



Configurez votre environnement Virtual Storage Console pour VMware vSphere VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/vsc-vasa-provider-sra-97/deploy/reference-esx-host-values-set-by-vsc-for-vmware-vsphere.html> on March 21, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configurez votre environnement Virtual Storage Console pour VMware vSphere	1
Configurer les paramètres de chemins d'accès multiples et de délai d'attente du serveur ESXi	1
Régénérer un certificat SSL pour Virtual Storage Console	7
Conditions requises pour l'enregistrement de VSC dans un environnement de plusieurs serveurs vCenter	7
Configurez les fichiers de préférences VSC	8
Activez le montage du datastore sur différents sous-réseaux	10
Accédez aux options de la console de maintenance de l'appliance virtuelle pour VSC, VASA Provider et SRA	11
Modifiez le mot de passe administrateur	13
Configurez la haute disponibilité de l'appliance virtuelle pour VSC, VASA Provider et SRA	13
Configurations MetroCluster prises en charge par l'appliance virtuelle pour VSC, VASA Provider et SRA ..	15

Configurez votre environnement Virtual Storage Console pour VMware vSphere

(VSC) prend en charge de nombreux environnements. Certaines fonctionnalités de ces environnements peuvent nécessiter une configuration supplémentaire.

Vous devrez peut-être effectuer les tâches suivantes pour configurer vos hôtes ESXi, les systèmes d'exploitation invités et VSC :

- Vérification des paramètres de l'hôte ESXi, y compris les paramètres UNMAP
- Ajout de valeurs de délai d'attente pour les systèmes d'exploitation invités
- Régénération du certificat SSL VSC
- Création de profils de capacité de stockage et d'alarmes de seuil
- Modification du fichier de préférences pour permettre le montage de datastores sur différents sous-réseaux

Configurer les paramètres de chemins d'accès multiples et de délai d'attente du serveur ESXi

Virtual Storage Console pour VMware vSphere vérifie et définit les paramètres de chemins d'accès multiples de l'hôte ESXi ainsi que les paramètres de délai d'expiration de la carte HBA qui fonctionnent le mieux avec les systèmes de stockage.

