Concepts

SnapCenter Software 4.9

NetApp
October 06, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/snapcenter-49/concept/concept_snapcenter_overview.html on October 06, 2025. Always check docs.netapp.com for the latest.

Sommaire

Concepts . . . 1
- Présentation de SnapCenter . . . 1
  - Architecture SnapCenter . . . 3
  - Composants de SnapCenter . . . 3
  - Serveur SnapCenter . . . 4
  - Plug-ins SnapCenter . . . 5
  - Référentiel SnapCenter . . . 8
- Fonctions de sécurité . . . 8
  - Présentation du certificat CA . . . 9
  - Communication SSL bidirectionnelle . . . 9
  - Présentation de l’authentification basée sur certificat . . . 9
  - Authentification multifacteur (MFA) . . . 9
- Contrôle d’accès basé sur des rôles (RBAC) SnapCenter . . . 10
  - Types de RBAC . . . 10
  - Autorisations et rôles RBAC . . . 11
  - Rôles et autorisations SnapCenter prédéfinis . . . 13
- Reprise d’activité SnapCenter . . . 17
- Ressources, groupes de ressources et politiques . . . 17
- Préscripts et postscripts . . . 19
  - Types de script pris en charge . . . 19
  - Chemin du script . . . 20
  - Où spécifier des scripts . . . 20
  - Délais d’expiration du script . . . 20
  - Sortie du script . . . 20
- Automatisation d’SnapCenter avec les API REST . . . 20

Concepts

Présentation de SnapCenter

Le logiciel SnapCenter est une plateforme simple, centralisée et évolutive qui protège les données de vos applications, bases de données, systèmes de fichiers hôtes et machines virtuelles qui s'exécutent sur les systèmes ONTAP à partir de n'importe quel point du cloud hybride.

SnapCenter exploite les technologies NetApp Snapshot, SnapRestore, FlexClone, SnapMirror et SnapVault pour offrir les avantages suivants :

- Des sauvegardes sur disque rapides, compactes et cohérentes au niveau des applications
- Des restaurations rapides et granulaires au niveau des applications
- Un clonage rapide et compact

SnapCenter inclut à la fois le serveur SnapCenter et des plug-ins légers. Vous pouvez automatiser le déploiement de plug-ins sur des hôtes d'application distants, planifier les sauvegardes, vérifier les opérations de clonage et surveiller toutes les opérations de protection des données.

SnapCenter peut être déployé de plusieurs manières :

- Sur site, pour protéger ce qui suit :
  - Les données qui résident dans les systèmes primaires ONTAP FAS, AFF ou ASA et qui sont répliquées vers les systèmes secondaires ONTAP FAS, AFF ou ASA
  - Les données qui résident dans les systèmes primaires ONTAP Select
  - Les données qui se trouvent sur les systèmes primaires et secondaires ONTAP FAS, AFF ou ASA et qui sont protégées pour le stockage objet local StorageGRID
- Sur site, dans un cloud hybride, pour protéger ce qui suit :
  - Les données qui résident dans les systèmes primaires ONTAP FAS, AFF ou ASA et qui sont répliquées vers Cloud Volumes ONTAP
  - Données qui se trouvent sur les systèmes primaires et secondaires ONTAP FAS, AFF ou ASA et protégées dans le stockage d'objets et d'archives dans le cloud à l'aide de l'intégration de sauvegarde et de récupération NetApp
- Dans un cloud public, pour protéger :
  - Les données qui résident dans les systèmes primaires Cloud Volumes ONTAP (anciennement ONTAP Cloud)
  - Données qui se trouvent sur Amazon FSX pour ONTAP

SnapCenter inclut les fonctionnalités clés suivantes :

- Protection des données centralisée et cohérente avec les applications

  La protection des données est prise en charge pour Microsoft Exchange Server, Microsoft SQL Server, les bases de données Oracle sous Linux ou AIX, les bases de données SAP HANA et les systèmes de fichiers hôtes Windows s'exécutant sur des systèmes ONTAP.

  La protection des données est également prise en charge pour d'autres applications et bases de données

standard ou personnalisées grâce à une structure permettant de créer des plug-ins SnapCenter définis par l'utilisateur. La protection des données est ainsi assurée pour d'autres applications et bases de données depuis une seule fenêtre. En tirant parti de ce framework, NetApp a publié des plug-ins personnalisés SnapCenter pour IBM DB2, MongoDB, MySQL, etc.

- Sauvegardes basées sur des règles

  Les sauvegardes basées sur des règles tirent parti de la technologie de copie NetApp Snapshot pour créer des sauvegardes sur disque rapides, compactes et cohérentes avec les applications. Vous pouvez également automatiser la protection de ces sauvegardes sur un stockage secondaire par une mise à jour des relations de protection existantes.

- Sauvegardez des sauvegardes multiples pour plusieurs ressources

  Vous pouvez sauvegarder simultanément plusieurs ressources (applications, bases de données ou systèmes de fichiers hôtes) du même type à l'aide des groupes de ressources SnapCenter.

- Restauration et reprise

  SnapCenter offre des restaurations rapides et granulaires de sauvegardes et de restaurations basées sur le temps et cohérentes avec les applications. Vous pouvez restaurer les données depuis n'importe quelle destination dans le cloud hybride.

- Clonage

  SnapCenter offre un clonage rapide, compact et cohérent au niveau des applications, ce qui permet d'accélérer le développement logiciel. Vous pouvez cloner sur n'importe quelle destination dans le cloud hybride.

- Interface utilisateur graphique de gestion utilisateur unique

  L'interface graphique de SnapCenter offre une interface complète pour la gestion des sauvegardes et des clones d'une ressource de toutes les destinations dans le cloud hybride.

- API REST, applets de commande Windows, commandes UNIX

  SnapCenter inclut des API REST pour la plupart des fonctionnalités d'intégration avec n'importe quel logiciel d'orchestration, et l'utilisation d'applets de commande Windows PowerShell et d'une interface de ligne de commandes.

