponibles en continu pour les configurations SQL Server sur SMB qui prennent en charge la continuité de l'activité.

Exigences en matière de partage

- Les volumes utilisés pour stocker les fichiers de la machine virtuelle doivent être créés en tant que volumes de sécurité NTFS.

  Pour assurer la continuité de l'activité des serveurs applicatifs en utilisant des connexions SMB disponibles en continu, le volume contenant le partage doit être un volume NTFS. En outre, il doit toujours avoir été un volume NTFS. Vous ne pouvez pas modifier un volume mixte de style de sécurité ou un volume de style de sécurité UNIX en un volume NTFS de type sécurité, et l'utiliser directement pour la continuité de l'activité sur les partages SMB. Si vous remplacez un volume de style de sécurité mixte par un volume de style de sécurité NTFS et que vous prévoyez de l'utiliser pour assurer la continuité des opérations sur des partages SMB, vous devez placer manuellement une liste de contrôle d'accès en haut du volume et la propager à tous les fichiers et dossiers contenus. Autrement, les migrations de machine virtuelle ou les exportations de fichiers de base de données et les importations où les fichiers sont déplacés vers un autre volume peuvent échouer si les volumes source ou de destination ont été initialement créés sous forme de volumes

de sécurité mixtes ou UNIX, puis modifiés vers le style de sécurité NTFS.

- Les partages utilisés par les serveurs d'applications doivent être configurés avec le jeu de propriétés disponible en continu.

  Les serveurs d'application qui se connectent aux partages disponibles en permanence sont dotés de pointeurs permanents qui leur permettent de se reconnecter sans interruption aux partages SMB et de récupérer les verrouillages de fichiers après des événements perturbateurs, tels que le basculement, le rétablissement et le transfert d'agrégats.

- Bien que le volume contenant les fichiers de base de données puisse contenir des jonctions, SQL Server ne traverse pas les jonctions lors de la création de la structure du répertoire de base de données.
- Pour que les opérations du plug-in SnapCenter pour Microsoft SQL Server réussissent, vous devez disposer de suffisamment d'espace disponible sur le volume.

  Le volume sur lequel les fichiers de base de données SQL Server résident doit être suffisamment grand pour contenir la structure du répertoire de base de données et tous les fichiers contenus résidant dans le partage.

- Les propriétés de partage suivantes ne doivent pas être définies sur les partages disponibles en continu utilisés par les serveurs d'applications :
  - Répertoire de base
  - Mise en cache des attributs
  - BranchCache

Partager des considérations

- Les quotas sont pris en charge par les partages disponibles en permanence.
- La fonctionnalité suivante n'est pas prise en charge dans les configurations SQL Server sur SMB :
  - Audit
  - FPolicy
- L'analyse antivirus n'est pas réalisée sur les partages SMB avec le `continuously-availability` ensemble de propriétés de partage.

Considérations relatives à VSS distant pour les configurations Hyper-V sur SMB

Vous devez tenir compte de certains éléments à prendre en compte lors de l'utilisation de solutions de sauvegarde Remote VSS-enabled pour les configurations Hyper-V over SMB.

Considérations générales de VSS distant

- Un maximum de 64 partages peut être configuré par serveur d'applications Microsoft.

  L'opération de copie en double échoue si plus de 64 partages se trouvent dans un jeu de clichés instantanés. Il s'agit d'une condition requise par Microsoft.

- Un seul jeu de clichés instantanés actif par serveur CIFS est autorisé.

  Une opération de copie en double échouera si une opération de copie en double est en cours sur le même

serveur CIFS. Il s'agit d'une condition requise par Microsoft.

- Aucune jonction n'est autorisée dans la structure de répertoire sur laquelle VSS distant crée une copie en double.
  - Dans le cas de la restauration automatique, la création de clichés instantanés échouera si une jonction est rencontrée lors du déplacement du partage.
  - Dans le cas de restauration non automatique, la création de clichés instantanés ne échoue pas, mais la jonction ne pointe en rien.

Considérations relatives à la VSS distante qui ne s'appliquent qu'aux clichés instantanés avec restauration automatique

Certaines limites s'appliquent uniquement aux clichés instantanés avec restauration automatique.

- Une profondeur maximale de répertoire de cinq sous-répertoires est autorisée pour la création de clichés instantanés.

  Il s'agit de la profondeur du répertoire sur laquelle le service Shadow Copy crée un jeu de sauvegarde Shadow Copy. La création de clichés instantanés échoue si les répertoires contenant un fichier de machine virtuelle sont imbriqués de plus de cinq niveaux. Cela permet de limiter la traversée de répertoire lors du clonage du partage. La profondeur maximale de répertoire peut être modifiée à l'aide d'une option de serveur CIFS.

- La quantité d'espace disponible sur le volume doit être adéquate.

  L'espace disponible doit être au moins aussi grand que l'espace combiné utilisé par tous les fichiers, répertoires et sous-répertoires contenus dans les partages inclus dans le jeu de sauvegarde Shadow Copy.

- Aucun lien ou fichier non régulier n'est autorisé dans la structure de répertoires sur laquelle VSS distant crée une copie en double.

  La création de la copie en double échoue si des liens ou des fichiers non standard se trouvent dans le partage vers la copie en double. Le processus de clonage ne les prend pas en charge.

- Les répertoires ne sont pas autorisés à ACL NFSv4.

  Bien que la création de clichés instantanés conserve les listes de contrôle d'accès NFSv4 sur les fichiers, les listes de contrôle d'accès NFSv4 sur les répertoires sont perdues.

- Un maximum de 60 secondes est autorisé à créer un jeu de clichés instantanés.