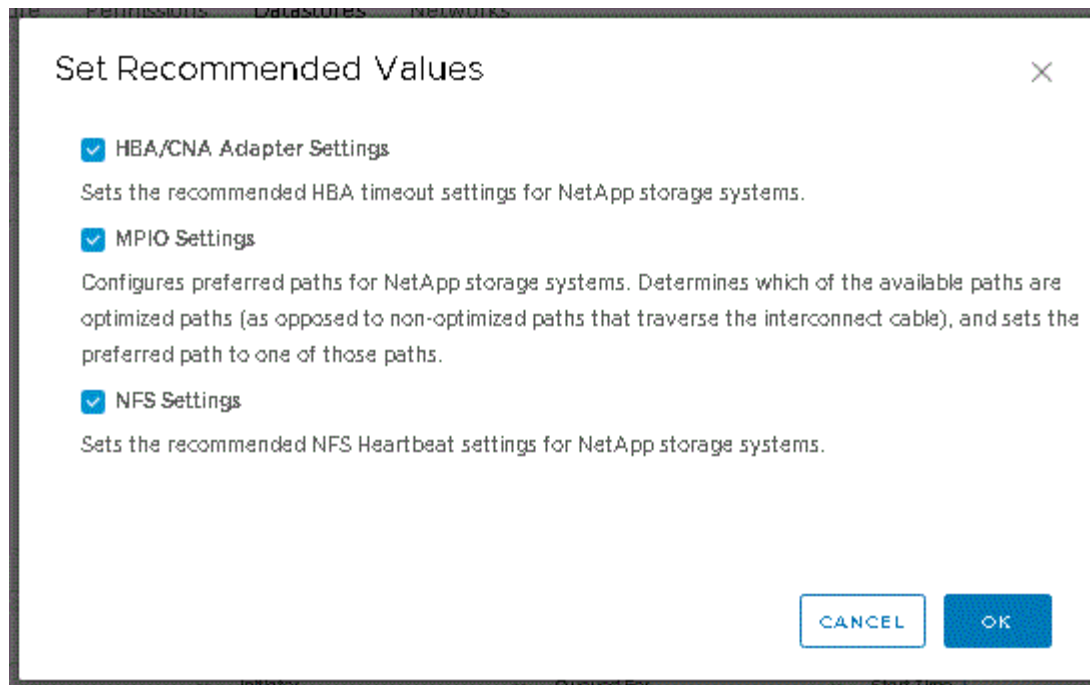
Description de la tâche

Ce processus peut prendre un certain temps, selon votre configuration et la charge du système. La progression de la tâche s'affiche dans le panneau **tâches récentes**. Lorsque les tâches sont terminées, l'icône d'alerte d'état de l'hôte est remplacée par l'icône Normal ou l'icône redémarrage en attente.

Étapes

1. Dans la page Web client VMware vSphere **Home**, cliquez sur **vCenter** > **hosts**.
2. Cliquez avec le bouton droit sur un hôte, puis sélectionnez menu :actions [NetApp VSC > définir les valeurs recommandées].
3. Dans la boîte de dialogue **Paramètres recommandés NetApp**, sélectionnez les valeurs qui conviennent le mieux à votre système.

Les valeurs standard recommandées sont définies par défaut.



4. Cliquez sur **OK**.

Valeurs de l'hôte ESXi définies à l'aide de Virtual Storage Console pour VMware vSphere

Vous pouvez définir des délais d'expiration et d'autres valeurs sur les hôtes ESXi à l'aide de Virtual Storage Console pour VMware vSphere pour garantir des performances optimales et un basculement réussi. Les valeurs obtenues par Virtual Storage Console (VSC) reposent sur des tests internes.

Vous pouvez définir les valeurs suivantes sur un hôte ESXi :

Configuration avancée ESXi

- **VMFS3.HardwareAccélérationde Locaking**

Vous devez définir cette valeur sur 1.

- **VMFS3.EnableBlockDelete**

Vous devez définir cette valeur sur 0.

Paramètres NFS

- **Net.TcpipHeapSize**

Si vous utilisez vSphere 6.0 ou version ultérieure, vous devez définir cette valeur sur 32.

- **Net.TcpipHeapMax**

Si vous utilisez vSphere 6.0 ou version ultérieure, vous devez définir cette valeur sur 1536.

- **NFS.Maxvolumes**

Si vous utilisez vSphere 6.0 ou version ultérieure, vous devez définir cette valeur sur 256.

- **NFS41.MaxVolumes**

Si vous utilisez vSphere 6.0 ou version ultérieure, vous devez définir cette valeur sur 256.

- **NFS.MaxQueueDepth**

Si vous utilisez la version vSphere 6.0 ou ultérieure de l'hôte ESXi, vous devez définir cette valeur sur 128 ou plus pour éviter les goulots d'étranglement dans la mise en file d'attente.

Dans le cas des versions vSphere antérieures à la version 6.0, définissez cette valeur sur 64.

- **NFS.HeartbeatMaxFailures**

Définissez cette valeur sur 10 pour toutes les configurations NFS.

- **NFS.HeartbeatFrequency**

Définissez cette valeur sur 12 pour toutes les configurations NFS.

- **NFS.HeartbeatTimeout**

Définissez cette valeur sur 5 pour toutes les configurations NFS.

Paramètres FC/FCoE

- **Politique de sélection de chemin**

Vous devez définir cette valeur sur « RR » (Round Robin) lorsque des chemins FC avec ALUA sont utilisés.

Vous devez définir cette valeur sur « FIXE » pour toutes les autres configurations.

La définition de cette valeur sur « RR » permet d'équilibrer la charge entre tous les chemins actifs/optimisés. La valeur « FIXE » est utilisée pour les anciennes configurations non ALUA et permet d'éviter les E/S proxy

- **Disk.QFullSampleSize**

Définissez cette valeur sur 32 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.

- **Disk.QFullThreshold**

Définissez cette valeur sur 8 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.

- **Délais de connexion HBA FC Emulex**

Utilisez la valeur par défaut.

- **Délais de connexion HBA FC QLogic**

Utilisez la valeur par défaut.

Paramètres iSCSI

- **Politique de sélection de chemin**

Vous devez définir cette valeur sur « RR » pour tous les chemins iSCSI.