  Pour plus d'informations sur les API REST, voir "Présentation de l'API REST".

  Pour plus d'informations sur les applets de commande Windows, reportez-vous à la section "Guide de référence de l'applet de commande".

  Pour plus d'informations sur les commandes UNIX, voir "Guide de référence sur les commandes du logiciel SnapCenter".

- Tableau de bord et reporting centralisés pour la protection des données
- Contrôle d'accès basé sur des rôles (RBAC) pour la sécurité et la délégation.
- Base de données de référentiel avec haute disponibilité

  SnapCenter fournit une base de données de référentiel intégrée avec une haute disponibilité pour stocker toutes les métadonnées de sauvegarde.

- Installation automatisée des plug-ins

  Vous pouvez automatiser une poussée à distance des plug-ins SnapCenter depuis l'hôte SnapCenter Server vers les hôtes applicatifs.

- Haute disponibilité

  La haute disponibilité de SnapCenter est configurée à l'aide d'un équilibreur de charge externe (F5). Un même data Center prend en charge jusqu'à deux nœuds.

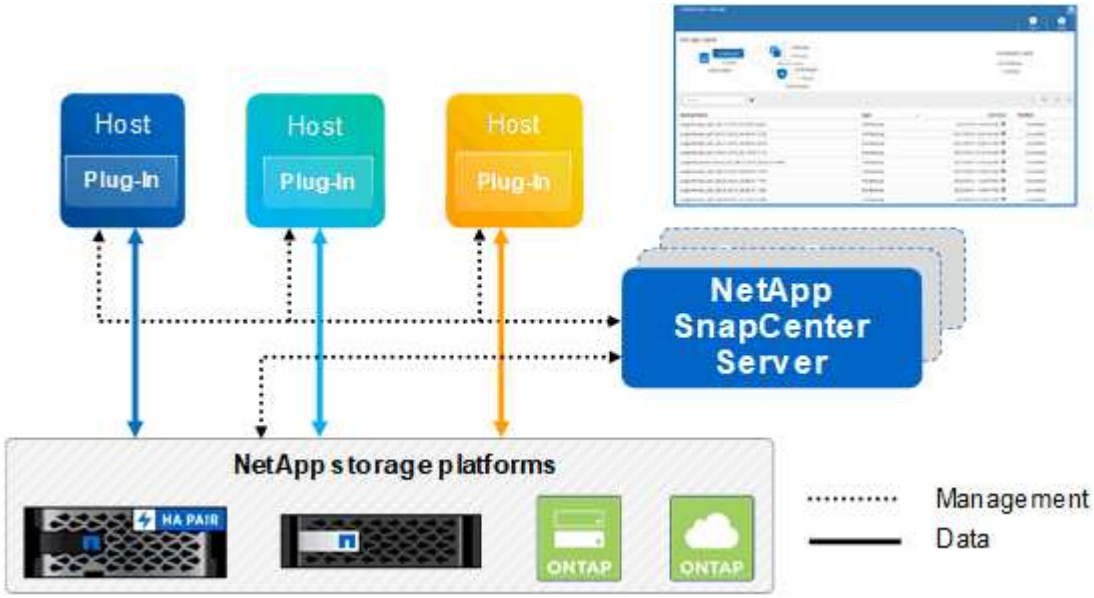
- Reprise après incident

  Vous pouvez restaurer le serveur SnapCenter en cas d'incident, comme une corruption des ressources ou une panne du serveur.

Architecture SnapCenter

La plateforme SnapCenter est basée sur une architecture multiniveaux qui inclut un serveur de gestion centralisée (SnapCenter Server) et un hôte de plug-in SnapCenter.

SnapCenter prend en charge les data centers multisites. Le serveur SnapCenter et l'hôte du plug-in peuvent se trouver à différents emplacements géographiques.



Composants de SnapCenter

SnapCenter se compose du serveur SnapCenter et des plug-ins SnapCenter. Vous devez installer uniquement les plug-ins appropriés aux données que vous souhaitez protéger.

- Serveur SnapCenter
- Package de plug-ins SnapCenter pour Windows, qui comprend les plug-ins suivants :
  - Plug-in SnapCenter pour Microsoft SQL Server
  - Plug-in SnapCenter pour Microsoft Windows
  - Plug-in SnapCenter pour Microsoft Exchange Server

    - Plug-in SnapCenter pour base de données SAP HANA
- SnapCenter Plug-ins Package pour Linux, qui comprend les plug-ins suivants :
    - Plug-in SnapCenter pour bases de données Oracle
    - Plug-in SnapCenter pour base de données SAP HANA
    - Plug-in SnapCenter pour UNIX

> Le plug-in SnapCenter pour UNIX n'est pas un plug-in autonome et ne peut pas être installé indépendamment. Ce plug-in est automatiquement installé lorsque vous installez le plug-in SnapCenter pour Oracle Database ou le plug-in SnapCenter pour SAP HANA Database.

- SnapCenter Plug-ins Package pour AIX, qui comprend les plug-ins suivants :
    - Plug-in SnapCenter pour bases de données Oracle
    - Plug-in SnapCenter pour UNIX

> Le plug-in SnapCenter pour UNIX n'est pas un plug-in autonome et ne peut pas être installé indépendamment. Ce plug-in est automatiquement installé lorsque vous installez le plug-in SnapCenter pour la base de données Oracle.

- Plug-ins personnalisés SnapCenter

  Des plug-ins personnalisés sont pris en charge par la communauté.

Le plug-in SnapCenter pour VMware vSphere, anciennement NetApp Data Broker, est une appliance virtuelle autonome prenant en charge les opérations de protection des données SnapCenter sur des bases de données et des systèmes de fichiers virtualisés.