  Les spécifications Microsoft permettent de créer le jeu de clichés instantanés pendant 60 secondes au maximum. Si le client VSS ne peut pas créer l'ensemble de clichés instantanés dans ce délai, l'opération de copie en double échoue ; ceci limite donc le nombre de fichiers dans un jeu de clichés instantanés. Le nombre réel de fichiers ou de machines virtuelles pouvant être inclus dans un jeu de sauvegardes varie ; ce nombre dépend de nombreux facteurs et doit être déterminé pour chaque environnement du client.

Conditions d'allègement de la charge des copies d'ODX pour SQL Server et Hyper-V sur SMB

L'allègement de la charge des copies (ODX) doit être activé pour migrer les fichiers de machines virtuelles ou pour exporter et importer les fichiers de base de données

directement depuis la source vers l'emplacement de stockage de destination, sans envoyer de données par le biais des serveurs applicatifs. Certaines exigences sont à prendre en compte lors de l'utilisation de l'allègement de la charge des copies d'ODX avec les solutions SQL Server et Hyper-V sur SMB.

L'utilisation de l'allègement de la charge des copies (ODX) offre des performances importantes. Cette option de serveur CIFS est activée par défaut.

- SMB 3.0 doit être activé pour utiliser l'allègement de la charge des copies (ODX).
- Les volumes source doivent être d'au moins 1.25 Go.
- La déduplication doit être activée sur les volumes utilisés avec l'allègement de la charge des copies.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

  Le type de compression secondaire n'est pas pris en charge
- Pour utiliser le délestage des copies ODX pour migrer des invités Hyper-V dans et entre les disques, les serveurs Hyper-V doivent être configurés pour utiliser des disques SCSI.

  La valeur par défaut consiste à configurer des disques IDE, mais l'allègement de charge des copies d'ODX ne fonctionne pas lorsque les invités sont migrés si des disques sont créés à l'aide de disques IDE.

Recommandations concernant les configurations SQL Server et Hyper-V sur SMB

Pour être certain que vos configurations SQL Server et Hyper-V sur SMB sont robustes et opérationnelles, vous devez connaître les meilleures pratiques recommandées lors de la configuration des solutions.

Recommandations générales

- Séparez les fichiers du serveur d'applications des données générales de l'utilisateur.

  Si possible, consacrer un SVM complet et son stockage aux données du serveur d'applications.
- Pour obtenir les meilleures performances, n'activez pas la signature SMB sur les SVM utilisés pour stocker les données du serveur d'applications.
- Pour des performances optimales et une meilleure tolérance aux pannes, SMB Multichannel permet de fournir plusieurs connexions entre ONTAP et les clients au cours d'une seule session SMB.
- Ne créez pas de partages disponibles en permanence sur d'autres partages que ceux utilisés dans la configuration Hyper-V ou SQL Server sur SMB.
- Désactiver l'alerte de modification sur les partages utilisés pour la disponibilité continue.
- N'effectuez pas de déplacement de volume simultanément au transfert d'agrégats (ARL), car les phases de l'ARL sont suspendues.
- Pour les solutions Hyper-V sur SMB, utilisez des disques iSCSI invités lors de la création de machines virtuelles en cluster. Partagée `.VHDX` Les fichiers ne sont pas pris en charge par Hyper-V sur SMB dans les partages ONTAP SMB.

Planifiez la configuration Hyper-V ou SQL Server sur SMB

Renseignez la fiche technique de configuration des volumes

Cette fiche fournit un moyen simple d'enregistrer les valeurs nécessaires lors de la création de volumes pour les configurations SQL Server et Hyper-V sur SMB.

Pour chaque volume, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

  Le nom du SVM est identique pour tous les volumes.

- Nom du volume
- Nom de l'agrégat

  Vous pouvez créer des volumes sur des agrégats situés sur n'importe quel nœud du cluster.

- Taille
- Un chemin de jonction

Lorsque vous créez des volumes utilisés pour stocker des données de serveur d'applications, vous devez garder à l'esprit les éléments suivants :

- Si le volume racine n'a pas de style de sécurité NTFS, vous devez spécifier le style de sécurité comme NTFS lorsque vous créez le volume.

  Par défaut, les volumes héritent du style de sécurité du volume root du SVM.

- Les volumes doivent être configurés avec la garantie d'espace du volume par défaut.
- Vous pouvez éventuellement configurer le paramètre de gestion de l'espace de dimensionnement automatique.
- Vous devez définir l'option qui détermine la réserve d'espace de snapshot sur `0`.
- La politique de snapshot appliquée au volume doit être désactivée.

  Si la politique de snapshot du SVM est désactivée, il n'est pas nécessaire de spécifier une politique de snapshot pour les volumes. Les volumes héritent de la policy Snapshot pour le SVM. Si la politique de snapshot de la SVM n'est pas désactivée et qu'elle est configurée pour créer des snapshots, vous devez spécifier une politique de snapshot au niveau du volume, et cette politique doit être désactivée. Les sauvegardes basées sur le service Shadow Copy et les sauvegardes SQL Server gèrent la création et la suppression de snapshots.

- Vous ne pouvez pas configurer de miroirs de partage de charge pour les volumes.