La définition de cette valeur sur « RR » permet d'équilibrer la charge entre tous les chemins actifs/optimisés.

- **Disk.QFullSampleSize**

Définissez cette valeur sur 32 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.

- **Disk.QFullThreshold**

Définissez cette valeur sur 8 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.

Configurer les scripts des systèmes d'exploitation invités

Les images ISO des scripts du système d'exploitation invité sont montées sur la console de stockage virtuel pour le serveur VMware vSphere. Pour utiliser les scripts du système d'exploitation invité afin de définir les délais de stockage des machines virtuelles, vous devez monter les scripts à partir du client vSphere.

Type de système d'exploitation	paramètres de temporisation de 60 secondes	paramètres de temporisation de 190 secondes
Linux	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso</code>
Répertoires de base	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso</code>
Solaris	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso</code>

Vous devez installer le script à partir de la copie de l'instance VSC enregistrée sur vCenter Server qui gère la machine virtuelle. Si votre environnement inclut plusieurs serveurs vCenter, sélectionnez le serveur qui contient la machine virtuelle pour laquelle vous souhaitez définir les valeurs de délai de stockage.

Vous devez vous connecter à la machine virtuelle, puis exécuter le script pour définir les valeurs de délai de

stockage.

Définissez les valeurs de délai d'expiration des systèmes d'exploitation invités Windows

Les scripts d'expiration du délai d'attente du système d'exploitation invité (OS) définissent les paramètres d'expiration du délai d'E/S SCSI pour les systèmes d'exploitation invités Windows. Vous pouvez spécifier un délai de 60 secondes ou un délai de 190 secondes. Vous devez redémarrer le système d'exploitation invité Windows pour que les paramètres prennent effet.

Avant de commencer

Vous devez avoir monté l'image ISO contenant le script Windows.

Étapes

1. Accédez à la console de la machine virtuelle Windows et connectez-vous à un compte disposant des privilèges d'administrateur.
2. Si le script ne démarre pas automatiquement, ouvrez le lecteur de CD, puis exécutez le `windows_gos_timeout.reg` script.

La boîte de dialogue Éditeur du Registre s'affiche.

3. Cliquez sur **Oui** pour continuer.

Le message suivant s'affiche : The keys and values contained in
D:\windows_gos_timeout.reg have been successfully added to the registry.

4. Redémarrez le système d'exploitation invité Windows.
5. Démontez l'image ISO.

Définissez les valeurs de délai d'expiration pour les systèmes d'exploitation invités Solaris

Les scripts d'expiration du délai d'attente du système d'exploitation invité (OS) définissent les paramètres d'expiration du délai d'E/S SCSI pour Solaris 10. Vous pouvez spécifier un délai de 60 secondes ou un délai de 190 secondes.

Avant de commencer

Vous devez avoir monté l'image ISO contenant le script Solaris.

Étapes

1. Accédez à la console de la machine virtuelle Solaris et connectez-vous à un compte disposant des privilèges root.
2. Exécutez le `solaris_gos_timeout-install.sh` script.

Pour Solaris 10, un message similaire à ce qui suit s'affiche :

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

3. Démontez l'image ISO.

Définissez les valeurs de délai d'expiration des systèmes d'exploitation invités Linux

Les scripts d'expiration du délai d'attente du système d'exploitation invité (OS) définissent les paramètres d'expiration du délai d'E/S SCSI pour les versions 4, 5, 6 et 7 de Red Hat Enterprise Linux et les versions 9, 10 et 11 de SUSE Linux Enterprise Server. Vous pouvez spécifier un délai de 60 secondes ou un délai de 190 secondes. Vous devez exécuter le script à chaque mise à niveau vers une nouvelle version de Linux.

Avant de commencer

Vous devez avoir monté l'image ISO contenant le script Linux.

Étapes

1. Accédez à la console de la machine virtuelle Linux et connectez-vous à un compte disposant des privilèges root.
2. Exécutez le `linux_gos_timeout-install.sh` script.