Serveur SnapCenter

Le serveur SnapCenter comprend un serveur Web, une interface utilisateur centralisée basée sur HTML5, des applets de commande PowerShell, des API REST et un référentiel SnapCenter.

SnapCenter assure une haute disponibilité et une évolutivité horizontale sur plusieurs serveurs SnapCenter au sein d'une interface utilisateur unique. Vous pouvez obtenir une haute disponibilité à l'aide de l'équilibreur de charge externe (F5). Pour les environnements de taille supérieure avec des milliers d'hôtes, l'ajout de plusieurs serveurs SnapCenter peut vous aider à équilibrer la charge.

- Si vous utilisez le module de plug-ins SnapCenter pour Windows, l'agent hôte s'exécute sur le serveur SnapCenter et le plug-in Windows. L'agent hôte exécute les planifications de manière native sur l'hôte Windows distant ou, pour Microsoft SQL Server, le planning est exécuté sur l'instance SQL locale.

  Le serveur SnapCenter communique avec les plug-ins Windows via l'agent hôte.

- Si vous utilisez le module de plug-ins SnapCenter pour Linux ou le module de plug-ins SnapCenter pour AIX, les planifications sont exécutées sur le serveur SnapCenter en tant que planifications de tâches Windows.
    - Pour le plug-in SnapCenter pour la base de données Oracle, l'agent hôte qui s'exécute sur l'hôte SnapCenter Server communique avec le chargeur de plug-in SnapCenter (SPL) qui s'exécute sur l'hôte Linux ou AIX afin d'effectuer différentes opérations de protection des données.

- Pour le plug-in SnapCenter pour base de données SAP HANA et plug-ins personnalisés SnapCenter, le serveur SnapCenter communique avec ces plug-ins via l'agent SCCore qui s'exécute sur l'hôte.

Le serveur SnapCenter et les plug-ins communiquent avec l'agent hôte via HTTPS. Les informations relatives aux opérations SnapCenter sont stockées dans le référentiel SnapCenter.

SnapCenter prend en charge l'espace de noms disjoint pour les hôtes Windows. Si vous rencontrez des problèmes lors de l'utilisation d'un espace de noms disjoint, reportez-vous à la section "SnapCenter ne parvient pas à détecter les ressources lors de l'utilisation d'un namespace disjoint".

Plug-ins SnapCenter

Chaque plug-in SnapCenter prend en charge des environnements, des bases de données et des applications spécifiques.

Nom du plug-in	Inclus dans le package d'installation	Requiert d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in pour SQL Server	Plug-ins Package pour Windows	Plug-in pour Windows	Hôte SQL Server	Répertoires de base
Plug-in pour Windows	Plug-ins Package pour Windows		Hôte Windows	Répertoires de base
Plug-in pour Exchange	Plug-ins Package pour Windows	Plug-in pour Windows	Hôte Exchange Server	Répertoires de base
Plug-in pour Oracle Database	Plug-ins Package pour Linux et Plug-ins Package pour AIX	Plug-in pour UNIX	Hôte Oracle	Linux ou AIX
Plug-in pour base de données SAP HANA	Module de plug-ins pour Linux et module de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte client HDBSQL	Linux ou Windows
Plug-ins personnalisés		Pour les sauvegardes de système de fichiers, Plug-in pour Windows	Hôte d'application personnalisé	Linux ou Windows

Le plug-in SnapCenter pour VMware vSphere prend en charge les opérations de sauvegarde et de restauration cohérentes avec les défaillances et les machines virtuelles pour les machines virtuelles, les datastores et les disques virtuels (VMDK). Il prend également en charge les plug-ins spécifiques aux applications SnapCenter afin de protéger les opérations de sauvegarde et de restauration cohérentes avec les applications pour les bases de données et les systèmes de fichiers virtualisés.

Pour les utilisateurs de SnapCenter 4.1.1, la documentation du plug-in SnapCenter pour VMware vSphere 4.1.1 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers. Pour les utilisateurs de SnapCenter 4.2.x, NetApp Data Broker 1.0 et 1.0.1, la documentation relative à la protection des bases de données et des systèmes de fichiers virtualisés à l'aide du plug-in SnapCenter pour VMware vSphere fourni par le dispositif virtuel NetApp Data Broker basé sur Linux (format Open Virtual Appliance). Pour les utilisateurs utilisant SnapCenter 4.3 ou version ultérieure, le "Documentation du plug-in SnapCenter pour VMware vSphere" Possède des informations sur la protection des bases de données virtualisées et des systèmes de fichiers à l'aide du plug-in SnapCenter pour dispositif virtuel VMware vSphere (format Appliance virtuelle ouverte) basé sur Linux.

Fonctionnalités du plug-in SnapCenter pour Microsoft SQL Server

- Automatise les opérations de sauvegarde, de restauration et de clonage respectueuses des applications pour les bases de données Microsoft SQL Server dans votre environnement SnapCenter.
- Prend en charge les bases de données Microsoft SQL Server sur des LUN VMDK et RDM (Raw Device Mapping) lorsque vous déployez le plug-in SnapCenter pour VMware vSphere et enregistrez le plug-in avec SnapCenter
- Prend uniquement en charge le provisionnement des partages SMB. Elle n'est pas prise en charge pour la sauvegarde des bases de données SQL Server sur les partages SMB.
- Prise en charge de l'importation de sauvegardes depuis SnapManager pour Microsoft SQL Server vers SnapCenter.

Le plug-in SnapCenter pour les fonctionnalités de Microsoft Windows

- Protège les données respectueuses des applications pour les autres plug-ins exécutés dans les hôtes Windows de votre environnement SnapCenter
- Automatise les opérations de sauvegarde, de restauration et de clonage respectueuses des applications pour les systèmes de fichiers Microsoft dans votre environnement SnapCenter
- Prend en charge le provisionnement du stockage, la cohérence des copies Snapshot et la récupération d'espace pour les hôtes Windows

Le plug-in pour Windows provisionne les partages SMB et les systèmes de fichiers Windows sur les LUN physiques et RDM, mais ne prend pas en charge les opérations de sauvegarde pour les systèmes de fichiers Windows sur les partages SMB.

