



Protéger les systèmes de fichiers Unix

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-61/protect-scu/concept_overview_snapcenter_plug_in_for_UNIX_file_systems.html on November 06, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protéger les systèmes de fichiers Unix	1
Ce que vous pouvez faire avec le plug-in SnapCenter pour les systèmes de fichiers Unix	1
Configurations prises en charge	1
Limites	2
Caractéristiques	2
Installer le plug-in SnapCenter pour les systèmes de fichiers Unix	2
Conditions préalables à l'ajout d'hôtes et à l'installation du package Plug-ins pour Linux	3
Ajoutez des hôtes et installez le package de plug-ins pour Linux à l'aide de l'interface graphique	4
Configurer le service SnapCenter Plug-in Loader	7
Configurer un certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux	10
Activer les certificats CA pour les plug-ins	13
Installer le SnapCenter Plug-in for VMware vSphere	14
Déployer un certificat CA	14
Configurer le fichier CRL	14
Préparez-vous à protéger les systèmes de fichiers Unix	14
Sauvegarder les systèmes de fichiers Unix	15
Découvrez les systèmes de fichiers UNIX disponibles pour la sauvegarde	15
Créer des politiques de sauvegarde pour les systèmes de fichiers Unix	15
Créer des groupes de ressources et attacher des politiques pour les systèmes de fichiers Unix	18
Créer des groupes de ressources et activer la protection secondaire pour les systèmes de fichiers Unix sur les systèmes ASA r2	20
Sauvegarder les systèmes de fichiers Unix	23
Sauvegarder les groupes de ressources des systèmes de fichiers Unix	25
Surveiller la sauvegarde des systèmes de fichiers Unix	25
Afficher les systèmes de fichiers Unix protégés dans la page Topologie	26
Restaurer et récupérer les systèmes de fichiers Unix	29
Restaurer les systèmes de fichiers Unix	29
Surveiller les opérations de restauration des systèmes de fichiers Unix	31
Cloner les systèmes de fichiers Unix	31
Cloner la sauvegarde du système de fichiers Unix	31
Diviser un clone	33
Surveiller les opérations de clonage des systèmes de fichiers Unix	34

Protéger les systèmes de fichiers Unix

Ce que vous pouvez faire avec le plug-in SnapCenter pour les systèmes de fichiers Unix

Lorsque le plug-in pour les systèmes de fichiers Unix est installé dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner des systèmes de fichiers Unix. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Découvrir les ressources
- Sauvegarder les systèmes de fichiers Unix
- Planifier des opérations de sauvegarde
- Restaurer les sauvegardes du système de fichiers
- Cloner les sauvegardes du système de fichiers
- Surveiller les opérations de sauvegarde, de restauration et de clonage

Configurations prises en charge

Article	Configuration prise en charge
Environnements	• Serveur physique • Serveur virtuel Banques de données vVol sur NFS et SAN. La banque de données vVol ne peut être provisionnée qu'avec ONTAP Tools pour VMware vSphere.
Systèmes d'exploitation	• Red Hat Enterprise Linux • Oracle Linux • Serveur d'entreprise SUSE Linux (SLES)
Systèmes de fichiers	• SAN: ◦ Systèmes de fichiers basés et non basés sur LVM ◦ LVM sur VMDK ext3, ext4 et xfs • NFS : NFS v3, NFS v4.x

Article	Configuration prise en charge
Protocoles	• FC • FCoE • iSCSI • NFS
Trajets multiples	Oui

Limites

- La combinaison de RDM et de disques virtuels dans un groupe de volumes n'est pas prise en charge.
- La restauration au niveau des fichiers n'est pas prise en charge.

Cependant, vous pouvez effectuer manuellement une restauration au niveau des fichiers en clonant la sauvegarde, puis en copiant les fichiers manuellement.

- Le mélange de systèmes de fichiers répartis sur des VMDK provenant à la fois de banques de données NFS et VMFS n'est pas pris en charge.
- NVMe n'est pas pris en charge.
- Le provisionnement n'est pas pris en charge.

Caractéristiques

- Permet au plug-in pour Oracle Database d'effectuer des opérations de protection des données sur les bases de données Oracle en gérant la pile de stockage hôte sous-jacente sur les systèmes Linux ou AIX
- Prend en charge les protocoles Network File System (NFS) et Storage Area Network (SAN) sur un système de stockage exécutant ONTAP.
- Pour les systèmes Linux, les bases de données Oracle sur les LUN VMDK et RDM sont prises en charge lorsque vous déployez le SnapCenter Plug-in for VMware vSphere et enregistrez le plug-in auprès de SnapCenter.
- Prend en charge Mount Guard pour AIX sur les systèmes de fichiers SAN et la disposition LVM.
- Prend en charge le système de fichiers journalisé amélioré (JFS2) avec journalisation en ligne sur les systèmes de fichiers SAN et la disposition LVM pour les systèmes AIX uniquement.

Les périphériques SAN natifs, les systèmes de fichiers et les dispositions LVM créés sur des périphériques SAN sont pris en charge.

- Automatise les opérations de sauvegarde, de restauration et de clonage prenant en charge les applications pour les systèmes de fichiers UNIX dans votre environnement SnapCenter

Installer le plug-in SnapCenter pour les systèmes de fichiers Unix

Conditions préalables à l'ajout d'hôtes et à l'installation du package Plug-ins pour Linux

Avant d'ajouter un hôte et d'installer le package de plug-ins pour Linux, vous devez remplir toutes les conditions requises.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous pouvez utiliser l'authentification par mot de passe pour l'utilisateur root ou non root ou l'authentification par clé SSH.

Le plug-in SnapCenter pour les systèmes de fichiers Unix peut être installé par un utilisateur non root. Cependant, vous devez configurer les privilèges sudo pour que l'utilisateur non root puisse installer et démarrer le processus du plug-in. Après l'installation du plug-in, les processus s'exécuteront en tant qu'utilisateur non root effectif.

- Créez des informations d'identification avec le mode d'authentification Linux pour l'utilisateur d'installation.
- Vous devez avoir installé Java 11 sur votre hôte Linux.



Assurez-vous d'avoir installé uniquement l'édition certifiée de JAVA 11 sur l'hôte Linux.

Pour plus d'informations sur le téléchargement de JAVA, voir : ["Téléchargements Java pour tous les systèmes d'exploitation"](#)

- Vous devriez avoir **bash** comme shell par défaut pour l'installation du plug-in.

Configuration requise pour l'hôte Linux

Vous devez vous assurer que l'hôte répond aux exigences avant d'installer le package de plug-ins SnapCenter pour Linux.