Pour Red Hat Enterprise Linux 4 ou SUSE Linux Enterprise Server 9, un message similaire à ce qui suit s'affiche :

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Pour Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 et Red Hat Enterprise Linux 7, un message similaire à ce qui suit s'affiche :

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Pour SUSE Linux Enterprise Server 10 ou SUSE Linux Enterprise Server 11, un message similaire au message suivant s'affiche :


```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

3. Démontez l'image ISO.

Régénérer un certificat SSL pour Virtual Storage Console

Le certificat SSL est généré lors de l'installation de (VSC). Le nom distinctif (DN) généré pour le certificat SSL peut ne pas être un nom commun (CN) reconnu par les ordinateurs clients. En modifiant les mots de passe du magasin de clés et de la clé privée, vous pouvez régénérer le certificat et créer un certificat spécifique au site.

Description de la tâche

Vous pouvez activer le diagnostic à distance à l'aide de la console de maintenance et générer un certificat spécifique au site.

["Réponse de la base de connaissances NetApp 1075654 : Virtual Storage Console 7.x : mise en œuvre de certificats signés par une autorité de certification"](#)

Étapes

1. Connectez-vous à la console de maintenance.
2. Entrez 1 pour accéder au Application Configuration menu.
3. Dans le Application Configuration entrée, menu 3 Pour arrêter le service VSC.
4. Entrez 7 Pour régénérer le certificat SSL.

Conditions requises pour l'enregistrement de VSC dans un environnement de plusieurs serveurs vCenter

Si vous utilisez Virtual Storage Console pour VMware vSphere dans un environnement où un seul client VMware vSphere HTML5. Gère plusieurs instances de vCenter Server, vous devez enregistrer une instance de VSC avec chaque vCenter Server de sorte qu'il existe une association 1:1 entre VSC et vCenter Server. Cela vous permet de gérer tous les serveurs exécutant vCenter 6.0 ou version ultérieure en mode lié et en mode non lié à partir d'un seul client HTML5 vSphere.



Si vous souhaitez utiliser VSC avec un serveur vCenter, vous devez avoir configuré ou enregistré une instance VSC pour chaque instance de vCenter Server à gérer. Chaque instance VSC enregistrée doit avoir la même version.

Le mode lié est installé automatiquement pendant le déploiement de vCenter Server. Le mode lié utilise LE mode d'application Microsoft Active Directory (ADAM) pour stocker et synchroniser des données sur plusieurs systèmes vCenter Server.

L'utilisation du client HTML5 vSphere pour effectuer des tâches VSC sur plusieurs serveurs vCenter nécessite l'exécution des tâches suivantes :

- Chaque serveur vCenter dans l'inventaire VMware que vous souhaitez gérer doit disposer d'un seul serveur VSC enregistré avec lui sous une configuration unique 1:1.

Par exemple, vous pouvez faire enregistrer le serveur VSC A sur vCenter Server A, le serveur VSC B enregistré sur vCenter Server B, le serveur VSC C enregistré sur vCenter Server C, etc.

Le serveur VSC A ne peut pas être enregistré sur vCenter Server A et vCenter Server B.

Si un inventaire VMware inclut un serveur vCenter ne possédant pas de serveur VSC enregistré, mais un ou plusieurs serveurs vCenter sont enregistrés auprès de VSC, Vous pouvez alors afficher les instances de VSC et effectuer des opérations VSC pour les serveurs vCenter sur lesquels VSC est enregistré.

- Vous devez disposer du privilège View spécifique à VSC pour chaque serveur vCenter enregistré sur la connexion unique (SSO).

Vous devez également disposer des autorisations RBAC appropriées.

Lorsque vous effectuez une tâche qui nécessite la spécification d'un serveur vCenter, la liste déroulante **vCenter Server** affiche les serveurs vCenter disponibles dans l'ordre alphanumérique. Le serveur vCenter par défaut est toujours le premier serveur de la liste déroulante.

Si l'emplacement du stockage est connu (par exemple, lorsque vous utilisez l'assistant **Provisioning** et que le datastore se trouve sur un hôte géré par un serveur vCenter spécifique), la liste vCenter Server s'affiche sous forme d'option en lecture seule. Cela se produit uniquement lorsque vous utilisez l'option clic droit pour sélectionner un élément dans vSphere Web client.

VSC vous avertit lorsque vous essayez de sélectionner un objet qu'il ne gère pas.

Vous pouvez filtrer les systèmes de stockage basés sur un serveur vCenter spécifique depuis la page de résumé de VSC. Une page récapitule les instances VSC enregistrées avec un serveur vCenter. Vous pouvez gérer les systèmes de stockage associés à une instance VSC et à vCenter Server spécifique, mais vous devez séparer les informations d'enregistrement de chaque système de stockage si vous exécutez plusieurs instances de VSC.

Configurez les fichiers de préférences VSC

Les fichiers de préférences contiennent des paramètres qui contrôlent Virtual Storage Console pour les opérations VMware vSphere. Dans la plupart des cas, il n'est pas nécessaire de modifier les paramètres de ces fichiers. Il est utile de savoir quels fichiers de préférences (VSC) utilisent.

VSC possède plusieurs fichiers de préférences. Ces fichiers incluent des clés d'entrée de gamme et des

valeurs qui déterminent la façon dont VSC effectue diverses opérations. Voici quelques fichiers de préférences utilisés par VSC :