Fonctionnalités du plug-in SnapCenter pour Microsoft Exchange Server

- Automatise les opérations de sauvegarde et de restauration respectueuses des applications pour les bases de données Microsoft Exchange Server et les groupes de disponibilité de base de données (DAG) dans votre environnement SnapCenter
- Prise en charge des serveurs Exchange virtualisés sur des LUN RDM lors du déploiement du plug-in SnapCenter pour VMware vSphere et enregistrement du plug-in avec SnapCenter

Fonctionnalités du plug-in SnapCenter pour les bases de données Oracle

- Automatisation de la sauvegarde, de la restauration et de la récupération respectueuses des applications, de la vérification, du montage et Démontez et clonez des opérations de base de données Oracle dans votre environnement SnapCenter
- Prend en charge les bases de données Oracle pour SAP, mais l'intégration de SAP BR*Tools n'est pas fournie

Plug-in SnapCenter pour UNIX fonctionnalités

- 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 NFS (Network File System) et SAN (Storage Area Network) sur un système de stockage exécutant ONTAP.
- Pour les systèmes Linux, les bases de données Oracle sur des LUN VMDK et RDM sont prises en charge lorsque vous déployez le plug-in SnapCenter pour VMware vSphere et que vous enregistrez le plug-in avec SnapCenter.
- Prend en charge Mount Guard pour AIX sur les systèmes de fichiers SAN et la disposition LVM.
- Prise en charge du système JFS2 (Enhanced journalised File System) avec consignation en ligne sur les systèmes de fichiers SAN et disposition LVM pour les systèmes AIX uniquement.

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

Fonctionnalités du plug-in SnapCenter pour les bases de données SAP HANA

- Automatise la sauvegarde, la restauration et le clonage des bases de données SAP HANA respectueuses des applications dans votre environnement SnapCenter

Fonctionnalités des plug-ins personnalisés SnapCenter

- Prise en charge de plug-ins personnalisés pour gérer des applications ou des bases de données qui ne sont pas prises en charge par d'autres plug-ins SnapCenter. Les plug-ins personnalisés ne sont pas fournis lors de l'installation de SnapCenter.
- Prise en charge de la création de copies en miroir des jeux de sauvegarde sur un autre volume et de la réplication de sauvegarde disque à disque.
- Prise en charge des environnements Windows et Linux. Dans les environnements Windows, les applications personnalisées via des plug-ins personnalisés peuvent, en option, utiliser le plug-in SnapCenter pour Microsoft Windows pour créer des sauvegardes cohérentes avec le système de fichiers.

Les plug-ins personnalisés MySQL, DB2 et MongoDB sont pris en charge uniquement par les communautés NetApp.

NetApp prend en charge la possibilité de créer et d'utiliser des plug-ins personnalisés. Cependant, les plug-ins personnalisés que vous créez ne sont pas pris en charge par NetApp.

Pour plus d'informations, voir "Développez un plug-in pour votre application"

Référentiel SnapCenter

Le référentiel SnapCenter, parfois appelé base de données NSM, stocke des informations et des métadonnées pour chaque opération SnapCenter.

La base de données du référentiel du serveur MySQL est installée par défaut lorsque vous installez le serveur SnapCenter. Si MySQL Server est déjà installé et que vous effectuez une nouvelle installation de SnapCenter Server, vous devez désinstaller MySQL Server.

SnapCenter prend en charge MySQL Server 5.7.25 ou version ultérieure en tant que base de données de référentiel SnapCenter. Si vous utilisiez une version antérieure de MySQL Server avec une version antérieure de SnapCenter, pendant la mise à niveau de SnapCenter, le serveur MySQL est mis à niveau vers la version 5.7.25 ou ultérieure.

Le référentiel SnapCenter stocke les informations et métadonnées suivantes :

- Sauvegarde, clonage, restauration et vérification des métadonnées
- Informations sur les rapports, les tâches et les événements
- Informations sur l'hôte et les plug-ins
- Informations sur le rôle, l'utilisateur et les autorisations
- Informations de connexion du système de stockage

Fonctions de sécurité

SnapCenter utilise des fonctionnalités de sécurité et d'authentification strictes pour sécuriser vos données.

SnapCenter comprend les fonctions de sécurité suivantes :

- Toutes les communications avec SnapCenter utilisent HTTP over SSL (HTTPS).
- Toutes les identifiants de SnapCenter sont protégés à l'aide d'un chiffrement AES (Advanced Encryption Standard).
- SnapCenter utilise des algorithmes de sécurité conformes à la norme FIPS (Federal information Processing Standard).
- SnapCenter prend en charge l'utilisation des certificats d'autorité de certification agréés fournis par le client.
- SnapCenter 4.1.1 ou version ultérieure prend en charge la communication TLS (transport Layer Security) 1.2 avec ONTAP. Vous pouvez également utiliser la communication TLS 1.2 entre les clients et les serveurs.
- SnapCenter prend en charge un certain nombre de suites de cryptage SSL pour assurer la sécurité dans toute la communication réseau.

  Pour plus d'informations, voir "Configuration de la suite de cryptage SSL prise en charge".

- SnapCenter est installé à l'intérieur du pare-feu de votre entreprise pour permettre l'accès au serveur SnapCenter et permettre la communication entre le serveur SnapCenter et les plug-ins.
- L'accès en opération et l'API SnapCenter utilise des jetons chiffrés avec un chiffrement AES, qui expire au bout de 24 heures.