Article	Exigences
Systèmes d'exploitation	• Red Hat Enterprise Linux • Oracle Linux • Serveur d'entreprise SUSE Linux (SLES)
RAM minimale pour le plug-in SnapCenter sur l'hôte	2 Go

Article	Exigences
Espace minimum d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 Go  Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace journal requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récemment exécutées.
Logiciels requis	Java 11 Oracle Java et OpenJDK  Assurez-vous d'avoir installé uniquement l'édition certifiée de JAVA 11 sur l'hôte Linux. Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option <code>JAVA_HOME</code> située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.

Pour obtenir les dernières informations sur les versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp"](#) .

Ajoutez des hôtes et installez le package de plug-ins pour Linux à l'aide de l'interface graphique

Vous pouvez utiliser la page Ajouter un hôte pour ajouter des hôtes, puis installer le package de plug-ins SnapCenter pour Linux. Les plug-ins sont automatiquement installés sur les hôtes distants.

Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Vérifiez que l'onglet **Hôtes gérés** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page Hôtes, effectuez les actions suivantes :

Pour ce domaine...	Fais ceci...
Type d'hôte	Sélectionnez Linux comme type d'hôte.

Pour ce domaine...	Fais ceci...
Nom d'hôte	Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN. Si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le nom de domaine complet.
Informations d'identification	Sélectionnez le nom des informations d'identification que vous avez créées ou créez de nouvelles informations d'identification. L'identifiant doit disposer de droits administratifs sur l'hôte distant. Pour plus de détails, consultez les informations sur la création d'informations d'identification. Vous pouvez afficher les détails des informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez spécifié.  Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajouter un hôte.

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez **Systèmes de fichiers Unix**.

6. (Facultatif) Cliquez sur **Plus d'options**.

Pour ce domaine...	Fais ceci...
Port	Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port sera affiché comme port par défaut.  Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Sinon, l'opération échoue.

Pour ce domaine...	Fais ceci...
Chemin d'installation	Le chemin par défaut est <code>/opt/NetApp/snapcenter</code> . Vous pouvez éventuellement personnaliser le chemin. Si vous utilisez le chemin personnalisé, assurez-vous que le contenu par défaut des sudoers est mis à jour avec le chemin personnalisé.
Ignorer les vérifications de préinstallation facultatives	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas valider si l'hôte répond aux exigences d'installation du plug-in.

7. Cliquez sur **Soumettre**.

Si vous n'avez pas coché la case Ignorer les pré-vérifications, l'hôte est validé pour vérifier s'il répond aux exigences d'installation du plug-in.



Le script de pré-vérification ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

Des messages d'erreur ou d'avertissement appropriés s'affichent si les exigences minimales ne sont pas respectées. Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier `web.config` situé dans `C:\Program Files\NetApp\ SnapCenter WebApp` pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez résoudre le problème.



Dans une configuration HA, si vous mettez à jour le fichier `web.config`, vous devez mettre à jour le fichier sur les deux nœuds.

8. Vérifiez l'empreinte digitale, puis cliquez sur **Confirmer et soumettre**.



SnapCenter ne prend pas en charge l'algorithme ECDSA.



La vérification des empreintes digitales est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte digitale a été confirmée.

9. Surveiller la progression de l'installation.

Les fichiers journaux spécifiques à l'installation se trouvent dans `/custom_location/snapcenter/logs`.

Résultat

Tous les systèmes de fichiers montés sur l'hôte sont automatiquement découverts et affichés sous la page Ressources. Si rien ne s'affiche, cliquez sur **Actualiser les ressources**.

Surveiller l'état de l'installation

Vous pouvez surveiller la progression de l'installation du package de plug-in SnapCenter à l'aide de la page Tâches. Vous souhaitez peut-être vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page Tâches et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Tâches**, pour filtrer la liste afin que seules les opérations d'installation de plug-ins soient répertoriées, procédez comme suit :
 - a. Cliquez sur **Filtre**.
 - b. Facultatif : précisez la date de début et de fin.
 - c. Dans le menu déroulant Type, sélectionnez **Installation du plug-in**.
 - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
 - e. Cliquez sur **Appliquer**.
4. Sélectionnez la tâche d'installation et cliquez sur **Détails** pour afficher les détails de la tâche.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Configurer le service SnapCenter Plug-in Loader

Le service SnapCenter Plug-in Loader charge le package de plug-in pour que Linux interagisse avec le serveur SnapCenter . Le service SnapCenter Plug-in Loader est installé lorsque vous installez le package SnapCenter Plug-ins pour Linux.

À propos de cette tâche

Après l'installation du package de plug-ins SnapCenter pour Linux, le service SnapCenter Plug-in Loader démarre automatiquement. Si le service SnapCenter Plug-in Loader ne démarre pas automatiquement, vous devez :

- Assurez-vous que le répertoire dans lequel le plug-in fonctionne n'est pas supprimé
- Augmenter l'espace mémoire alloué à la machine virtuelle Java

Le fichier `spl.properties`, situé dans `/custom_location/ NetApp/snapcenter/spl/etc/`, contient les paramètres suivants. Des valeurs par défaut sont attribuées à ces paramètres.

Nom du paramètre	Description
LOG_LEVEL	Affiche les niveaux de journalisation pris en charge. Les valeurs possibles sont TRACE, DEBUG, INFO, WARN, ERROR et FATAL.
PROTOCOLE_SPL	Affiche le protocole pris en charge par SnapCenter Plug-in Loader. Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.
PROTOCOLE_SERVEUR_SNAPCENTER	Affiche le protocole pris en charge par SnapCenter Server. Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.
SKIP_JAVAHOME_UPDATE	Par défaut, le service SPL détecte le chemin Java et met à jour le paramètre JAVA_HOME. Par conséquent, la valeur par défaut est définie sur FAUX. Vous pouvez définir sur TRUE si vous souhaitez désactiver le comportement par défaut et corriger manuellement le chemin Java.
SPL_KEYSTORE_PASS	Affiche le mot de passe du fichier keystore. Vous ne pouvez modifier cette valeur que si vous modifiez le mot de passe ou créez un nouveau fichier de clés.
SPL_PORT	Affiche le numéro de port sur lequel le service SnapCenter Plug-in Loader est en cours d'exécution. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.  Vous ne devez pas modifier la valeur après l'installation des plug-ins.
SNAPCENTER_SERVER_HOST	Affiche l'adresse IP ou le nom d'hôte du serveur SnapCenter .
SPL_KEYSTORE_PATH	Affiche le chemin absolu du fichier keystore.