```
/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml
```

```
/opt/netapp/vscserver/etc/vsc/vscPreferences.xml
```

Vous devrez peut-être modifier les fichiers de préférences dans certaines situations. Par exemple, si vous utilisez iSCSI ou NFS et que le sous-réseau est différent entre vos hôtes ESXi et votre système de stockage, vous devez modifier les fichiers de préférences. Si vous ne modifiez pas les paramètres du fichier de préférences, le provisionnement des datastores échoue car VSC ne peut pas monter le datastore.

Définissez IPv4 ou IPv6

Une nouvelle option est ajoutée au fichier de préférences `kaminoprefs.xml` Que vous pouvez définir pour activer la prise en charge d'IPv4 ou d'IPv6 pour tous les systèmes de stockage ajoutés à VSC.

- Le `default.override.option.provision.mount.datastore.address.family` le paramètre a été ajouté au `kaminoprefs.xml` Fichier de préférences pour définir un protocole LIF de données préféré pour le provisionnement de datastores.

Cette préférence s'applique à tous les systèmes de stockage ajoutés à VSC.

- Les valeurs de la nouvelle option sont IPv4, IPv6, et NONE.
- Par défaut, la valeur est définie sur NONE.

Valeur	Description
AUCUNE	<ul style="list-style-type: none">• Le provisionnement se produit via la même LIF de données IPv6 ou IPv4 que le type de LIF de données de cluster ou de gestion utilisé pour l'ajout du stockage.• Si le même type d'adresse IPv6 ou IPv4 de LIF de données n'est pas présent dans le , alors le provisionnement se produit via l'autre type de LIF de données, si disponible.
IPv4	<ul style="list-style-type: none">• Le provisionnement se produit à l'aide de la LIF de données IPv4 dans la .• Si ne dispose pas de LIF de données IPv4, le provisionnement se fait via la LIF de données IPv6, si elle est disponible dans .
IPv6	<ul style="list-style-type: none">• Le provisionnement se produit à l'aide de la LIF de données IPv6 dans la .• Si ne dispose pas d'une LIF de données IPv6, le provisionnement se fait via la LIF de données IPv4, si elle est disponible dans .

Activez le montage du datastore sur différents sous-réseaux

Si vous utilisez iSCSI ou NFS et que le sous-réseau est différent entre vos hôtes ESXi et votre système de stockage, vous devez modifier les fichiers de préférences de Virtual Storage Console pour VMware vSphere. Si vous ne modifiez pas le fichier de préférences, l'approvisionnement du datastore échoue car (VSC) ne peut pas monter le datastore.

Description de la tâche

Lorsque le provisionnement du datastore échoue, VSC consigne les messages d'erreur suivants :