- SnapCenter s'intègre à Windows Active Directory pour la connexion et le contrôle d'accès basé sur des rôles (RBAC) qui régissent les autorisations d'accès.
- IPSec est pris en charge avec SnapCenter sur ONTAP pour les machines hôtes Windows et Linux. "En savoir plus >>".
- Les applets de commande SnapCenter PowerShell sont sécurisés pour la session.
- Après une période d'inactivité par défaut de 15 minutes, SnapCenter vous avertit que vous serez déconnecté dans 5 minutes. Au bout de 20 minutes d'inactivité, SnapCenter vous déconnecte et vous devez vous reconnecter. Vous pouvez modifier la période de déconnexion.
- La connexion est temporairement désactivée après 5 tentatives de connexion incorrectes ou plus.
- Prend en charge l'authentification de certificat d'autorité de certification entre le serveur SnapCenter et ONTAP. "En savoir plus >>".
- Le vérificateur d'intégrité est ajouté au serveur SnapCenter et aux plug-ins et il valide tous les binaires expédiés pendant les nouvelles opérations d'installation et de mise à niveau.

Présentation du certificat CA

Le programme d'installation du serveur SnapCenter active la prise en charge centralisée du certificat SSL pendant l'installation. Pour améliorer la communication sécurisée entre le serveur et le plug-in, SnapCenter prend en charge l'utilisation des certificats d'autorité de certification autorisés fournis par le client.

Vous devez déployer les certificats d'autorité de certification après avoir installé le serveur SnapCenter et les plug-ins correspondants. Pour plus d'informations, voir "Générer le fichier CSR de certificat CA".

Vous pouvez également déployer le certificat d'autorité de certification pour le plug-in SnapCenter pour VMware vSphere. Pour plus d'informations, voir "Créer et importer des certificats".

Communication SSL bidirectionnelle

La communication SSL bidirectionnelle sécurise la communication mutuelle entre le serveur SnapCenter et les plug-ins.

Présentation de l'authentification basée sur certificat

L'authentification basée sur certificat vérifie l'authenticité des utilisateurs qui tentent d'accéder à l'hôte du plug-in SnapCenter. L'utilisateur doit exporter le certificat du serveur SnapCenter sans clé privée et l'importer dans le magasin de confiance hôte du plug-in. L'authentification basée sur certificat fonctionne uniquement si la fonction SSL bidirectionnelle est activée.

Authentification multifacteur (MFA)

L'authentification multifacteur fait appel à un fournisseur d'identité tiers via le langage SAML pour gérer les sessions utilisateur. Cette fonctionnalité améliore la sécurité de l'authentification en ayant la possibilité d'utiliser plusieurs facteurs tels que le TOTP, la biométrie, les notifications push, etc., ainsi que le nom d'utilisateur et le mot de passe existants. De plus, il permet au client d'utiliser ses propres fournisseurs d'identité d'utilisateur pour obtenir un identifiant d'utilisateur unifié (SSO) dans son portefeuille.

L'authentification multifacteur s'applique uniquement à la connexion à l'interface utilisateur du serveur SnapCenter. Les identifiants de connexion sont authentifiés via le IDP Active Directory Federation Services (AD FS). Vous pouvez configurer différents facteurs d'authentification sur AD FS. SnapCenter est le fournisseur de services. Vous devez configurer SnapCenter en tant que fournisseur de stockage basé dans AD FS. Pour activer MFA dans SnapCenter, vous aurez besoin des métadonnées AD FS.

Pour plus d'informations sur l'activation de MFA, reportez-vous à la section "Activer l'authentification multifacteur".

Contrôle d'accès basé sur des rôles (RBAC) SnapCenter

Types de RBAC

Le contrôle d'accès basé sur des rôles (RBAC) SnapCenter et les autorisations ONTAP permettent aux administrateurs SnapCenter de déléguer le contrôle des ressources SnapCenter à différents utilisateurs ou groupes d'utilisateurs. Cet accès géré de manière centralisée permet aux administrateurs d'applications de travailler en toute sécurité dans les environnements délégués.

Vous pouvez créer et modifier des rôles, ajouter un accès aux ressources aux utilisateurs à tout moment, mais lorsque vous configurez SnapCenter pour la première fois, vous devez ajouter au moins des utilisateurs ou des groupes Active Directory aux rôles, puis ajouter un accès aux ressources à ces utilisateurs ou groupes.

> Vous ne pouvez pas utiliser SnapCenter pour créer des comptes d'utilisateur ou de groupe. Vous devez créer des comptes d'utilisateur ou de groupe dans Active Directory du système d'exploitation ou de la base de données.

SnapCenter utilise les types suivants de contrôle d'accès basé sur les rôles :

- RBAC SnapCenter
- Plug-in RBAC SnapCenter (pour certains plug-ins)
- RBAC au niveau des applications
- Autorisations ONTAP

RBAC SnapCenter

Rôles et autorisations

SnapCenter propose des rôles prédéfinis avec des autorisations déjà attribuées. Vous pouvez affecter des utilisateurs ou des groupes d'utilisateurs à ces rôles. Vous pouvez également créer de nouveaux rôles et gérer les autorisations et les utilisateurs.

Affectation d'autorisations aux utilisateurs ou aux groupes

Vous pouvez attribuer des autorisations aux utilisateurs ou aux groupes pour accéder aux objets SnapCenter tels que les hôtes, les connexions de stockage et les groupes de ressources. Vous ne pouvez pas modifier les autorisations du rôle SnapCenterAdmin.

Vous pouvez attribuer des autorisations RBAC aux utilisateurs et groupes au sein de la même forêt et aux utilisateurs appartenant à différentes forêts. Vous ne pouvez pas attribuer d'autorisations RBAC aux utilisateurs appartenant à des groupes imbriqués dans les forêts.

> Si vous créez un rôle personnalisé, il doit contenir toutes les autorisations du rôle d'administrateur SnapCenter. Si vous copiez uniquement certaines autorisations, par exemple, l'ajout ou le retrait d'hôte, vous ne pouvez pas effectuer ces opérations.