Nom du paramètre	Description
PORT_SERVEUR_SNAPCENTER	Affiche le numéro de port sur lequel le serveur SnapCenter est en cours d'exécution.
NOMBRE_MAX_LOGS	Affiche le nombre de fichiers journaux du Loader de plug-in SnapCenter conservés dans le dossier <i>/custom_location/snapcenter/spl/logs</i>. La valeur par défaut est définie sur 5000. Si le nombre est supérieur à la valeur spécifiée, les 5 000 derniers fichiers modifiés sont conservés. La vérification du nombre de fichiers est effectuée automatiquement toutes les 24 heures à partir du démarrage du service SnapCenter Plug-in Loader .  Si vous supprimez manuellement le fichier <i>spl.properties</i>, le nombre de fichiers à conserver est défini sur 9999.
JAVA_HOME	Affiche le chemin d'accès absolu du répertoire <i>JAVA_HOME</i> qui est utilisé pour démarrer le service SPL. Ce chemin est déterminé lors de l'installation et dans le cadre du démarrage de SPL.
LOG_MAX_SIZE	Affiche la taille maximale du fichier journal des tâches. Une fois la taille maximale atteinte, le fichier journal est compressé et les journaux sont écrits dans le nouveau fichier de ce travail.
CONSERVER_LES_JOURNAUX_DES_DERNIERS_JOURS	Affiche le nombre de jours pendant lesquels les journaux sont conservés.
ACTIVER_LA_VALIDATION_DU_CERTIFICAT	Affiche vrai lorsque la validation du certificat CA est activée pour l'hôte. Vous pouvez activer ou désactiver ce paramètre en modifiant le fichier <i>spl.properties</i> ou en utilisant l'interface graphique ou l'applet de commande SnapCenter .

Si l'un de ces paramètres n'est pas affecté à la valeur par défaut ou si vous souhaitez affecter ou modifier la valeur, vous pouvez modifier le fichier *spl.properties*. Vous pouvez également vérifier le fichier *spl.properties* et le modifier pour résoudre tout problème lié aux valeurs attribuées aux paramètres. Après avoir modifié le fichier *spl.properties*, vous devez redémarrer le service SnapCenter Plug-in Loader .

Mesures

1. Effectuez l'une des actions suivantes, selon vos besoins :

- Démarrez le service SnapCenter Plug-in Loader :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl start`
- Arrêtez le service SnapCenter Plug-in Loader :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`



Vous pouvez utiliser l'option `-force` avec la commande `stop` pour arrêter de force le service SnapCenter Plug-in Loader . Cependant, vous devez faire preuve de prudence avant de procéder ainsi, car cela met également fin aux opérations existantes.

- Redémarrez le service SnapCenter Plug-in Loader :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Rechercher l'état du service SnapCenter Plug-in Loader :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Recherchez la modification dans le service SnapCenter Plug-in Loader :
 - En tant qu'utilisateur root, exécutez :
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - En tant qu'utilisateur non root, exécutez : `sudo`
`/custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurer un certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux

Vous devez gérer le mot de passe du magasin de clés SPL et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance SPL et configurer la paire de clés signée CA dans le magasin de confiance SPL avec le service SnapCenter Plug-in Loader pour activer le certificat numérique installé.



SPL utilise le fichier « `keystore.jks` », qui se trouve dans « `/var/opt/snapcenter/spl/etc` », à la fois comme magasin de confiance et comme magasin de clés.

Gérer le mot de passe du magasin de clés SPL et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

Mesures

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL à partir du fichier de propriétés SPL.

Il s'agit de la valeur correspondant à la clé 'SPL_KEYSTORE_PASS'.

2. Modifier le mot de passe du keystore :

```
keytool -storepasswd -keystore keystore.jks  
. Modifiez le mot de passe de tous les alias des entrées de clés privées  
dans le magasin de clés avec le même mot de passe que celui utilisé pour  
le magasin de clés :
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Mettez à jour la même chose pour la clé SPL_KEYSTORE_PASS dans le fichier spl.properties.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du keystore SPL et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

Configurer les certificats racine ou intermédiaires dans le magasin de confiance SPL

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée dans le magasin de confiance SPL.

Mesures

1. Accédez au dossier contenant le keystore SPL : `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier « keystore.jks ».
3. Répertoriez les certificats ajoutés dans le keystore :

```
keytool -list -v -keystore keystore.jks  
. Ajouter un certificat racine ou intermédiaire :
```

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks  
. Redémarrez le service après avoir configuré les certificats racine ou  
intermédiaires dans le magasin de confiance SPL.
```



Vous devez ajouter le certificat CA racine, puis les certificats CA intermédiaires.

Configurer la paire de clés signée par l'autorité de certification pour le magasin de confiance SPL

Vous devez configurer la paire de clés signée par l'autorité de certification sur le magasin de confiance SPL.

Mesures

1. Accédez au dossier contenant le keystore du SPL `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier « `keystore.jks` ».
3. Répertoriez les certificats ajoutés dans le keystore :

```
keytool -list -v -keystore keystore.jks
```

. Ajoutez le certificat CA contenant à la fois une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

. Répertoriez les certificats ajoutés dans le keystore.

```
keytool -list -v -keystore keystore.jks
```

. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat CA, qui a été ajouté au magasin de clés.

. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe par défaut du magasin de clés SPL est la valeur de la clé `SPL_KEYSTORE_PASS` dans le fichier `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks
```

. Si le nom d'alias dans le certificat CA est long et contient des espaces ou des caractères spéciaux (« `*` », « `»`, « `»`), remplacez le nom d'alias par un nom simple :

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks
```

. Configurez le nom d'alias à partir du keystore situé dans le fichier `spl.properties`.

Mettez à jour cette valeur par rapport à la clé `SPL_CERTIFICATE_ALIAS`.

4. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification sur le magasin de confiance SPL.

Configurer la liste de révocation de certificats (CRL) pour SPL

Vous devez configurer la CRL pour SPL

À propos de cette tâche

- SPL recherchera les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour SPL est `/var/opt/snapcenter/spl/etc/crl`.

Mesures

1. Vous pouvez modifier et mettre à jour le répertoire par défaut dans le fichier `spl.properties` par rapport à la clé `SPL_CRL_PATH`.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés par rapport à chaque CRL.

Activer les certificats CA pour les plug-ins

Vous devez configurer les certificats CA et déployer les certificats CA sur le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat CA pour les plug-ins.

Avant de commencer

- Vous pouvez activer ou désactiver les certificats d'autorité de certification à l'aide de l'applet de commande `run Set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat des plug-ins à l'aide de `Get-SmCertificateSettings`.