```
Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts."
```

Étapes

1. Connectez-vous à votre instance de vCenter Server.
2. Lancez la console de maintenance à l'aide de votre machine virtuelle d'appliance unifiée.

["Accédez aux options de la console de maintenance de l'appliance virtuelle pour VSC, VASA Provider et SRA"](#)
3. Entrez 4 Pour accéder à l'option **support et Diagnostics**.
4. Entrez 2 Pour accéder à l'option **Access diagnostic Shell**.
5. Entrez `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` pour mettre à jour le `kaminoprefs.xml` fichier.
6. Mettez à jour le `kaminoprefs.xml` fichier.

Si vous utilisez...	Procédez comme ça...
ISCSI	Modifiez la valeur de la clé d'entrée <code>default.allow.iscsi.mount.networks</code> De TOUT à la valeur de vos réseaux hôtes VMware ESXi.
NFS	Modifiez la valeur de la clé d'entrée <code>default.allow.nfs.mount.networks</code> De TOUT à la valeur de vos réseaux hôtes VMware ESXi.

Le fichier de préférences contient des exemples de valeurs pour ces clés de saisie.



La valeur « TOUS » ne signifie pas tous les réseaux. La valeur « TOUS » permet d'utiliser tous les réseaux de correspondance, entre l'hôte et le système de stockage, pour le montage de datastores. Lorsque vous spécifiez des réseaux hôtes, vous ne pouvez activer le montage que sur les sous-réseaux spécifiés.

7. Enregistrez et fermez le `kaminoprefs.xml` fichier.

Accédez aux options de la console de maintenance de l'appliance virtuelle pour VSC, VASA Provider et SRA

Vous pouvez gérer vos configurations applicatives, système et réseau à l'aide de la console de maintenance de l'appliance virtuelle pour Virtual Storage Console (VSC), VASA Provider et Storage Replication adapter (SRA). Vous pouvez modifier votre mot de passe administrateur et votre mot de passe de maintenance. Vous pouvez également générer des offres de support, définir différents niveaux de journal, afficher et gérer les configurations TLS et démarrer les diagnostics à distance.


Avant de commencer

Vous devez avoir installé les outils VMware après le déploiement de l'appliance virtuelle pour VSC, VASA Provider et SRA.

Description de la tâche

- Vous devez utiliser « saint » en tant que nom d'utilisateur et mot de passe configurés lors du déploiement pour vous connecter à la console de maintenance de l'appliance virtuelle pour VSC, VASA Provider et SRA.
- Vous devez définir un mot de passe pour l'utilisateur "diag" tout en activant les diagnostics à distance.

Étapes

1. Accédez à l'onglet **Résumé** de votre appliance virtuelle déployée.
2. Cliquez sur  pour démarrer la console de maintenance.

Les options de la console de maintenance suivantes sont disponibles :

◦ Configuration de l'application

Les options suivantes sont disponibles :

- Afficher le récapitulatif de l'état du serveur
- Démarrage du service Virtual Storage Console
- Arrêtez le service Virtual Storage Console
- Démarrer le service VASA Provider et SRA
- Arrêt du service VASA Provider et SRA
- Modifier le mot de passe utilisateur « administrateur »
- Re-générez des certificats
- Réinitialisation matérielle du magasin de clés et des certificats

- Réinitialisation matérielle de la base de données
- Modifiez le niveau DE JOURNALISATION du service Virtual Storage Console
- Modifier le niveau DE JOURNALISATION pour les services VASA Provider et SRA
- Afficher la configuration TLS
- Activez le protocole TLS
- Désactivez le protocole TLS

◦ **Configuration du système**

Les options suivantes sont disponibles :

- Redémarrez la machine virtuelle
- Arrêter la machine virtuelle
- Modifier le mot de passe utilisateur « familiariser »
- Modifier le fuseau horaire
- Modifier le serveur NTP

Vous pouvez fournir une adresse IPv6 pour votre serveur NTP.

- Activer/Désactiver l'accès SSH
- Augmentation de la taille des disques de prison (/prison)
- Mise à niveau
- Installez VMware Tools

◦ **Configuration réseau**

Les options suivantes sont disponibles :

- Afficher les paramètres d'adresse IP
- Modifier les paramètres d'adresse IP

Vous pouvez utiliser cette option pour modifier l'adresse IP post-déploiement sur IPv6.

- Afficher les paramètres de recherche du nom de domaine
- Modifier les paramètres de recherche du nom de domaine
- Afficher les routes statiques
- Modifier les routes statiques