Authentification

Les utilisateurs doivent fournir une authentification lors de la connexion, via l'interface utilisateur graphique ou via les applets de commande PowerShell. Si les utilisateurs sont membres de plusieurs rôles, après avoir saisi des informations d'identification, ils sont invités à spécifier le rôle qu'ils souhaitent utiliser. Les utilisateurs doivent également fournir une authentification pour l'exécution des API.

RBAC au niveau des applications

SnapCenter utilise les identifiants pour vérifier que les utilisateurs SnapCenter autorisés disposent également des autorisations au niveau de l'application.

Par exemple, si vous souhaitez effectuer des opérations de copie Snapshot et de protection des données dans un environnement SQL Server, vous devez définir des identifiants avec les identifiants Windows ou SQL appropriés. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une ou l'autre méthode. Pour effectuer des opérations de copie Snapshot et de protection des données dans un environnement de système de fichiers Windows sur un système de stockage ONTAP, le rôle d'administrateur SnapCenter doit disposer de privilèges d'administration sur l'hôte Windows.

De même, si vous souhaitez effectuer des opérations de protection des données sur une base de données Oracle et si l'authentification du système d'exploitation est désactivée dans l'hôte de la base de données, vous devez définir les informations d'identification avec la base de données Oracle ou les informations d'identification Oracle ASM. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une de ces méthodes, en fonction de l'opération.

Plug-in SnapCenter pour VMware vSphere RBAC

Si vous utilisez le plug-in SnapCenter pour la protection de données cohérente avec les machines virtuelles, vCenter Server offre un niveau supplémentaire de contrôle d'accès basé sur des rôles (RBAC). Le plug-in SnapCenter prend en charge le RBAC de vCenter Server et le RBAC d'Data ONTAP.

Pour plus d'informations, reportez-vous à la section "Plug-in SnapCenter pour VMware vSphere RBAC"

Autorisations ONTAP

Vous devez créer un compte vsadmin avec les autorisations requises pour accéder au système de stockage

Pour plus d'informations sur la création du compte et l'attribution des autorisations, reportez-vous à la section "Créez un rôle de cluster ONTAP avec des privilèges minimaux"

Autorisations et rôles RBAC

Le contrôle d'accès basé sur des rôles (RBAC) SnapCenter vous permet de créer des rôles et d'attribuer des autorisations à ces rôles, puis d'attribuer des utilisateurs ou des groupes d'utilisateurs aux rôles. Les administrateurs SnapCenter peuvent ainsi créer un environnement géré de manière centralisée, tandis que les administrateurs d'applications peuvent gérer les tâches de protection des données. SnapCenter propose des rôles et des autorisations prédéfinis.

Rôles SnapCenter

SnapCenter propose les rôles prédéfinis suivants. Vous pouvez attribuer des utilisateurs et des groupes à ces rôles ou créer de nouveaux rôles.

Lorsque vous attribuez un rôle à un utilisateur, seuls les travaux pertinents à cet utilisateur sont visibles dans la page travaux, à moins que vous n'ayez affecté le rôle d'administrateur SnapCenter.

- Admin sauvegarde et clonage d'applications
- Sauvegardez et clonez Viewer
- Administrateur de l'infrastructure
- SnapCenter

Le plug-in SnapCenter pour les rôles VMware vSphere

Pour gérer la protection des données cohérente avec les machines virtuelles des machines virtuelles, des VMDK et des datastores, les rôles suivants sont créés dans vCenter par le plug-in SnapCenter pour VMware vSphere :

- Administrateur de distributeurs sélectifs
- Vue du distributeur auxiliaire
- Secours du distributeur auxiliaire
- Restauration du distributeur auxiliaire
- Restauration du fichier invité du distributeur auxiliaire

Pour plus d'informations, voir "Types de RBAC pour le plug-in SnapCenter pour les utilisateurs VMware vSphere"

Meilleure pratique : NetApp vous recommande de créer un rôle ONTAP pour les opérations du plug-in SnapCenter pour VMware vSphere et de lui attribuer tous les privilèges requis.

Autorisations SnapCenter

SnapCenter offre les autorisations suivantes :

- Groupe de ressources
- Politique
- Sauvegarde
- Hôte
- Connexion de stockage
- Clonage
- Provisionnement (uniquement pour la base de données Microsoft SQL)
- Tableau de bord
- Rapports
- Restaurer
  - Restauration du volume complet (uniquement pour les plug-ins personnalisés)
- Ressource

  Les privilèges de plug-in sont requis de la part de l'administrateur pour que les non-administrateurs puissent effectuer une opération de découverte des ressources.

- Installation ou désinstallation du plug-in

  > Lorsque vous activez les autorisations d'installation du plug-in, vous devez également modifier l'autorisation Host pour activer les lectures et les mises à jour.

- Migration
- Montage (uniquement pour la base de données Oracle)
- Démonter (uniquement pour la base de données Oracle)
- Moniteur de tâche

  L'autorisation moniteur de tâches permet aux membres de différents rôles de voir les opérations sur tous les objets auxquels ils sont affectés.

Rôles et autorisations SnapCenter prédéfinis

SnapCenter propose des rôles prédéfinis, chacun avec un ensemble d'autorisations déjà activé. Lors de la configuration et de l'administration du contrôle d'accès basé sur des rôles (RBAC), vous pouvez utiliser ces rôles prédéfinis ou en créer de nouveaux.

SnapCenter inclut les rôles prédéfinis suivants :

- Rôle d'administrateur SnapCenter
- Rôle d'administrateur de clones et de sauvegarde des applications
- Rôle Backup and Clone Viewer
- Rôle d'administrateur de l'infrastructure

Lorsque vous ajoutez un utilisateur à un rôle, vous devez attribuer l'autorisation StorageConnection pour activer la communication SVM (Storage Virtual machine) ou affecter un SVM à l'utilisateur pour permettre l'utilisation de la SVM. L'autorisation Storage Connection permet aux utilisateurs de créer des connexions SVM.