Les chemins de jonction sur lesquels vous prévoyez de créer des partages que les serveurs d'applications doivent être choisis de sorte qu'aucun volume relié par jonction ne se trouve sous le point d'entrée du partage.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle sur quatre volumes nommés « vol1 », « vol2 », « vol3 » et « vol4 », vous pouvez créer l'espace de noms indiqué dans l'exemple. Vous pouvez ensuite créer des partages pour les serveurs d'applications aux chemins suivants : `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, et `/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
```

Types d'information	Valeurs
Volume 1 : nom du volume, agrégat, taille, Junction path	
Volume 2 : nom du volume, agrégat, taille, chemin de jonction	
Volume 3 : nom du volume, agrégat, taille, chemin de jonction	
Volume 4 : nom du volume, agrégat, taille, chemin de jonction	
Volume 5 : nom du volume, agrégat, taille, chemin de jonction	
Volume 6 : nom du volume, agrégat, taille, chemin de jonction	
Volumes supplémentaires : nom du volume, agrégat, taille, Junction path	

Remplissez la fiche de configuration du partage SMB

Cette fiche vous permet d'enregistrer les valeurs dont vous avez besoin lors de la création de partages SMB disponibles en continu pour les configurations SQL Server et Hyper-V sur SMB.

Informations sur les propriétés des partages SMB et les paramètres de configuration

Pour chaque partage, vous devez spécifier les informations suivantes :

- Nom de la machine virtuelle de stockage (SVM)

  Le nom du SVM est identique pour tous les partages

- Nom de partage
- Chemin
- Propriétés du partage

  Vous devez configurer les deux propriétés de partage suivantes :

  - `oplocks`
  - `continuously-available`

Les propriétés de partage suivantes ne doivent pas être définies :

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Les symlinks doivent être désactivés (la valeur de l' `-symlink-properties` le paramètre doit être nul [""]).

Informations sur les chemins de partage

Si vous utilisez VSS distant pour sauvegarder les fichiers Hyper-V, il est important de choisir les chemins de partage à utiliser lors des connexions SMB des serveurs Hyper-V vers les emplacements de stockage dans lesquels sont stockés les fichiers des machines virtuelles. Bien que les partages peuvent être créés à tout moment dans l'espace de noms, les chemins pour les partages utilisés par les serveurs Hyper-V ne doivent pas contenir de volumes reliés. Les opérations de copie en double ne peuvent pas être effectuées sur des chemins de partage qui contiennent des points de jonction.

SQL Server ne peut pas traverser les jonctions lors de la création de la structure du répertoire de la base de données. Vous ne devez pas créer de chemins de partage pour SQL Server contenant des points de jonction.

Par exemple, si vous souhaitez stocker des fichiers de machine virtuelle ou de base de données sur des volumes « vol1 », « vol2 », « vol3 » et « vol4 », vous devez créer des partages pour les serveurs d'applications aux chemins suivants : `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, et `/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
```

Bien que vous puissiez créer des partages sur le `/data1` et les `/data2` chemins pour la gestion administrative, ne configurez pas les serveurs d'applications pour qu'ils utilisent ces partages pour stocker des données.

Fiche de planification

Types d'information	Valeurs
Volume 1 : nom du partage SMB et chemin	
Volume 2 : nom et chemin du partage SMB	
Volume 3 : nom et chemin du partage SMB	
Volume 4 : nom et chemin du partage SMB	
Volume 5 : nom et chemin du partage SMB	
Volume 6 : nom et chemin du partage SMB	
Volume 7 : nom et chemin du partage SMB	
Volumes supplémentaires : noms et chemins de partage SMB	

Créez des configurations ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server over SMB

Créez des configurations ONTAP pour la continuité de l'activité grâce à la présentation Hyper-V et SQL Server sur SMB

Vous devez effectuer plusieurs étapes de configuration ONTAP pour préparer les installations Hyper-V et SQL Server qui assurent la continuité de l'activité sur SMB.

Avant de créer la configuration ONTAP pour la continuité de l'activité avec Hyper-V et SQL Server sur SMB, les tâches suivantes doivent être effectuées :

- Les services de temps doivent être configurés sur le cluster.
- La mise en réseau doit être configurée pour le SVM.
- Le SVM doit être créé.
- Les interfaces LIF de données doivent être configurées sur le SVM.
- DNS doit être configuré sur le SVM.
- Les services de noms souhaités doivent être configurés pour la SVM.
- Le serveur SMB doit être créé.

Informations associées

Planifiez la configuration Hyper-V ou SQL Server sur SMB

Configuration requise et considérations

Vérifier que les authentifications Kerberos et NTLMv2 sont autorisées (Hyper-V sur les partages SMB)

La continuité de l'activité pour Hyper-V over SMB requiert que le serveur CIFS d'un SVM de données et le serveur Hyper-V autorisent l'authentification Kerberos et NTLMv2. Vous devez vérifier les paramètres du serveur CIFS et des serveurs Hyper-V qui contrôlent les méthodes d'authentification autorisées.

Description de la tâche

L'authentification Kerberos est requise lors de la mise en place d'une connexion de partage disponible en continu. Une partie du processus VSS distant utilise l'authentification NTLMv2. Par conséquent, les connexions utilisant les deux méthodes d'authentification doivent être prises en charge dans les configurations Hyper-V sur SMB.

Les paramètres suivants doivent être configurés pour autoriser l'authentification Kerberos et NTLMv2 :

- Les export policy pour SMB doivent être désactivées sur le serveur virtuel de stockage (SVM).

Les authentifications Kerberos et NTLMv2 sont toujours activées sur les SVM, mais les règles d'exportation peuvent être utilisées pour limiter l'accès en fonction de la méthode d'authentification.

Les export policy pour SMB sont facultatives et désactivées par défaut. Si les règles d'exportation sont désactivées, l'authentification Kerberos et NTLMv2 sont autorisées par défaut sur un serveur CIFS.

- Le domaine auquel le serveur CIFS et les serveurs Hyper-V appartiennent doit autoriser l'authentification Kerberos et NTLMv2.