Vous pouvez utiliser cette option pour ajouter une route IPv6.

- Valider les modifications
- Envoyez une requête ping à un hôte

Vous pouvez utiliser cette option pour envoyer une requête ping vers un hôte IPv6.

- Restaurez les paramètres par défaut

◦ **Support et diagnostics**

Les options suivantes sont disponibles :

- Générez un bundle de support
- Accéder au shell de diagnostic
- Activer l'accès aux diagnostics à distance

Informations connexes

[Fichiers journaux de VSC et VASA Provider](#)

Modifiez le mot de passe administrateur

Vous pouvez modifier le mot de passe d'administrateur de l'appliance virtuelle pour le déploiement de VSC, VASA Provider et SRA à l'aide de la console de maintenance.

Étapes

1. Depuis vCenter Server, ouvrez une console vers l'appliance virtuelle pour VSC, VASA Provider et SRA.
2. Connectez-vous en tant qu'utilisateur de maintenance.
3. Entrez 1 Dans la console de maintenance pour sélectionner **Configuration de l'application** .
4. Entrez 6 Pour sélectionner **Modifier le mot de passe utilisateur 'administrateur'**.
5. Saisissez un mot de passe de huit caractères minimum et de 63 caractères maximum.
6. Entrez y dans la boîte de dialogue de confirmation.

Configurez la haute disponibilité de l'appliance virtuelle pour VSC, VASA Provider et SRA

L'appliance virtuelle pour Virtual Storage Console (VSC), VASA Provider et Storage Replication adapter (SRA) prend en charge une configuration (HA) afin d'assurer la continuité de l'activité de VSC, VASA Provider et SRA en cas de défaillance.

L'appliance virtuelle pour VSC, VASA Provider et SRA repose sur la fonctionnalité VMware vSphere (HA) et la fonctionnalité vSphere Fault Tolerance (FT) pour offrir . (HA) assure une reprise rapide en cas de pannes causées par :

- Défaillance d'hôte
- Défaillance du réseau
- Défaillance de machine virtuelle (défaillance du système d'exploitation invité)
- Panne des applications (VSC, VASA Provider et SRA)

Aucune configuration supplémentaire n'est requise sur l'appliance virtuelle pour fournir . Seuls les hôtes vCenter Server et ESXi doivent être configurés à l'aide de la fonction HA de VMware vSphere ou de la fonction FT de vSphere en fonction de leurs besoins. La haute disponibilité et la tolérance de défaillance nécessitent des hôtes en cluster associés au stockage partagé. FT a des exigences et des limites supplémentaires.

Outre la solution HA VMware vSphere et la solution vSphere FT, l'appliance virtuelle permet également de garantir le fonctionnement continu des services VSC, VASA Provider et SRA. Le processus de surveillance de l'appliance virtuelle surveille régulièrement les trois services et les redémarre automatiquement en cas de

défaillance. Ainsi, il est possible d'éviter les défaillances des applications.



VCenter HA n'est pas pris en charge par l'appliance virtuelle pour VSC, VASA Provider et SRA.

Haute disponibilité VMware vSphere

Vous pouvez configurer votre environnement vSphere sur lequel l'appliance virtuelle pour Virtual Storage Console (VSC), VASA Provider et Storage Replication adapter (SRA) est déployée pour (HA). La fonction de haute disponibilité de VMware offre une protection contre les défaillances matérielles et les défaillances du système d'exploitation dans les environnements virtuels.

La fonction VMware HA surveille les machines virtuelles afin de détecter les défaillances du système d'exploitation et du matériel. Lorsqu'une défaillance est détectée, la fonction VMware HA redémarre les machines virtuelles sur les autres serveurs physiques du pool de ressources. Une intervention manuelle n'est pas requise lorsqu'une défaillance de serveur est détectée.

La procédure de configuration de VMware HA dépend de la version de votre serveur vCenter. Par exemple, vous pouvez utiliser le lien de référence suivant et sélectionner la version de vCenter Server requise pour afficher les étapes de configuration de VMware HA.

["Documentation VMware vSphere : création et utilisation de clusters vSphere HA"](#)

Tolérance aux pannes VMware vSphere

La fonction VMware vSphere Fault Tolerance (FT) fournit (HA) à un niveau supérieur et permet de protéger les machines virtuelles sans perte de données ni de connexions. Vous devez activer ou désactiver vSphere FT pour l'appliance virtuelle pour VSC, VASA Provider et SRA depuis votre vCenter Server.

