En savoir plus sur le SnapCenter software

SnapCenter software

NetApp
November 06, 2025

Sommaire

En savoir plus sur le SnapCenter software

Présentation de SnapCenter

Le SnapCenter software est une plate-forme simple, centralisée et évolutive pour une protection des données cohérente avec les applications. Il protège les applications, les bases de données, les systèmes de fichiers hôtes et les machines virtuelles sur les systèmes ONTAP dans le cloud hybride.

SnapCenter utilise les technologies NetApp Snapshot, SnapRestore, FlexClone, SnapMirror et SnapVault pour fournir :

- Sauvegardes rapides, peu encombrantes, cohérentes avec les applications et basées sur disque
- Restauration rapide et détaillée et récupération cohérente avec les applications
- Clonage rapide et peu encombrant

SnapCenter inclut SnapCenter Server et des plug-ins légers. Vous pouvez automatiser le déploiement de plug-ins sur des hôtes d'applications distants, planifier des opérations de sauvegarde, de vérification et de clonage, et surveiller les opérations de protection des données.

Vous pouvez installer SnapCenter sur site ou sur un cloud public pour protéger les données.

- Sur site pour protéger les éléments suivants :
  - Données qui se trouvent sur les systèmes principaux ONTAP FAS, AFF ou ASA et répliquées sur les systèmes secondaires ONTAP FAS, AFF ou ASA
  - Données qui se trouvent sur les systèmes primaires ONTAP Select
  - Données qui se trouvent sur les systèmes primaires et secondaires ONTAP FAS, AFF ou ASA et protégées sur le stockage d'objets StorageGRID local
  - Données présentes sur les systèmes primaires et secondaires ONTAP ASA r2
- Sur site dans un cloud hybride pour protéger les éléments suivants :
  - Données qui se trouvent sur les systèmes principaux ONTAP FAS, AFF ou ASA et répliquées sur 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 éléments suivants :
  - Données qui se trouvent sur les systèmes principaux Cloud Volumes ONTAP (anciennement ONTAP Cloud)
  - Données présentes sur Amazon FSX pour ONTAP
  - Données présentes sur les Azure NetApp Files principaux (Oracle, Microsoft SQL et SAP HANA)

Caractéristiques principales

SnapCenter fournit les fonctionnalités clés suivantes :

- Protection centralisée et cohérente des données des différentes applications

La protection des données est prise en charge pour Microsoft Exchange Server, Microsoft SQL Server, les bases de données Oracle sur Linux ou AIX, la base de données SAP HANA, IBM Db2, PostgreSQL, MySQL et les systèmes de fichiers hôtes Windows exécutés sur les systèmes ONTAP . SnapCenter prend également en charge la protection d'applications telles que MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Sauvegardes basées sur des politiques

  Les sauvegardes basées sur des politiques exploitent la technologie NetApp Snapshot pour créer des sauvegardes sur disque rapides, économes en espace et cohérentes avec les applications. Vous pouvez également configurer la protection automatique de ces sauvegardes sur un stockage secondaire en mettant à jour les relations de protection existantes.

- Sauvegardes pour plusieurs ressources

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

- Restauration et récupération

  SnapCenter fournit des restaurations rapides et granulaires des sauvegardes et une récupération cohérente avec les applications et basée sur le temps. Vous pouvez restaurer à partir de n'importe quelle destination dans le Cloud hybride.

- Clonage

  SnapCenter permet un clonage rapide, peu encombrant et cohérent avec les applications. Vous pouvez cloner sur n'importe quelle destination dans le Cloud hybride.

- Interface utilisateur graphique de gestion mono-utilisateur

  SnapCenter fournit une interface unique pour gérer les sauvegardes et les clones dans n'importe quelle destination de cloud hybride.