L'authentification Kerberos est activée par défaut sur les domaines Active Directory. Toutefois, l'authentification NTLMv2 peut être refusée, en utilisant des paramètres de stratégie de sécurité ou des stratégies de groupe.

Étapes

1. Effectuer les opérations suivantes pour vérifier que les export policies sont désactivée sur le SVM:
   a. Définissez le niveau de privilège sur avancé :

      ```
      set -privilege advanced
      ```

   b. Vérifiez que le `-is-exportpolicy-enabled` L'option de serveur CIFS est définie sur `false`:

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

   c. Retour au niveau de privilège admin :

      ```
      set -privilege admin
      ```

2. Si les export policy pour SMB ne sont pas désactivées, désactivez-les :

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

3. Vérifiez que les authentifications NTLMv2 et Kerberos sont autorisées dans le domaine.

   Pour plus d'informations sur la détermination des méthodes d'authentification autorisées dans le domaine,

consultez la bibliothèque Microsoft TechNet.

4. Si le domaine n'autorise pas l'authentification NTMLv2, activez l'authentification NTLMv2 en utilisant l'une des méthodes décrites dans la documentation Microsoft.

Exemple

Les commandes suivantes vérifient que les export policies pour SMB sont désactivées sur le 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
```

Vérifiez que les comptes de domaine correspondent à l'utilisateur UNIX par défaut dans ONTAP

Hyper-V et SQL Server utilisent des comptes de domaine pour créer des connexions SMB à des partages disponibles en continu. Pour réussir la création de la connexion, le compte d'ordinateur doit être mappé avec un utilisateur UNIX. Le moyen le plus pratique pour y parvenir est de mapper le compte d'ordinateur à l'utilisateur UNIX par défaut.

Description de la tâche

Hyper-V et SQL Server utilisent les comptes d'ordinateur de domaine pour créer des connexions SMB. En outre, SQL Server utilise un compte d'utilisateur de domaine comme compte de service qui établit également des connexions SMB.

Lorsque vous créez une machine virtuelle de stockage (SVM), ONTAP crée automatiquement l'utilisateur par défaut nommé `pcuser` (avec un UID de `65534`) et le groupe nommé `pcuser` (avec un GID de `65534`), et ajoute l'utilisateur par défaut au `pcuser` groupe. Si vous configurez une solution Hyper-V sur SMB sur un SVM existant avant de mettre à niveau le cluster vers Data ONTAP 8.2, l'utilisateur et le groupe par défaut risquent de ne pas exister. Dans le cas contraire, vous devez les créer avant de configurer l'utilisateur UNIX par défaut du serveur CIFS.

Étapes

1. Déterminez s'il existe un utilisateur UNIX par défaut :

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

2. Si l'option utilisateur par défaut n'est pas définie, déterminez si un utilisateur UNIX peut être désigné comme utilisateur UNIX par défaut :

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

3. Si l'option utilisateur par défaut n'est pas définie et qu'aucun utilisateur UNIX ne peut être désigné comme utilisateur UNIX par défaut, créez le groupe par défaut et l'utilisateur UNIX par défaut, puis ajoutez l'utilisateur par défaut au groupe.
4. Le groupe par défaut reçoit généralement le nom de groupe « pcuser » Le GID attribué au groupe doit être `65534`.
   a. Créez le groupe par défaut :

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

   b. Créez l'utilisateur par défaut et ajoutez l'utilisateur par défaut au groupe par défaut :

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

   c. Vérifiez que l'utilisateur par défaut et le groupe par défaut sont correctement configurés :

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

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

5. Si l'utilisateur par défaut du serveur CIFS n'est pas configuré, effectuez les opérations suivantes :
   a. Configurez l'utilisateur par défaut :

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

   b. Vérifiez que l'utilisateur UNIX par défaut est configuré correctement :

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

6. Pour vérifier que le compte de l'ordinateur du serveur d'application correspond correctement à l'utilisateur par défaut, mappez un disque sur un partage résidant sur le SVM et confirmez que l'utilisateur Windows correspond au mappage utilisateur UNIX à l'aide de `vserver cifs session show` commande.

Pour en savoir plus, `vserver cifs options` consultez le "Référence de commande ONTAP".

Exemple

Les commandes suivantes déterminent que l'utilisateur par défaut du serveur CIFS n'est pas défini, mais déterminent que le `pcuser` utilisateur et `pcuser` groupe existe. Le `pcuser` l'utilisateur est affecté comme utilisateur par défaut du serveur CIFS sur 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           : -
```

Vérifier que le style de sécurité du volume root du SVM est défini sur NTFS

Pour assurer la continuité de l'activité pour Hyper-V et SQL Server sur SMB, des volumes doivent être créés avec le style de sécurité NTFS. Comme le style de sécurité du volume root est appliqué par défaut aux volumes créés sur la machine virtuelle de stockage (SVM), le style de sécurité du volume root doit être défini sur NTFS.

Description de la tâche

- Vous pouvez spécifier le style de sécurité du volume root au moment de la création de la SVM.
- Si le SVM n'est pas créé avec le volume root défini sur le style de sécurité NTFS, vous pouvez changer le style de sécurité plus tard en utilisant le `volume modify` commande.