Assurez-vous que votre licence vSphere prend en charge FT avec le nombre de CPU virtuels requis pour l'appliance virtuelle de votre environnement (au moins 2 CPU virtuels ; 4 CPU virtuels pour les environnements à grande échelle).

vSphere FT permet aux machines virtuelles de fonctionner en continu, même en cas de panne de serveur. Lorsque vSphere FT est activé sur une machine virtuelle, une copie de la machine virtuelle principale est automatiquement créée sur un autre hôte (la machine virtuelle secondaire) sélectionné par Distributed Resource Scheduler (DRS). Si DRS n'est pas activé, l'hôte cible est sélectionné à partir des hôtes disponibles. vSphere FT exploite la machine virtuelle principale et la machine virtuelle secondaire en mode parallèle, chaque mise en miroir de l'état d'exécution de la machine virtuelle principale vers la machine virtuelle secondaire.

En cas de défaillance matérielle causant la défaillance de la machine virtuelle principale, la machine virtuelle secondaire reprend immédiatement l'endroit où la machine virtuelle principale est arrêtée. La machine virtuelle secondaire continue de fonctionner sans perte de connexions réseau, de transactions ou de données.

Votre système doit répondre aux exigences du processeur, aux exigences de limite des machines virtuelles et aux exigences de licence pour la configuration de vSphere FT pour votre instance vCenter Server.

La procédure de configuration de HA dépend de la version de votre serveur vCenter. Par exemple, vous pouvez utiliser le lien de référence suivant et sélectionner la version de vCenter Server requise pour afficher les étapes de configuration de HA.

Configurations MetroCluster prises en charge par l'appliance virtuelle pour VSC, VASA Provider et SRA

L'appliance virtuelle pour Virtual Storage Console (VSC), VASA Provider et Storage Replication adapter (SRA) prend en charge les environnements qui utilisent les configurations IP et FC de MetroCluster pour ONTAP. La majeure partie de ce support est automatique. Toutefois, vous remarquerez peut-être quelques différences si vous utilisez un environnement MetroCluster avec VSC et VASA Provider.

Les configurations MetroCluster et VSC

Vous devez vous assurer que VSC détecte les contrôleurs du système de stockage sur le site principal et sur le site secondaire. En général, VSC détecte automatiquement les contrôleurs de stockage. Si vous utilisez une LIF de gestion de cluster, il est recommandé de vérifier que VSC a détecté les clusters sur les deux sites. Vous pouvez également ajouter manuellement les contrôleurs de stockage à VSC. Vous pouvez également modifier les paires de noms d'utilisateur et de mots de passe que VSC utilise pour se connecter aux contrôleurs de stockage.

Lorsqu'un basculement se produit, le basculement sur le site secondaire prend le relais. Ceux-ci ont le suffixe «-mc» annexé à leurs noms. Si une opération de basculement se produit pendant que vous effectuez des opérations telles que le provisionnement d'un datastore, le nom de l'emplacement du datastore est modifié pour inclure le suffixe «-mc ». Ce suffixe n'est supprimé que lorsque le rétablissement a lieu et que le contrôle de reprise sur le site principal est activé.



Si vous avez ajouté directement avec la configuration MetroCluster à VSC, puis après le basculement, la modification du nom de SVM (l'ajout du suffixe «-mc ») n'est pas reflétée. Toutes les autres opérations de basculement continuent à s'exécuter normalement.

En cas de basculement ou de rétablissement, VSC peut prendre quelques minutes pour détecter et détecter automatiquement les clusters. Si cela se produit pendant l'exécution d'une opération VSC comme le provisionnement d'un datastore, vous risquez de rencontrer un retard.

Configurations MetroCluster et VASA Provider

Vasa Provider prend automatiquement en charge les environnements qui utilisent les configurations MetroCluster. Le basculement est transparent dans les environnements VASA Provider. Vous ne pouvez pas ajouter directement à VASA Provider.



Vasa Provider n'ajoute pas le suffixe "-mc" aux noms du sur le site secondaire après un basculement.

Configurations MetroCluster et SRA

SRA ne prend pas en charge les configurations MetroCluster.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.