Les informations concernant les paramètres pouvant être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Alternativement, vous pouvez également vous référer à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Hôtes**.
2. Dans la page Hôtes, cliquez sur **Hôtes gérés**.
3. Sélectionnez un ou plusieurs hôtes de plug-in.
4. Cliquez sur **Plus d'options**.
5. Sélectionnez **Activer la validation du certificat**.

Après avoir terminé

L'onglet Hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre SnapCenter Server et l'hôte du plug-in.

- *  * indique que le certificat CA n'est ni activé ni attribué à l'hôte du plug-in.
- *  * indique que le certificat CA est validé avec succès.

- *  * indique que le certificat CA n'a pas pu être validé.
- *  * indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque le statut est jaune ou vert, les opérations de protection des données se terminent avec succès.

Installer le SnapCenter Plug-in for VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM), ou si vous souhaitez protéger les machines virtuelles et les banques de données, vous devez déployer le SnapCenter Plug-in for VMware vSphere .

Pour plus d'informations sur le déploiement, voir "[Présentation du déploiement](#)" .

Déployer un certificat CA

Pour configurer le certificat CA avec le SnapCenter Plug-in for VMware vSphere, consultez "[Créer ou importer un certificat SSL](#)" .

Configurer le fichier CRL

Le SnapCenter Plug-in for VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour SnapCenter Plug-in for VMware vSphere est `/opt/netapp/config/crl`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés par rapport à chaque CRL.

Préparez-vous à protéger les systèmes de fichiers Unix

Avant d'effectuer toute opération de protection des données telle que des opérations de sauvegarde, de clonage ou de restauration, vous devez configurer votre environnement. Vous pouvez également configurer le serveur SnapCenter pour utiliser les technologies SnapMirror et SnapVault .

Pour profiter de la technologie SnapVault et SnapMirror , vous devez configurer et initialiser une relation de protection des données entre les volumes source et de destination sur le périphérique de stockage. Vous pouvez utiliser NetAppSystem Manager ou la ligne de commande de la console de stockage pour effectuer ces tâches.

Avant d'utiliser le plug-in pour les systèmes de fichiers Unix, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server. "[Apprendre encore plus](#)"
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage. "[Apprendre encore plus](#)"



SnapCenter ne prend pas en charge plusieurs SVM portant le même nom sur différents clusters. Chaque SVM enregistré auprès de SnapCenter à l'aide de l'enregistrement SVM ou de l'enregistrement de cluster doit être unique.

- Ajoutez des hôtes, installez les plug-ins et découvrez les ressources.
- Si vous utilisez SnapCenter Server pour protéger les systèmes de fichiers Unix qui résident sur des LUN VMware RDM ou des VMDK, vous devez déployer le SnapCenter Plug-in for VMware vSphere et enregistrer le plug-in auprès de SnapCenter.
- Installez Java sur votre hôte Linux.
- Configurez SnapMirror et SnapVault sur ONTAP, si vous souhaitez une réplication de sauvegarde.

Sauvegarder les systèmes de fichiers Unix

Découvrez les systèmes de fichiers UNIX disponibles pour la sauvegarde

Après l'installation du plug-in, tous les systèmes de fichiers sur cet hôte sont automatiquement découverts et affichés dans la page Ressources. Vous pouvez ajouter ces systèmes de fichiers à des groupes de ressources pour effectuer des opérations de protection des données.

Avant de commencer

- Vous devez avoir effectué des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la création de connexions au système de stockage.
- Si les systèmes de fichiers résident sur un disque de machine virtuelle (VMDK) ou un mappage de périphériques bruts (RDM), vous devez déployer le SnapCenter Plug-in for VMware vSphere et enregistrer le plug-in auprès de SnapCenter.

Pour plus d'informations, consultez la section ["Déployer le SnapCenter Plug-in for VMware vSphere"](#).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Chemin** dans la liste Affichage.
3. Cliquez sur **Actualiser les ressources**.

Les systèmes de fichiers sont affichés avec des informations telles que le type, le nom d'hôte, les groupes de ressources et les politiques associés, ainsi que l'état.

Créer des politiques de sauvegarde pour les systèmes de fichiers Unix

Avant d'utiliser SnapCenter pour sauvegarder des systèmes de fichiers Unix, vous devez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources que vous souhaitez sauvegarder. Une politique de sauvegarde est un ensemble de règles qui régissent la manière dont vous gérez, planifiez et conservez les sauvegardes. Vous pouvez également spécifier les paramètres de réplication, de script et de type de sauvegarde. La création d'une politique permet de gagner du temps lorsque vous souhaitez réutiliser la politique sur une autre ressource ou un autre groupe de ressources.

Avant de commencer

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la découverte des systèmes de fichiers et la création de connexions au système de stockage.
- Si vous répliquez des snapshots vers un stockage secondaire miroir ou coffre, l'administrateur SnapCenter doit vous avoir attribué les SVM pour les volumes source et de destination.
- Consultez les conditions préalables et les limitations spécifiques à la synchronisation active de SnapMirror . Pour plus d'informations, reportez-vous à "[Limites d'objets pour la synchronisation active de SnapMirror](#)".

À propos de cette tâche

- SnapLock
 - Si l'option « Conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation de SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.

La spécification d'une période de verrouillage des instantanés empêche la suppression des instantanés jusqu'à l'expiration de la période de conservation. Cela pourrait conduire à conserver un nombre d'instantanés supérieur au nombre spécifié dans la politique.

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des instantanés SnapLock Vault dans le cadre de la restauration hériteront du délai d'expiration de SnapLock Vault. L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Politiques**.
3. Sélectionnez **Systèmes de fichiers Unix** dans la liste déroulante.
4. Cliquez sur **Nouveau**.
5. Dans la page Nom, saisissez le nom et les détails de la politique.
6. Dans la page Sauvegarde et réplication, effectuez les actions suivantes :
 - a. Spécifiez les paramètres de sauvegarde.
 - b. Spécifiez la fréquence de planification en sélectionnant **À la demande**, **Toutes les heures**, **Quotidien**, **Hebdomadaire** ou **Mensuel**.
 - c. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une ou les deux options de réplication secondaire suivantes :

Pour ce domaine...	Fais ceci...
Mettre à jour SnapMirror après avoir créé une copie Snapshot locale	Sélectionnez ce champ pour créer des copies miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror). Cette option doit être activée pour la synchronisation active de SnapMirror .
Mettre à jour SnapVault après avoir créé une copie Snapshot locale	Sélectionnez cette option pour effectuer une réplication de sauvegarde de disque à disque (sauvegardes SnapVault).