Étapes

1. Déterminer la méthode de sécurité actuelle du volume root du SVM :

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

2. Si le volume racine n'est pas un volume de style de sécurité NTFS, remplacez le style de sécurité par NTFS :

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

3. Vérifier que le volume root du SVM est défini sur le style de sécurité NTFS :

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

Exemple

Les commandes suivantes vérifient que le style de sécurité du volume root est NTFS sur le 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
```

Vérifiez que les options requises pour les serveurs CIFS sont configurées

Vous devez vérifier que les options des serveurs CIFS requis sont activées et configurées conformément aux exigences de continuité de l'activité pour Hyper-V et SQL Server sur SMB.

Description de la tâche

- SMB 2.x et SMB 3.0 doivent être activés.
- L'allègement de la charge des copies (ODX) doit être activé pour que l'allègement de la performance des copies soit délesté.
- Les services VSS Shadow Copy doivent être activés si la solution Hyper-V sur SMB utilise des services de sauvegarde VSS distants (Hyper-V uniquement).

Étapes

1. Vérifier que les options des serveurs CIFS requis sont activées sur la machine virtuelle de stockage (SVM) :
   a. Définissez le niveau de privilège sur avancé :

      `set -privilege advanced`

   b. Saisissez la commande suivante :

      `vserver cifs options show -vserver *vserver_name*`

      Les options suivantes doivent être définies sur `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Hyper-V uniquement)
2. Si l'une des options n'est pas définie sur `true`, effectuez les opérations suivantes :

a. Réglez-les sur `true` à l'aide du `vserver cifs options modify` commande.

b. Vérifiez que les options sont définies sur `true` à l'aide du `vserver cifs options show` commande.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

Les commandes suivantes vérifient que les options requises pour la configuration Hyper-V sur SMB sont activées sur le SVM vs1. Dans l'exemple, l'allègement de la charge des copies (ODX) doit être activé pour répondre aux exigences des options.

```
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
```

Configurez SMB Multichannel pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. L'amélioration du débit et de la tolérance aux pannes pour les configurations Hyper-V et SQL Server sur SMB.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

  Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

  Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- `-max-connections-per-session`

  Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

  Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- `-max-lifs-per-session`

  Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Activez SMB Multichannel sur le serveur SMB :

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

3. Vérifiez que ONTAP signale les sessions SMB multicanaux :

```
vserver cifs session show
```

4. Retour au niveau de privilège admin :

```
set -privilege admin
```

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```
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
```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 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: -
```

Création de volumes de données NTFS

Vous devez créer des volumes de données NTFS sur la machine virtuelle de stockage (SVM) avant de pouvoir configurer les partages disponibles en continu pour une utilisation avec Hyper-V ou SQL Server sur les serveurs d'applications SMB. Utilisez la fiche de configuration des volumes pour créer vos volumes de données.

Description de la tâche

Vous pouvez utiliser des paramètres facultatifs pour personnaliser un volume de données. Pour plus d'informations sur la personnalisation des volumes, reportez-vous à la section "Gestion du stockage logique".

Lorsque vous créez vos volumes de données, vous ne devez pas créer de points de jonction au sein d'un volume contenant les éléments suivants :

- Hyper-V Files pour lesquels ONTAP crée des clichés instantanés
- Fichiers de base de données SQL Server sauvegardés à l'aide de SQL Server

Si vous créez par inadvertance un volume utilisant un style de sécurité mixte ou UNIX, vous ne pouvez pas le remplacer par un volume de style de sécurité NTFS, puis l'utiliser directement pour créer des partages disponibles en continu pour assurer la continuité de l'activité. La continuité de l'activité pour Hyper-V et SQL Server over SMB ne fonctionne pas correctement, sauf si les volumes utilisés dans la configuration sont créés en tant que volumes de sécurité NTFS.vous devez supprimer le volume et recréer le volume avec le style de sécurité NTFS, Vous pouvez également mapper le volume sur un hôte Windows et appliquer une liste de contrôle d'accès en haut du volume et propager la liste de contrôle d'accès à tous les fichiers et dossiers du volume.

Étapes

1. Créez le volume de données en entrant la commande appropriée :

Si vous souhaitez créer un volume dans un SVM où le root volume Security style…	Entrez la commande…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Pas 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. Vérifiez que la configuration de volume est correcte :

   `volume show -vserver vserver_name -volume volume_name`

Créer des partages SMB disponibles en permanence

Une fois les volumes de données créés, vous pouvez créer les partages disponibles en continu que les serveurs d'applications utilisent pour accéder aux fichiers de la machine virtuelle et de configuration Hyper-V ainsi qu'aux fichiers de la base de données SQL Server. Vous devez utiliser la fiche de configuration du partage lors de la création des partages SMB.

Étapes

1. Afficher des informations sur les volumes de données existants et leurs Junction paths :

   `volume show -vserver vserver_name -junction`

2. Créer un partage SMB disponible en continu :

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

- Vous pouvez éventuellement ajouter un commentaire à la configuration du partage.
- Par défaut, la propriété de partage de fichiers hors ligne est configurée sur le partage et est définie sur `manual`.
- ONTAP crée le partage avec l'autorisation de partage par défaut Windows de `Everyone` / `Full Control`.

3. Répétez l'étape précédente pour tous les partages de la fiche de configuration du partage.
4. Vérifiez que votre configuration est correcte à l'aide du `vserver cifs share show` commande.
5. Configurez les autorisations de fichiers NTFS sur les partages disponibles en permanence en mappant un lecteur sur chaque partage et en configurant les autorisations de fichiers à l'aide de la fenêtre **Propriétés Windows**.

Exemple

Les commandes suivantes créent un partage disponible en continu nommé « data2 » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1. Les symlinks sont désactivés en définissant l' `-symlink` paramètre à `""`:

```
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
```

Ajoutez le privilège SeSecurityPrivilege au compte d'utilisateur (pour SQL Server des partages SMB)

Le compte d'utilisateur de domaine utilisé pour installer le serveur SQL doit être affecté au privilège "`SteSecurityPrivilege" pour effectuer certaines actions sur le serveur CIFS qui exigent des privilèges non attribués par défaut aux utilisateurs de domaine.

Avant de commencer

Le compte de domaine utilisé pour installer SQL Server doit déjà exister.

Description de la tâche

Lors de l'ajout du privilège au compte du programme d'installation de SQL Server, ONTAP peut valider le compte en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Ajoutez le privilège "S`SecurityPrivilege" :

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

   La valeur pour le `-user-or-group-name` Paramètre est le nom du compte utilisateur de domaine utilisé pour l'installation de SQL Server.

2. Vérifiez que le privilège est appliqué au compte :

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

Exemple

La commande suivante ajoute le privilège "SteSecurityPrivilege" au compte du programme d'installation de SQL Server dans le domaine D'EXEMPLE pour la machine virtuelle de stockage (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
```

Configurer la profondeur du répertoire de copie « shadow » VSS (pour les partages Hyper-V sur SMB)

Vous pouvez également configurer la profondeur maximale des répertoires dans les partages SMB sur lesquels vous souhaitez créer des clichés instantanés. Ce paramètre est utile si vous souhaitez contrôler manuellement le niveau maximal de sous-répertoires

sur lesquels ONTAP doit créer des clichés instantanés.

Avant de commencer

La fonction VSS Shadow Copy doit être activée.

Description de la tâche

La valeur par défaut est de créer des clichés instantanés pour un maximum de cinq sous-répertoires. Si la valeur est définie sur `0`, ONTAP crée des clichés instantanés pour tous les sous-répertoires.

> Bien que vous puissiez spécifier que la profondeur du répertoire du jeu de clichés instantanés inclut plus de cinq sous-répertoires ou tous les sous-répertoires, Microsoft a besoin que la création du jeu de clichés instantanés soit terminée dans les 60 secondes. La création d'un jeu de clichés instantanés échoue s'il ne peut pas être terminé dans ce délai. La profondeur du répertoire de copie en double que vous choisissez ne doit pas entraîner le dépassement du délai de création.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Définissez la profondeur du répertoire de copie fantôme VSS au niveau souhaité :

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

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

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérez les configurations Hyper-V et SQL Server sur SMB

Configurez les partages existants pour assurer la disponibilité sans interruption

Vous pouvez modifier les partages existants pour devenir des partages disponibles en permanence que les serveurs d'applications Hyper-V et SQL Server utilisent pour accéder sans interruption aux fichiers de configuration et des machines virtuelles Hyper-V et aux fichiers de base de données SQL Server.

Description de la tâche

Vous ne pouvez pas utiliser un partage existant comme partage disponible en continu pour assurer la continuité de l'activité avec des serveurs applicatifs sur SMB si le partage présente les caractéristiques suivantes :

- Si le `homedirectory` la propriété partager est définie sur ce partage
- Si le partage contient des symlinks ou des widelinks activés
- Si le partage contient des volumes sous la racine du partage

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Les propriétés de partage suivantes doivent être configurées :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies. S'ils sont présents dans la liste des propriétés de partage actuelles, ils doivent être supprimés du partage disponible en continu :

- `attributecache`
- `branchcache`

Étapes

1. Afficher les paramètres de partage actuels et la liste actuelle des propriétés de partage configurées :

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

2. Si nécessaire, modifiez les paramètres de partage pour désactiver les liens symboliques et définissez les fichiers hors ligne sur manuel à l'aide de la `vserver cifs share modify` commande.
   - Vous pouvez désactiver les symlinks en définissant la valeur de l' `-symlink` paramètre à `""`.
   - Vous pouvez définir le `-offline-files` paramètre au réglage correct en spécifiant `manual`.
3. Ajoutez la `continuously-available` propriété de partage et, si nécessaire, la `oplocks` propriété de partage :

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

   Si le `oplocks` la propriété de partage n'est pas déjà définie, vous devez l'ajouter avec `continuously-available` propriété de partage.

4. Supprimez toutes les propriétés de partage qui ne sont pas prises en charge sur les partages disponibles en continu :

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

   Vous pouvez supprimer une ou plusieurs propriétés de partage en spécifiant les propriétés de partage avec une liste délimitée par des virgules.

5. Vérifiez que le `-symlink` et `-offline-files` les paramètres sont correctement réglés :

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

6. Vérifiez que la liste des propriétés de partage configurées est correcte :

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

Exemples

L'exemple suivant montre comment configurer un partage existant nommé « share1 » sur la machine virtuelle de stockage (SVM) « vs1 » pour les NDO avec un serveur d'application sur SMB :

- Les liens symboliques sont désactivés sur le partage en définissant le `-symlink` paramètre sur `""`.
- Le `-offline-file` le paramètre est modifié et défini sur `manual`.
- Le `continuously-available` la propriété de partage est ajoutée au partage.
- Le `oplocks` la propriété de partage figure déjà dans la liste des propriétés de partage ; il n'est donc pas nécessaire de l'ajouter.
- Le `attributecache` la propriété de partage est supprimée du partage.
- Le `browsable` La propriété de partage est facultative pour un partage disponible en continu utilisé pour les NDO avec des serveurs d'application sur SMB et est conservée comme une des propriétés de partage.

```
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
```

Activez ou désactivez les clichés instantanés VSS pour les sauvegardes Hyper-V sur SMB

Si vous utilisez une application de sauvegarde VSS pour sauvegarder les fichiers de machine virtuelle Hyper-V stockés sur des partages SMB, la copie Shadow VSS doit être activée. Vous pouvez désactiver la copie « shadow Copy VSS » si vous n'utilisez pas d'applications de sauvegarde « VSS Aware ». La valeur par défaut est d'activer la copie fantôme VSS.