Par exemple, un utilisateur avec le rôle administrateur SnapCenter peut créer des connexions SVM et les affecter à un utilisateur avec le rôle Administrateur App Backup and Clone, qui par défaut n'a pas la permission de créer ou de modifier des connexions SVM. Sans connexion SVM, les utilisateurs ne peuvent pas mener à bien les opérations de sauvegarde, de clonage ou de restauration.

Rôle d'administrateur SnapCenter

Toutes les autorisations sont activées pour le rôle d'administrateur SnapCenter. Vous ne pouvez pas modifier les autorisations pour ce rôle. Vous pouvez ajouter des utilisateurs et des groupes au rôle ou les supprimer.

Rôle d'administrateur de clones et de sauvegarde des applications

Le rôle d'administrateur d'applications et de clones dispose des autorisations nécessaires pour effectuer des actions administratives pour les sauvegardes d'applications et les tâches liées au clonage. Ce rôle ne dispose pas des autorisations nécessaires pour la gestion des hôtes, le provisionnement, la gestion des connexions de stockage ou l'installation à distance.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.
Politique	Sans objet	Oui.	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Oui.	Oui.	Oui.	Oui.
Provisionnement	Sans objet	Non	Oui.	Non	Non
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Non	Sans objet		Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle Backup and Clone Viewer

Le rôle de la visionneuse de sauvegarde et de clonage dispose d'une vue en lecture seule de toutes les autorisations. Ce rôle est également doté d'autorisations pour la découverte, le reporting et l'accès au Tableau

de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Non	Oui.	Non	Non
Politique	Sans objet	Non	Oui.	Non	Non
Sauvegarde	Sans objet	Non	Oui.	Non	Non
Hôte	Sans objet	Non	Oui.	Non	Non
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Non	Oui.	Non	Non
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Non	Non	Sans objet	Sans objet	Sans objet
Ressource	Non	Non	Oui.	Oui.	Non
Installation/désinstallation du plug-in	Non	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Sans objet	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle d’administrateur de l’infrastructure

Le rôle d’administrateur de l’infrastructure possède des autorisations pour la gestion des hôtes, la gestion du stockage, le provisionnement, les groupes de ressources, les rapports d’installation à distance, Et l’accès au Tableau de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.
Politique	Sans objet	Non	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Oui.	Oui.	Oui.	Oui.
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Oui.	Oui.	Oui.	Oui.
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Non	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Non	Sans objet	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Reprise d'activité SnapCenter

Vous pouvez restaurer le serveur SnapCenter en cas d'incidents tels que la corruption de ressources ou la panne du serveur grâce à la fonction de reprise après incident SnapCenter. Vous pouvez restaurer le référentiel SnapCenter, les planifications de serveur et les composants de configuration de serveur. Vous pouvez également restaurer le plug-in SnapCenter pour SQL Server et le plug-in SnapCenter pour le stockage SQL Server.

Cette section décrit les deux types de reprise sur incident dans SnapCenter :

Reprise après incident du serveur SnapCenter

- Les données du serveur SnapCenter sont sauvegardées et peuvent être restaurées sans ajout ou gestion de plug-in au serveur SnapCenter.
- Le serveur SnapCenter secondaire doit être installé sur le même répertoire d'installation et sur le même port que le serveur SnapCenter principal.
- Pour l'authentification multifacteur (MFA), pendant la reprise sur incident du serveur SnapCenter, fermez tous les onglets du navigateur et rouvrez un navigateur pour vous reconnecter. Ceci effacera les cookies de session existants ou actifs et mettra à jour les données de configuration correctes.
- La fonctionnalité de reprise après incident SnapCenter utilise les API REST pour sauvegarder SnapCenter Server. Voir "Workflows d'API REST pour la reprise après incident d'un serveur SnapCenter".
- Le fichier de configuration associé aux paramètres d'audit n'est pas sauvegardé dans la sauvegarde de reprise sur incident ni sur le serveur DR après l'opération de restauration. Vous devez répéter manuellement les paramètres du journal d'audit.

Plug-in SnapCenter et reprise après incident du stockage

La reprise après incident est uniquement prise en charge pour le plug-in SnapCenter pour SQL Server. Lorsque le plug-in SnapCenter pour SQL Server est en panne, basculez vers un autre hôte SQL et restaurez les données en suivant quelques étapes. Voir "Reprise après incident du plug-in SnapCenter pour SQL Server".

SnapCenter réplique les données à l'aide de la technologie ONTAP SnapMirror. Celui-ci peut servir à répliquer des données vers un site secondaire pour la reprise après incident et à les synchroniser. Un basculement peut être initié en casser la relation de réplication dans SnapMirror. En cas de rétablissement, la synchronisation peut être inversée et les données du site de reprise sur incident peuvent être répliquées à nouveau vers l'emplacement principal.

Ressources, groupes de ressources et politiques

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- **Les ressources** sont généralement des bases de données, des systèmes de fichiers Windows ou des partages de fichiers que vous sauvegardez ou clonez avec SnapCenter.

  Toutefois, selon votre environnement, les ressources peuvent être des instances de base de données, des groupes de disponibilité Microsoft SQL Server, des bases de données Oracle RAC, des systèmes de fichiers Windows ou un groupe d'applications personnalisées.

- Un **groupe de ressources** est un ensemble de ressources sur un hôte ou un cluster. Le groupe de ressources peut également contenir des ressources provenant de plusieurs hôtes et de plusieurs clusters.

  Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur toutes les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

  Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également configurer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

  > Si vous mettez un hôte d'un groupe de ressources partagé en mode maintenance et si des planifications sont associées au même groupe de ressources partagées, toutes les opérations planifiées seront suspendues pour tous les autres hôtes du groupe de ressources partagées.