Pour ce domaine...	Fais ceci...
Nombre de tentatives d'erreur	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.

7. Dans la page Rétention, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionné dans la page Sauvegarde et réplication :

Si vous voulez...	Alors...
Conserver un certain nombre de clichés	Sélectionnez Copies à conserver, puis spécifiez le nombre d'instantanés que vous souhaitez conserver. Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés, les copies les plus anciennes étant supprimées en premier.  La valeur de rétention maximale est de 1018. Les sauvegardes échoueront si la rétention est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.  Vous devez définir le nombre de rétention sur 2 ou plus si vous prévoyez d'activer la réplication SnapVault . Si vous définissez le nombre de rétention sur 1, l'opération de rétention peut échouer car le premier instantané est l'instantané de référence pour la relation SnapVault jusqu'à ce qu'un instantané plus récent soit répliqué sur la cible.
Conservez les instantanés pendant un certain nombre de jours	Sélectionnez Conserver les copies pendant , puis spécifiez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage de la copie instantanée	Sélectionnez Période de verrouillage de la copie instantanée et spécifiez la durée en jours, mois ou années. La période de rétention du Snaplock doit être inférieure à 100 ans.

8. Sélectionnez l'étiquette de la politique.



Vous pouvez attribuer des étiquettes SnapMirror aux snapshots principaux pour la réplication à distance, permettant ainsi aux snapshots principaux de décharger l'opération de réplication de snapshot de SnapCenter vers les systèmes secondaires ONTAP . Cela peut être fait sans activer l'option SnapMirror ou SnapVault dans la page de politique.

9. Dans la page Script, entrez le chemin et les arguments du prescript ou du postscript que vous souhaitez exécuter respectivement avant ou après l'opération de sauvegarde.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir du chemin `_ /opt/NetApp/snapcenter/scc/etc/allowed_commands.config_`.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est de 60 secondes.

10. Consultez le résumé, puis cliquez sur **Terminer**.

Créer des groupes de ressources et attacher des politiques pour les systèmes de fichiers Unix

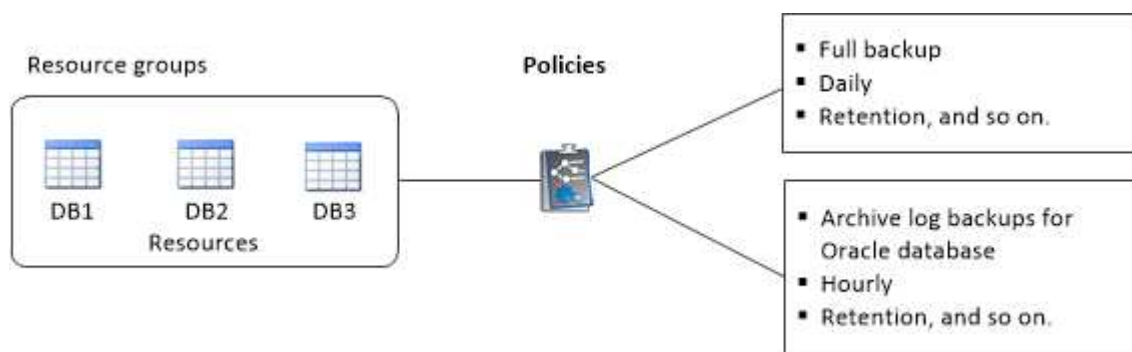
Un groupe de ressources est un conteneur dans lequel vous ajoutez les ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder toutes les données associées aux systèmes de fichiers.

À propos de cette tâche

- Une base de données avec des fichiers dans des groupes de disques ASM doit être à l'état « MOUNT » ou « OPEN » pour vérifier ses sauvegardes à l'aide de l'utilitaire Oracle DBVERIFY.

Attachez une ou plusieurs politiques au groupe de ressources pour définir le type de tâche de protection des données que vous souhaitez effectuer.

L'image suivante illustre la relation entre les ressources, les groupes de ressources et les stratégies pour les bases de données :



- Pour les stratégies activées par SnapLock , pour ONTAP 9.12.1 et les versions antérieures, si vous spécifiez une période de verrouillage des snapshots, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront du délai d'expiration de SnapLock . L'administrateur de stockage doit nettoyer manuellement les clones après l'expiration de SnapLock .
- L'ajout de nouveaux systèmes de fichiers sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec synchronisation active SnapMirror n'est pas pris en charge.

- L'ajout de nouveaux systèmes de fichiers à un groupe de ressources existant en mode de basculement de SnapMirror Active Sync n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement dans un état normal ou de restauration automatique.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources** et le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les actions suivantes :
 - a. Saisissez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ Balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez RH comme balise à plusieurs groupes de ressources, vous pouvez ultérieurement trouver tous les groupes de ressources associés à la balise RH.

- c. Cochez la case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, customtext_resource group_policy_hostname ou resource group_hostname. Par défaut, un horodatage est ajouté au nom de l'instantané.

4. Dans la page Ressources, sélectionnez un nom d'hôte de système de fichiers Unix dans la liste déroulante **Hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource est découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaîtront dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources dans la section Ressources disponibles et déplacez-les vers la section Ressources sélectionnées.

6. Dans la page Paramètres de l'application, procédez comme suit :

- Sélectionnez la flèche Scripts et entrez les commandes pré et post pour les opérations de mise en veille, de capture instantanée et de rétablissement. Vous pouvez également saisir les commandes préalables à exécuter avant de quitter en cas de panne.
- Sélectionnez l'une des options de cohérence de sauvegarde :
 - Sélectionnez **Cohérent avec le système de fichiers** si vous souhaitez vous assurer que les données mises en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde et qu'aucune opération d'entrée ou de sortie n'est autorisée sur le système de fichiers lors de la création de la sauvegarde.



Pour la cohérence du système de fichiers, des instantanés de groupe de cohérence seront pris pour les LUN impliqués dans le groupe de volumes.

- Sélectionnez **Crash Consistent** si vous souhaitez vous assurer que les données mises en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde.



Si vous avez ajouté différents systèmes de fichiers dans le groupe de ressources, tous les volumes des différents systèmes de fichiers du groupe de ressources seront placés dans un groupe de cohérence.

7. Dans la page Politiques, effectuez les étapes suivantes :

- a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez également créer une politique en cliquant sur  .

Dans la section Configurer les planifications pour les stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez  dans la colonne Configurer les planifications pour la politique pour laquelle vous souhaitez configurer une planification.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis cliquez sur **OK**.

Où, *policy_name* est le nom de la politique que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne Planifications appliquées.