Description de la tâche

Vous pouvez activer ou désactiver les clichés instantanés VSS à tout moment.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez que les clichés instantanés VSS soient…	Entrez la commande…
Activé	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
Désactivé	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemple

Les commandes suivantes permettent d'activer les clichés instantanés VSS sur le 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
```

Utilisez les statistiques pour surveiller l'activité Hyper-V et SQL Server sur SMB

Déterminez les objets statistiques et les compteurs disponibles dans ONTAP

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez déterminer…	Entrer…
Les objets disponibles	`statistics catalog object show`
Objets spécifiques disponibles	`statistics catalog object show -object` *`object_name`*
Quels compteurs sont disponibles	`statistics catalog counter show -object` *`object_name`*

   En savoir plus sur `statistics catalog object show` et `statistics catalog counter show` dans le "Référence de commande ONTAP" .

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
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
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au niveau de privilège avancé :

> Cet exemple n'affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.

```
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


[...]
```

Pour en savoir plus, `statistics start` consultez le "Référence de commande ONTAP".

Affiche les statistiques SMB dans ONTAP

Vous pouvez afficher différentes statistiques SMB pour surveiller les performances et diagnostiquer les problèmes.

Étapes

1. Utilisez le `statistics start` et en option `statistics stop` commandes pour collecter un échantillon de données.
2. Effectuez l'une des opérations suivantes :

Pour afficher les statistiques de…	Saisissez la commande suivante…
Toutes les versions de SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x et SMB 3.0	**`statistics show -object smb2`**
Sous-système SMB du nœud	**`statistics show -object nblade_cifs`**

Informations associées

- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Vérifiez que la configuration permet la continuité de l'activité

Utilisez le contrôle de l'état de l'intégrité pour déterminer si l'état de la continuité de l'activité fonctionne correctement

Le contrôle de l'état fournit des informations relatives à l'état du système sur le cluster. Le contrôle de l'état surveille les configurations Hyper-V et SQL Server sur SMB pour assurer la continuité de l'activité pour les serveurs applicatifs. Si l'état est dégradé, vous pouvez afficher des détails sur le problème, y compris la cause probable et les actions de récupération recommandées.

Il y a plusieurs moniteurs de santé. ONTAP contrôle à la fois l'état global du système et l'état de santé des personnes. Le contrôle de l'état de connectivité des nœuds contient le sous-système CIFS-NDO Le contrôle dispose d'un ensemble de règles d'intégrité qui déclenchent des alertes si certaines conditions physiques peuvent entraîner des interruptions et, si une condition de perturbation existe, génère des alertes et fournit des informations sur les actions correctives à mettre en œuvre. Pour les configurations NDO sur SMB, des alertes sont générées dans les deux conditions suivantes :

L'ID d'alerte	Gravité	Condition
HaNotReadyCifsNdo_Alert	Majeur	Un ou plusieurs fichiers hébergés par un volume dans un agrégat du nœud ont été ouverts via un partage SMB disponible en continu, avec la promesse de persistance en cas de défaillance. Cependant, la relation de haute disponibilité avec le partenaire n'est pas configurée ou n'est pas saine.
NoStandbyLifCifsNdo_Alert	Mineur	Le SVM (Storage Virtual machine) transmet activement les données via SMB via un nœud, et les fichiers SMB sont ouverts de manière continue sur des partages disponibles. Cependant, son nœud partenaire n'expose pas de LIF de données actives pour la SVM.

Affichez l'état de l'opération sans interruption grâce à la surveillance de l'état du système

Vous pouvez utiliser le `system health` Commandes permettant d'afficher des informations relatives à l'état global du cluster et à l'état de santé du sous-système CIFS-NDO, de répondre aux alertes, de configurer les alertes futures et d'afficher des informations sur la configuration du contrôle de l'état.

Étapes

1. Surveillez l'état de l'état de santé en effectuant l'action appropriée :

Si vous voulez afficher…	Entrez la commande…
L'état d'intégrité du système, qui reflète l'état global des moniteurs d'état individuels	**system health status show**
Informations sur l'état de santé du sous-système CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Afficher des informations sur la configuration de la surveillance des alertes CIFS-NDO en effectuant les actions appropriées :

Pour afficher des informations sur…	Entrez la commande…
La configuration et l'état du contrôle de l'état du sous-système CIFS-NDO, tels que les nœuds contrôlés, l'état d'initialisation et l'état	**system health config show -subsystem CIFS-NDO**

Pour afficher des informations sur…	Entrez la commande…
CIFS-NDO signale qu'un contrôle de l'état peut générer	**system health alert definition show -subsystem CIFS-NDO**
Règles de contrôle de l'état de la CONTINUITÉ de l'ACTIVITÉ CIFS qui déterminent la date d'émission des alertes	**system health policy definition show -monitor node-connect**

Utilisez le `-instance` paramètre pour afficher des informations détaillées.

Exemples

Le résultat suivant affiche des informations sur l'état d'intégrité global du cluster et le sous-système 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
```

