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

ONTAP 9

NetApp
April 24, 2024

Sommaire

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 sont mis en correspondance avec l'utilisateur UNIX par défaut

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 un SVM (Storage Virtual machine), ONTAP crée automatiquement l'utilisateur par défaut nommé « pcuser » (avec un UID sur `65534`) Et le groupe nommé « pcuser » (avec un GID de `65534`), et ajoute l'utilisateur par défaut au groupe « pcuser ». 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'il n'y a pas d'utilisateur UNIX qui peut être désigné comme utilisateur UNIX par défaut, créez l'utilisateur UNIX par défaut et le groupe par défaut, puis ajoutez l'utilisateur par défaut au groupe.

Généralement, l'utilisateur par défaut est nommé « pcuser » et doit être affecté à l'UID de `65534`. Le groupe par défaut est généralement attribué au nom de groupe « pcuser ». Le GID affecté au groupe doit être de `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

4. 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*

5. 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 plus d'informations sur l'utilisation de cette commande, consultez les pages de manuels.

Exemple

Les commandes suivantes déterminent que l'utilisateur par défaut du serveur CIFS n'est pas défini, mais déterminent que l'utilisateur « pcuser » et le groupe « pcuser » existent. L'utilisateur « pcuser » est attribué en tant qu'utilisateur par défaut du serveur CIFS sur le 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.

Ce dont vous avez besoin

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 options 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 xref:./smb-hyper-v-sql/"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.

Ce dont vous avez besoin

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.

Ce dont vous avez besoin

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
   ```