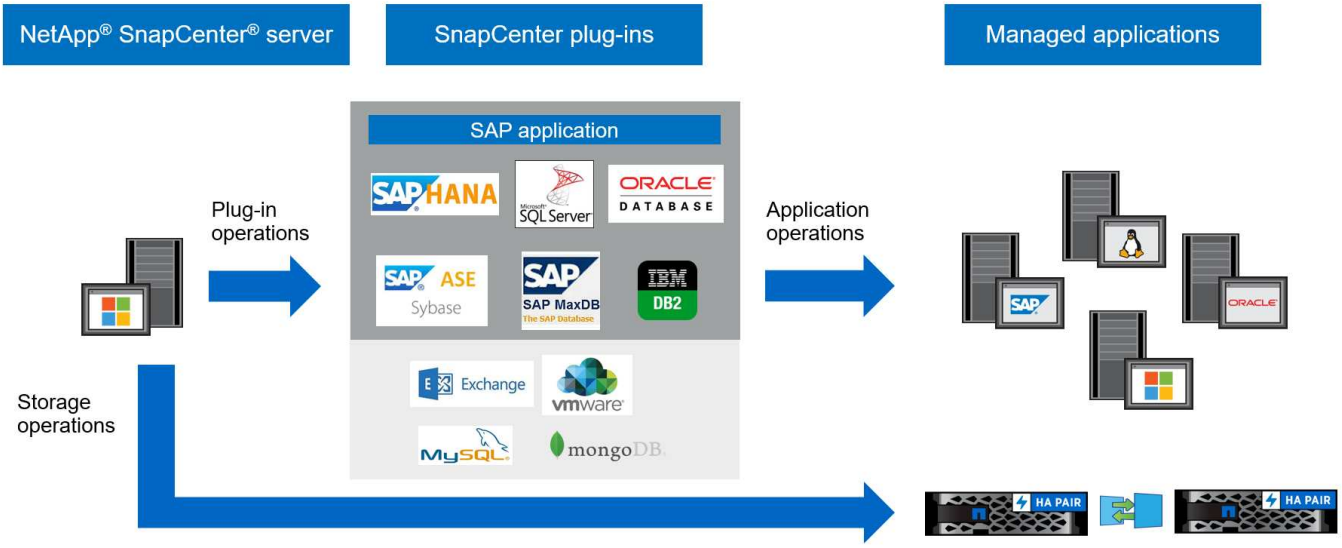
- API REST, applets de commande Windows, commandes UNIX

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

- Tableau de bord et rapports centralisés sur la protection des données
- Contrôle d'accès basé sur les rôles (RBAC) pour la sécurité et la délégation
- Une base de données de référentiel intégrée à haute disponibilité pour stocker toutes les métadonnées de sauvegarde
- Installation automatique des plug-ins
- Haute disponibilité
- Reprise après sinistre (DR)
- SnapLock "En savoir plus"
- Synchronisation active SnapMirror (initialement publié sous le nom de SnapMirror Business Continuity [SM-BC])
- Mise en miroir synchrone "En savoir plus"

Architecture et composants de SnapCenter

SnapCenter utilise une conception en couches avec un serveur de gestion central et des hôtes de plug-in. Le serveur et les hôtes du plug-in peuvent se trouver à des emplacements différents.



SnapCenter inclut le serveur SnapCenter , le package de plug-in SnapCenter pour Windows et le package de plug-in SnapCenter pour Linux. Chaque package contient des plug-ins pour diverses applications et composants d'infrastructure.

Serveur SnapCenter

Le serveur SnapCenter prend en charge les systèmes d'exploitation Microsoft Windows et Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Le serveur SnapCenter comprend un serveur Web, une interface utilisateur centralisée basée sur HTML5, des applets de commande PowerShell, des API REST et le référentiel SnapCenter .

SnapCenter stocke les informations sur ses opérations dans le référentiel SnapCenter .

Plugins 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	Nécessite d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour Microsoft SQL Server	Pack de plug-ins pour Windows	Plug-in pour Windows	Hôte SQL Server	Windows
Plug-in SnapCenter pour Windows	Pack de plug-ins pour Windows		hôte Windows	Windows

Nom du plug-in	Inclus dans le package d'installation	Nécessite d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour Microsoft Exchange Server	Pack de plug-ins pour Windows	Plug-in pour Windows	Hôte du serveur Exchange	Windows
Plug-in SnapCentre pour la base de données Oracle	Pack de plug-ins pour Linux et pack de plug-ins pour AIX	Plug-in pour UNIX	Hôte Oracle	Linux ou AIX
Plug-in SnapCenter pour la base de données SAP HANA	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte client HDBSQL	Linux ou Windows
Plug-in SnapCenter pour IBM Db2	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte Db2	Linux, AIX ou Windows
Plug-in SnapCenter pour PostgreSQL	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte PostgreSQL	Linux ou Windows
Plug-in SnaoCenter pour MySQL	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou Plug-in pour Windows	Hôte MySQL	Linux ou Windows
Plug-in SnapCenter pour MongoDB	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte MongoDB	Linux ou Windows
Plug-in SnapCenter pour ORASCPM (Oracle Applications)	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte Oracle	Linux ou Windows
Plug-in SnapCenter pour SAP ASE	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	hôte SAP	Linux ou Windows

Nom du plug-in	Inclus dans le package d'installation	Nécessite d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour SAP MaxDB	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte SAP MaxDB	Linux ou Windows
Plug-in SnapCenter pour le plug-in de stockage	Pack de plug-ins pour Linux et pack de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte de stockage	Linux ou Windows

Le SnapCenter Plug-in for VMware vSphere prend en charge les opérations de sauvegarde et de restauration cohérentes en cas de panne et cohérentes avec les machines virtuelles (VM), les banques de données et les disques de machines virtuelles (VMDK). Il prend également en charge les opérations de sauvegarde et de restauration cohérentes avec les applications pour les bases de données et les systèmes de fichiers virtualisés.