Le résultat suivant affiche des informations détaillées sur la configuration et l'état du contrôle de l'état du sous-système 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
```

Vérifiez la configuration du partage SMB disponible en continu

Pour prendre en charge la continuité de l'activité, les partages SMB Hyper-V et SQL Server doivent être configurés en tant que partages disponibles en continu. En outre, vous devez vérifier certains autres paramètres de partage. Vérifiez que les partages sont correctement configurés pour assurer la continuité de l'activité des serveurs applicatifs en cas d'événements planifiés ou non.

Description de la tâche

Vous devez vérifier que les deux paramètres de partage suivants sont correctement définis :

- Le `-offline-files` le paramètre est défini sur l'un ou l'autre `manual` (valeur par défaut) ou `none`.
- Les symlinks doivent être désactivés.

Pour garantir la continuité de l'activité, les propriétés de partage suivantes doivent être définies :

- `continuously-available`
- `oplocks`

Les propriétés de partage suivantes ne doivent pas être définies :

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

Étapes

1. Vérifiez que les fichiers hors ligne sont définis sur `manual` ou `disabled` et que les symlinks sont désactivés :

   vserver cifs shares show -vserver *vserver_name*

2. Vérifiez que les partages SMB sont configurés pour une disponibilité continue :

   vserver cifs shares properties show -vserver *vserver_name*

Exemples

L'exemple suivant présente le paramètre de partage d'un partage nommé « `sunre1' » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) vs1. Les fichiers hors ligne sont définis sur `manual` et les symlinks sont désactivés (désignés par un tiret dans le `Symlink Properties` sortie de champ) :

```
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
```

L'exemple suivant affiche les propriétés de partage d'un partage nommé «`sunre1'» sur la SVM vs1 :

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

Vérifiez l'état du LIF

Même si vous configurez des SVM (Storage Virtual machines) avec des configurations Hyper-V et SQL Server over SMB pour avoir des LIF sur chaque nœud d'un cluster, au cours des opérations quotidiennes, certaines LIF peuvent être déplacées vers des ports sur un autre nœud. Vous devez vérifier le statut de la LIF et prendre les mesures correctives nécessaires.

Description de la tâche

Pour assurer la prise en charge transparente et sans interruption de l'activité, chaque nœud d'un cluster doit disposer d'au moins une LIF pour le SVM et toutes les LIF doivent être associées à un port de rattachement. Si certaines des LIFs configurées ne sont actuellement pas associées à leur port de base, vous devez résoudre un problème de port, puis rétablir les LIF sur leur port de base.

Étapes

1. Afficher les informations relatives aux LIFs configurées pour le SVM :

   network interface show -vserver *vserver_name*

Dans cet exemple, « lites1 » n'est pas situé sur le port d'attache.

`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
```

Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

2. Si certaines des LIFs ne se trouvent pas sur leurs ports de home, effectuez les opérations suivantes :

   a. Pour chaque LIF, déterminez ce que le port de base de la LIF est :

      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. Pour chaque LIF, déterminez si le port de base de la LIF est active :

      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
      ```

      Dans cet exemple, « lie1 » doit être remigré vers son port d'origine, `node1:e0d`.

   Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

3. Si l'une des interfaces réseau du port de attache à laquelle les LIFs doivent être associées n'est pas dans `up` l'état, résolvez le problème afin que ces interfaces fonctionnent. Pour en savoir plus, `up` consultez le

"Référence de commande ONTAP".

4. Si besoin, rerestaurez les LIF sur leurs ports de base :

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

   network interface revert -vserver vs1 -lif lif1

   Pour en savoir plus, `network interface revert` consultez le "Référence de commande ONTAP".

5. Vérifier que chaque nœud du cluster dispose d'une LIF active pour le 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
```

Déterminez si les sessions SMB sont disponibles en continu

Affiche les informations relatives aux sessions SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et son niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

  Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.

- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
Pour toutes les sessions sur le SVM sous forme résumée	**vserver cifs session show -vserver *vserver_name***
Sur un ID de connexion spécifié	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
À partir d'une adresse IP de poste de travail spécifiée	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Sur une adresse IP LIF spécifiée	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Sur un nœud spécifié	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	D'un utilisateur Windows spécifié
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Le format de `user_name` est `[domain]\user`.	Avec un mécanisme d'authentification spécifié

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
`vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism` La valeur pour `-auth -mechanism` peut être l'une des suivantes : • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Avec une version de protocole spécifiée

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version La valeur pour `-protocol-version` peut être l'une des suivantes : • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Avec un niveau spécifié de protection disponible en continu

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
`vserver cifs session show -vserver` ***`vserver_name`*** **`-continuously -available`** ***`continuously_available_protection_level`*** La valeur pour `-continuously -available` peut être l'une des suivantes : • `No` • `Yes` • `Partial`	Avec un état de session de signature SMB spécifié

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse 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
```

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

```
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
```

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en continu.

ouvert en continu
disponible
mais que
sont pas
ouverts
avec une
protection
disponible
en
continu.

continu.

```
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
```

Affiche des informations sur les fichiers SMB ouverts dans ONTAP

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez également afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM (Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show`

commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
Sur le SVM sous forme résumée	**vserver cifs session file show -vserver *vserver_name***
Sur un nœud spécifié	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Sur un ID de fichier spécifié
vserver cifs session file show -vserver *vserver_name* -file-id integer	Sur un ID de connexion SMB spécifié
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Sur un ID de session SMB spécifié
vserver cifs session file show -vserver *vserver_name* -session-id integer	Sur l'agrégat d'hébergement spécifié
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Sur le volume spécifié
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Sur le chemin SMB spécifié
vserver cifs session file show -vserver *vserver_name* -path *path*	Avec le niveau spécifié de protection disponible en continu
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* La valeur pour `-continuously-available` peut être l'une des suivantes : • `No` • `Yes` Si l'état disponible en continu est de `No`, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité.	Avec l'état reconnecté spécifié

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le 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
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le 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
```

Informations sur le copyright

Informations sur les marques commerciales