  Vous devez utiliser un plug-in de base de données pour sauvegarder des bases de données, un plug-in de système de fichiers pour sauvegarder des systèmes de fichiers et le plug-in SnapCenter pour VMware vSphere pour sauvegarder des machines virtuelles et des datastores.

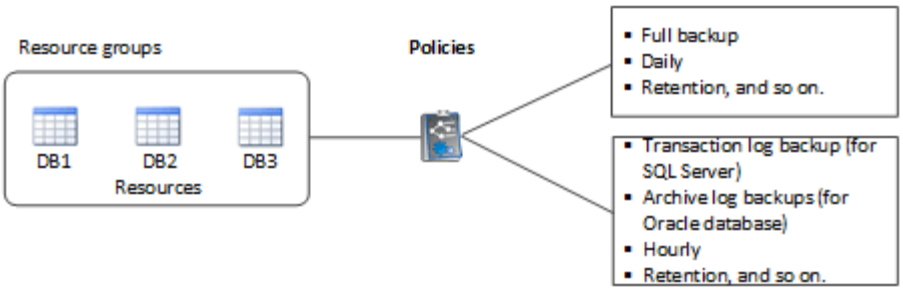
- **Stratégies** spécifier la fréquence de sauvegarde, la conservation des copies, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

  Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande.

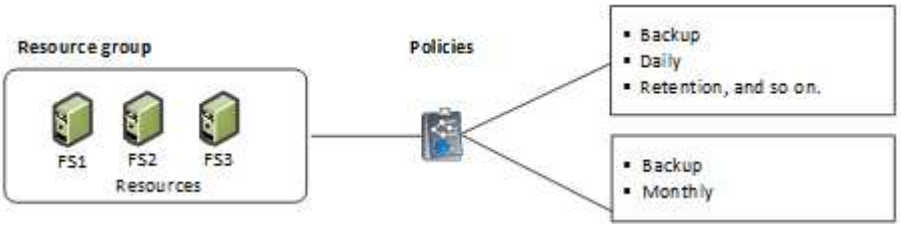
Pensez à un groupe de ressources comme définissant *quoi* vous voulez protéger et quand vous voulez le protéger en termes de jour et de temps. Pensez à une stratégie comme définir *comment* vous voulez la protéger. Si vous sauvegardez toutes les bases de données ou que vous sauvegardez tous les systèmes de fichiers d'un hôte, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données ou tous les systèmes de fichiers de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire.

Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources pour effectuer une sauvegarde complète tous les jours et un autre programme qui effectue des sauvegardes de journaux toutes les heures.

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



L'image suivante illustre la relation entre les ressources, les groupes de ressources et les stratégies des systèmes de fichiers Windows :



Préscripts et postscripts

Vous pouvez utiliser des prescripteurs et des postscripts personnalisés dans le cadre de vos opérations de protection des données. Ces scripts permettent l'automatisation avant ou après votre tâche de protection des données. Vous pouvez, par exemple, inclure un script qui vous informe automatiquement des échecs ou des avertissements liés aux tâches de protection des données. Avant de configurer vos prescripteurs et vos postscripts, vous devez comprendre certaines des conditions requises pour la création de ces scripts.

Types de script pris en charge

Les types de scripts suivants sont pris en charge pour Windows :

- Fichiers de traitement par lots
- Scripts PowerShell
- Scripts Perl

Les types de scripts suivants sont pris en charge pour UNIX :

- Scripts Perl
- Scripts Python
- Scripts de shell

> Outre le shell bash par défaut, d'autres shells comme sh-shell, k-shell et c-shell sont également pris en charge.

Chemin du script

Tous les scripts prescripteurs et post-scripts exécutés dans le cadre des opérations SnapCenter, sur les systèmes de stockage virtualisés et non virtualisés, sont exécutés sur l'hôte du plug-in.

- Les scripts Windows doivent se trouver sur l'hôte du plug-in.

Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN_SCRIPTS.

- Les scripts UNIX doivent se trouver sur l'hôte du plug-in.

Le chemin du script est validé au moment de l'exécution.

Où spécifier des scripts

Les scripts sont spécifiés dans les politiques de sauvegarde. Lorsqu'une tâche de sauvegarde est lancée, la stratégie associe automatiquement le script aux ressources sauvegardées. Lorsque vous créez une stratégie de sauvegarde, vous pouvez spécifier les arguments prescripteurs et PostScript.

Vous ne pouvez pas spécifier plusieurs scripts.

Délais d'expiration du script

Le délai est défini sur 60 secondes, par défaut. Vous pouvez modifier la valeur de temporisation.

Sortie du script

Le répertoire par défaut des fichiers de sortie Windows prescripts et postscripts est Windows\System32.

Il n'existe pas d'emplacement par défaut pour les prescripteurs et les postscripts UNIX. Vous pouvez rediriger le fichier de sortie vers n'importe quel emplacement préféré.

Automatisation d'SnapCenter avec les API REST

Vous pouvez utiliser des API REST pour effectuer plusieurs opérations de gestion du SnapCenter. Les API REST sont exposées via la page Web de swagger. Vous pouvez accéder à la page Web swagger pour afficher la documentation de l'API REST, ainsi que pour lancer manuellement un appel d'API. Vous pouvez utiliser des API REST pour gérer votre serveur SnapCenter ou votre hôte SnapCenter vSphere.

Les API REST pour…	Sont situés dans…
Serveur SnapCenter	\Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/
Plug-in SnapCenter pour VMware vSphere	\Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html#

Pour plus d’informations sur les API REST de SnapCenter, reportez-vous à la section "Présentation des API REST"

Pour plus d’informations sur le plug-in SnapCenter pour les API REST VMware vSphere, consultez la section "Plug-in SnapCenter pour les API REST VMware vSphere"

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 DÉLICTUELLE (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.