Les planifications de sauvegarde tierces ne sont pas prises en charge lorsqu'elles chevauchent les planifications de sauvegarde SnapCenter .

8. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell Set-SmSmtServer.

9. Consultez le résumé, puis cliquez sur **Terminer**.

Créer des groupes de ressources et activer la protection secondaire pour les systèmes de fichiers Unix sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas à la fois des ressources ONTAP 9.x et des ressources ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et des ressources ASA r2.

À propos de cette tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonctionnalité **SecondaryProtection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources est mis en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors du mode maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clonée.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources** et le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les actions suivantes :

- a. Saisissez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ Balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez RH comme balise à plusieurs groupes de ressources, vous pouvez ultérieurement trouver tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, customtext_resource group_policy_hostname ou resource group_hostname. Par défaut, un horodatage est ajouté au nom de l'instantané.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Vous devez utiliser exactement la même destination que celle définie dans l'application, y compris le préfixe, si nécessaire.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **Hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource est découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaîtront dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les vers la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page Politiques, effectuez les étapes suivantes :
 - a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez également créer une politique en cliquant sur  .

Dans la section Configurer les planifications pour les stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez  dans la colonne Configurer les planifications pour la politique pour laquelle vous souhaitez configurer une planification.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis cliquez sur **OK**.

Où, *policy_name* est le nom de la politique que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne Planifications appliquées.

Les planifications de sauvegarde tierces ne sont pas prises en charge lorsqu'elles chevauchent les planifications de sauvegarde SnapCenter .

8. Si la protection secondaire est activée pour la politique que vous avez sélectionnée, la page Protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de politique de réplication.



La politique de réplication synchrone n'est pas prise en charge.

- b. Spécifiez le suffixe du groupe de cohérence que vous souhaitez utiliser.
- c. Dans les listes déroulantes Cluster de destination et SVM de destination, sélectionnez le cluster apparié et le SVM que vous souhaitez utiliser.



Le peering de cluster et de SVM n'est pas pris en charge par SnapCenter. Vous devez utiliser System Manager ou les CLI ONTAP pour effectuer l'appairage de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, ces ressources seront affichées dans la section Ressources protégées secondaires.

1. Sur la page de vérification, effectuez les étapes suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer la vérification sur le stockage secondaire.
- b. Cliquez  dans la colonne Configurer les planifications pour configurer la planification de vérification pour tous les types de planification de la politique.
- c. Dans la boîte de dialogue Ajouter des planifications de vérification *policy_name*, effectuez les actions suivantes :

Si vous voulez...	Fais ceci...
Exécuter la vérification après la sauvegarde	Sélectionnez Exécuter la vérification après la sauvegarde .

Si vous voulez...	Fais ceci...
Planifier une vérification	Sélectionnez Exécuter la vérification planifiée , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **Vérifier sur un emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne Planifications appliquées.

2. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell Set-SmSntpServer.

3. Consultez le résumé, puis cliquez sur **Terminer**.

Sauvegarder les systèmes de fichiers Unix

Si une ressource ne fait partie d'aucun groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources** et le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Chemin** dans la liste Affichage.
3. Cliquez sur , puis sélectionnez le nom de l'hôte et les systèmes de fichiers Unix pour filtrer les ressources.
4. Sélectionnez le système de fichiers que vous souhaitez sauvegarder.
5. Dans la page Ressources, vous pouvez effectuer les étapes suivantes :
 - a. Cochez la case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, `customtext_policy_hostname` ou `resource_hostname`. Un horodatage est ajouté au nom de l'instantané par défaut.

6. Dans la page Paramètres de l'application, procédez comme suit :
 - Sélectionnez la flèche Scripts et entrez les commandes pré et post pour les opérations de mise en veille, de capture instantanée et de rétablissement. Vous pouvez également saisir les commandes préalables à exécuter avant de quitter en cas de panne.
 - Sélectionnez l'une des options de cohérence de sauvegarde :
 - Sélectionnez **Cohérent avec le système de fichiers** si vous souhaitez garantir que les données

mis en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde et qu'aucune opération n'est effectuée sur le système de fichiers lors de la création de la sauvegarde.

- Sélectionnez **Crash Consistent** si vous souhaitez vous assurer que les données mises en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde.

7. Dans la page Politiques, effectuez les étapes suivantes :

- a. Sélectionnez une ou plusieurs politiques dans la liste déroulante.



Vous pouvez créer une politique en cliquant  .

Dans la section Configurer les planifications pour les stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez  dans la colonne Configurer les planifications pour configurer une planification pour la politique souhaitée.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy_name*, configurez la planification, puis sélectionnez OK .

policy_name est le nom de la politique que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne Planifications appliquées.

8. Dans la page Notification, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails dans la liste déroulante **Préférences de courrier électronique**.

Vous devez spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de sauvegarde effectuée sur la ressource, sélectionnez **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell. `Set-SmSmtServer` .

9. Consultez le résumé, puis cliquez sur **Terminer**.

La page de topologie s'affiche.

10. Cliquez sur **Sauvegarder maintenant**.

11. Dans la page Sauvegarde, effectuez les étapes suivantes :

- a. Si vous avez appliqué plusieurs politiques à la ressource, dans la liste déroulante Politique, sélectionnez la politique que vous souhaitez utiliser pour la sauvegarde.

Si la politique sélectionnée pour la sauvegarde à la demande est associée à une planification de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de planification.

- b. Cliquez sur **Sauvegarder**.

12. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

Sauvegarder les groupes de ressources des systèmes de fichiers Unix

Vous pouvez sauvegarder les systèmes de fichiers Unix définis dans le groupe de ressources. Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si un groupe de ressources dispose d'une politique associée et d'une planification configurée, les sauvegardes sont créées conformément à la planification.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources** et le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Saisissez le nom du groupe de ressources dans la zone de recherche ou cliquez sur , et sélectionnez la balise.

Cliquez  pour fermer le volet de filtre.

4. Dans la page Groupe de ressources, sélectionnez le groupe de ressources à sauvegarder.
5. Dans la page Sauvegarde, effectuez les étapes suivantes :
 - a. Si vous avez plusieurs politiques associées au groupe de ressources, sélectionnez la politique de sauvegarde que vous souhaitez utiliser dans la liste déroulante **Politique**.

Si la politique sélectionnée pour la sauvegarde à la demande est associée à une planification de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de planification.
 - b. Sélectionnez **Sauvegarde**.
6. Surveillez la progression en sélectionnant **Surveillance > Tâches**.

Surveiller la sauvegarde des systèmes de fichiers Unix

Découvrez comment surveiller la progression des opérations de sauvegarde et de protection des données.

Surveiller les opérations de sauvegarde des systèmes de fichiers Unix

Vous pouvez surveiller la progression des différentes opérations de sauvegarde en utilisant la page SnapCenterJobs. Vous souhaitez peut-être vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page Tâches et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente

-  Annulé

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page Moniteur, cliquez sur **Tâches**.
3. Dans la page Emplois, effectuez les étapes suivantes :
 - a. Cliquez  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Sauvegarde**.
 - d. Dans la liste déroulante **Statut**, sélectionnez l'état de la sauvegarde.
 - e. Cliquez sur **Appliquer** pour afficher les opérations terminées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche de sauvegarde s'affiche  , lorsque vous cliquez sur les détails de la tâche, vous pouvez voir que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées par des signes d'avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

Surveiller les opérations de protection des données dans le volet Activité

Le volet Activité affiche les cinq opérations les plus récentes effectuées. Le volet Activité affiche également le moment où l'opération a été lancée et l'état de l'opération.

Le volet Activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez  dans le volet Activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

Afficher les systèmes de fichiers Unix protégés dans la page Topologie

Lorsque vous vous préparez à sauvegarder, restaurer ou cloner une ressource, il peut être utile d'afficher une représentation graphique de toutes les sauvegardes, des systèmes de fichiers restaurés et des clones sur le stockage principal et secondaire.

À propos de cette tâche

Dans la page Topologie, vous pouvez voir toutes les sauvegardes, les systèmes de fichiers restaurés et les clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes, systèmes de fichiers restaurés et clones, puis les sélectionner pour effectuer des

opérations de protection des données.

Vous pouvez consulter les icônes suivantes dans la vue Gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies miroir ou copies Vault).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  affiche le nombre de sauvegardes et de clones mis en miroir sur le stockage secondaire à l'aide de la technologie SnapMirror .
-  affiche le nombre de sauvegardes et de clones répliqués sur le stockage secondaire à l'aide de la technologie SnapVault .

Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une politique visant à conserver uniquement 4 sauvegardes, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible en termes de version sur un volume de type coffre-fort miroir sont affichés dans la vue topologique, mais le nombre de sauvegardes miroir dans la vue topologique n'inclut pas la sauvegarde flexible en termes de version.

Si vous avez une relation secondaire en tant que synchronisation active SnapMirror (initialement publié sous le nom de SnapMirror Business Continuity [SM-BC]), vous pouvez voir les icônes supplémentaires suivantes :

-  Le site de réplique est en ligne.
-  Le site de réplique est en panne.
-  La relation miroir secondaire ou coffre-fort n'a pas été rétablie.

Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Afficher**.
3. Sélectionnez la ressource soit à partir de la vue des détails de la ressource, soit à partir de la vue des détails du groupe de ressources.

Si la ressource est protégée, la page Topologie de la ressource sélectionnée s'affiche.

4. Consultez la carte récapitulative pour voir un résumé du nombre de sauvegardes et de clones disponibles sur le stockage principal et secondaire.

La section Carte récapitulative affiche le nombre total de sauvegardes et de clones.

Cliquer sur le bouton **Actualiser** lance une requête sur le stockage pour afficher un décompte précis.

Si une sauvegarde activée par SnapLock est effectuée, cliquer sur le bouton **Actualiser** actualise l'heure d'expiration principale et secondaire de SnapLock récupérée à partir d' ONTAP. Un calendrier hebdomadaire actualise également l'heure d'expiration du SnapLock principal et secondaire récupérée à partir d' ONTAP.

Lorsque le système de fichiers est réparti sur plusieurs volumes, le délai d'expiration de SnapLock pour la sauvegarde correspond au délai d'expiration de SnapLock le plus long défini pour un snapshot dans un volume. Le délai d'expiration SnapLock le plus long est récupéré à partir d' ONTAP.

Pour la synchronisation active de SnapMirror , cliquer sur le bouton **Actualiser** actualise l'inventaire de sauvegarde SnapCenter en interrogeant ONTAP pour les sites principaux et réplicas. Un planning hebdomadaire exécute également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror .

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations Async Mirror ou Async MirrorVault avec la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir d' ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
 - Après le basculement, une sauvegarde doit être créée pour que SnapCenter soit informé du basculement. Vous ne pouvez cliquer sur **Actualiser** qu'après la création d'une sauvegarde.
5. Dans la vue Gérer les copies, cliquez sur **Sauvegardes** ou **Clones** à partir du stockage principal ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Les détails des sauvegardes et des clones sont affichés sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez pas renommer ou supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

7. Si vous souhaitez supprimer un clone, sélectionnez le clone dans le tableau, puis cliquez sur  .

Exemple montrant des sauvegardes et des clones sur le stockage principal



Restaurer et récupérer les systèmes de fichiers Unix

Restaurer les systèmes de fichiers Unix

En cas de perte de données, vous pouvez utiliser SnapCenter pour restaurer les systèmes de fichiers Unix.

À propos de cette tâche

- Vous devez exécuter les commandes suivantes pour établir la connexion avec le serveur SnapCenter , répertorier les sauvegardes et récupérer ses informations, puis restaurer la sauvegarde.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Alternativement, vous pouvez également vous référer à la ["Guide de référence des commandes du logiciel SnapCenter"](#) .

- Pour l'opération de restauration de synchronisation active de SnapMirror , vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Chemin** ou **Groupe de ressources** dans la liste **Affichage**.

3. Sélectionnez le système de fichiers à partir de la vue des détails ou de la vue des détails du groupe de ressources.

La page de topologie s'affiche.

4. Dans la vue Gérer les copies, sélectionnez **Sauvegardes** à partir du système de stockage principal ou secondaire (en miroir ou répliqué).

5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur *  *.

6. Dans la page Restaurer l'étendue :

- Pour les systèmes de fichiers NFS, par défaut, la restauration **Connecter et copier** est sélectionnée. Vous pouvez également sélectionner **Rétablir le volume** ou **Restauration rapide**.
- Pour les systèmes de fichiers non NFS, l'étendue de la restauration est sélectionnée en fonction de la disposition.

Les nouveaux fichiers créés après la sauvegarde peuvent ne pas être disponibles après la restauration en fonction du type et de la disposition du système de fichiers.

7. Dans la page PreOps, entrez les commandes de pré-restauration à exécuter avant d'effectuer une tâche de restauration.
8. Sur la page PostOps, entrez les commandes de post-restauration à exécuter après avoir effectué une tâche de restauration.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à l'emplacement `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` path.

9. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les notifications par courrier électronique.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de restauration effectuée, vous devez sélectionner **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `Set-SmSmtServer`.

10. Consultez le résumé, puis cliquez sur **Terminer**.



Si l'opération de restauration échoue, la restauration n'est pas prise en charge.



En cas de restauration d'un système de fichiers résidant sur un groupe de volumes, l'ancien contenu du système de fichiers n'est pas supprimé. Seul le contenu du système de fichiers cloné sera copié sur le système de fichiers source. Ceci s'applique lorsqu'il existe plusieurs systèmes de fichiers sur le groupe de volumes et des restaurations de système de fichiers NFS par défaut.

11. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

Surveiller les opérations de restauration des systèmes de fichiers Unix

Vous pouvez surveiller la progression des différentes opérations de restauration de SnapCenter à l'aide de la page **Tâches**. Vous souhaitez peut-être vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les états post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez entreprendre.

Les icônes suivantes apparaissent sur la page **Tâches** et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente
-  Annulé

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Emplois**, effectuez les étapes suivantes :
 - a. Cliquez  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
 - d. Dans la liste déroulante **État**, sélectionnez l'état de restauration.
 - e. Cliquez sur **Appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez la tâche de restauration, puis cliquez sur **Détails** pour afficher les détails de la tâche.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

Cloner les systèmes de fichiers Unix

Cloner la sauvegarde du système de fichiers Unix

Vous pouvez utiliser SnapCenter pour cloner le système de fichiers Unix à l'aide de la sauvegarde du système de fichiers.

Avant de commencer

- Vous pouvez ignorer la mise à jour du fichier `fstab` en définissant la valeur de `SKIP_FSTAB_UPDATE` sur **true** dans le fichier `agent.properties` situé dans `/opt/NetApp/snapcenter/scc/etc`.

- Vous pouvez avoir un nom de volume de clonage statique et un chemin de jonction en définissant la valeur de `USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT` sur **true** dans le fichier *agent.properties* situé dans `/opt/NetApp/snapcenter/scc/etc`. Après avoir mis à jour le fichier, vous devez redémarrer le service de création du plug-in SnapCenter en exécutant la commande :
`/opt/NetApp/snapcenter/scc/bin/scc restart`.

Exemple : sans cette propriété, le nom du volume cloné et le chemin de jonction seront comme `<Source_volume_name>_Clone_<Timestamp>` mais maintenant ce sera `<Source_volume_name>_Clone_<Clone_Name>`

Cela maintient le nom constant afin que vous puissiez maintenir manuellement le fichier `fstab` à jour si vous ne préférez pas mettre à jour le `fstab` par SnapCenter.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Chemin** ou **Groupe de ressources** dans la liste **Affichage**.
3. Sélectionnez le système de fichiers à partir de la vue des détails ou de la vue des détails du groupe de ressources.

La page de topologie s'affiche.

4. Dans la vue Gérer les copies, sélectionnez les sauvegardes parmi les copies locales (principales), les copies miroir (secondaires) ou les copies Vault (secondaires).
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur *  *.
6. Dans la page Emplacement, effectuez les actions suivantes :

Pour ce domaine...	Fais ceci...
Cloner le serveur	Par défaut, l'hôte source est renseigné.
Cloner le point de montage	Spécifiez le chemin où le système de fichiers sera monté.

7. Dans la page Scripts, effectuez les étapes suivantes :
 - a. Saisissez les commandes de pré-clonage ou de post-clonage qui doivent être exécutées respectivement avant ou après l'opération de clonage.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir du chemin `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`.

8. Dans la page Notification, dans la liste déroulante **Préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les courriers électroniques.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **Joindre le rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell Set-SmSntpServer.

9. Consultez le résumé, puis cliquez sur **Terminer**.
10. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

Diviser un clone

Vous pouvez utiliser SnapCenter pour diviser une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

À propos de cette tâche

- Vous ne pouvez pas effectuer l'opération de division de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de division de clone sur clone1. Cependant, vous pouvez effectuer l'opération de division de clone sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de division du clone sur le clone1 car le clone1 n'est plus le clone intermédiaire.

- Lorsque vous divisez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de division de volume FlexClone, voir, "[Diviser un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat sur le système de stockage est en ligne.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Afficher :

Option	Description
Pour les applications de base de données	Sélectionnez Base de données dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez Chemin dans la liste Affichage.

3. Sélectionnez la ressource appropriée dans la liste.

La page de topologie des ressources s'affiche.

4. Dans la vue **Gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou le LUN), puis cliquez sur *  *.
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Démarrer**.
6. Surveillez la progression de l'opération en cliquant sur **Surveiller > Tâches**.

L'opération de division du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter l'applet de commande Stop-SmJob pour arrêter l'opération de division du clonage, puis réessayer l'opération de division du clonage.

Si vous souhaitez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pendant lequel SMCore doit interroger l'état de l'opération de division du clone. La valeur est en millisecondes et la valeur par défaut est de 5 minutes.

Par exemple:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si une sauvegarde, une restauration ou un autre fractionnement du clone est en cours. Vous ne devez redémarrer l'opération de division du clone qu'une fois les opérations en cours terminées.

Informations connexes

["Le clonage ou la vérification de SnapCenter échoue avec l'agrégat qui n'existe pas"](#)

Surveiller les opérations de clonage des systèmes de fichiers Unix

Vous pouvez surveiller la progression des opérations de clonage de SnapCenter à l'aide de la page Tâches. Vous souhaitez peut-être vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

À propos de cette tâche

Les icônes suivantes apparaissent sur la page Tâches et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échoué
-  Terminé avec des avertissements ou n'a pas pu démarrer en raison d'avertissements
-  En file d'attente
-  Annulé

Mesures

1. Dans le volet de navigation de gauche, cliquez sur **Moniteur**.
2. Dans la page **Moniteur**, cliquez sur **Tâches**.
3. Dans la page **Emplois**, effectuez les étapes suivantes :
 - a. Cliquez  pour filtrer la liste afin que seules les opérations de clonage soient répertoriées.
 - b. Précisez les dates de début et de fin.
 - c. Dans la liste déroulante **Type**, sélectionnez **Cloner**.

- d. Dans la liste déroulante **Statut**, sélectionnez le statut du clonage.
 - e. Cliquez sur **Appliquer** pour afficher les opérations terminées avec succès.
4. Sélectionnez la tâche de clonage, puis cliquez sur **Détails** pour afficher les détails de la tâche.
 5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Informations sur le copyright

Copyright © 2025 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.