Pour protéger les bases de données, les systèmes de fichiers, les machines virtuelles ou les banques de données sur les machines virtuelles, déployez le SnapCenter Plug-in for VMware vSphere . Pour plus d'informations, reportez-vous à "Documentation du SnapCenter Plug-in for VMware vSphere" .

Référentiel SnapCenter

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

L'installation de SnapCenter Server installe la base de données du référentiel MySQL Server par défaut. Si vous avez déjà installé MySQL Server et que vous souhaitez effectuer une nouvelle installation de SnapCenter Server, vous devez désinstaller MySQL Server.

SnapCenter prend en charge MySQL Server 8.0.37 ou version ultérieure comme base de données de référentiel SnapCenter . Si vous utilisez une version antérieure de MySQL Server avec une version antérieure de SnapCenter, le processus de mise à niveau de SnapCenter met à niveau MySQL Server vers la version 8.0.37 ou ultérieure.

Le référentiel SnapCenter stocke les informations et métadonnées suivantes :

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

Fonctionnalités de sécurité dans SnapCenter

SnapCenter utilise des fonctionnalités de sécurité et d'authentification strictes pour vous permettre de protéger vos données.

SnapCenter inclut les fonctionnalités de sécurité suivantes :

- Toutes les communications avec SnapCenter utilisent HTTP sur SSL (HTTPS).
- Toutes les informations d'identification dans SnapCenter sont protégées à l'aide du cryptage Advanced Encryption Standard (AES).
- Prend en charge les algorithmes de sécurité conformes à la norme fédérale de traitement de l'information (FIPS).
- Prend en charge l'utilisation des certificats CA autorisés fournis par le client.
- Prend en charge Transport Layer Security (TLS) 1.3 pour la communication avec ONTAP. Vous pouvez également utiliser TLS 1.2 pour la communication entre les clients et les serveurs.
- Prend en charge un certain ensemble de suites de chiffrement SSL pour assurer la sécurité des communications réseau. "Apprendre encore plus" .
- SnapCenter est installé à l'intérieur du pare-feu de votre entreprise pour permettre l'accès au serveur SnapCenter et pour permettre la communication entre le serveur SnapCenter et les plug-ins.
- L'accès à l'API et aux opérations SnapCenter utilise des jetons chiffrés avec le chiffrement AES, qui expirent après 24 heures.
- SnapCenter s'intègre à Windows Active Directory pour la connexion et le contrôle d'accès basé sur les rôles (RBAC) qui régissent les autorisations d'accès.
- IPsec est pris en charge avec SnapCenter sur ONTAP pour les machines hôtes Windows et Linux. "Apprendre encore plus" .
- Les applets de commande SnapCenter PowerShell sont sécurisées par session.
- Après une période d'inactivité par défaut de 15 minutes, SnapCenter vous avertit que vous serez déconnecté dans 5 minutes.

  Après 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.
- Prend en charge l'authentification par certificat CA entre SnapCenter Server et ONTAP. "Apprendre encore plus" .
- Integrity Verifier est ajouté au serveur SnapCenter et aux plug-ins et il valide tous les binaires livrés lors des nouvelles opérations d'installation et de mise à niveau.

Présentation du certificat CA

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

Vous devez déployer les certificats CA après l'installation du serveur SnapCenter et des plug-ins respectifs. Pour plus d'informations, consultez la section "Générer le fichier CSR du certificat CA" .

Vous pouvez également déployer un certificat CA pour le plug-in SnapCenter pour VMware vSphere. Pour plus d'informations, consultez la section "Créer et importer des certificats" .

Communication SSL bidirectionnelle

La communication SSL bidirectionnelle sécurise la communication mutuelle entre SnapCenter Server et les

plug-ins.

Présentation de l'authentification basée sur les certificats

L'authentification basée sur un certificat vérifie l'authenticité des utilisateurs respectifs 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 de l'hôte du plug-in. L'authentification basée sur un certificat ne fonctionne que si la fonction SSL bidirectionnelle est activée.

Authentification multifacteur (MFA)

MFA utilise un fournisseur d'identité tiers (IdP) via le langage SAML (Security Assertion Markup Language) pour gérer les sessions utilisateur. Cette fonctionnalité améliore la sécurité de l'authentification en offrant la possibilité d'utiliser plusieurs facteurs tels que TOTP, la biométrie, les notifications push, etc. avec le nom d'utilisateur et le mot de passe existants. En outre, il permet au client d'utiliser ses propres fournisseurs d'identité utilisateur pour obtenir une connexion utilisateur unifiée (SSO) sur l'ensemble de son portefeuille.

L'authentification multifacteur s'applique uniquement à la connexion à l'interface utilisateur de SnapCenter Server. Les connexions sont authentifiées via les services de fédération Active Directory (AD FS) du fournisseur d'identité. Vous pouvez configurer différents facteurs d'authentification sur AD FS. SnapCenter est le fournisseur de services et vous devez configurer SnapCenter comme partie de confiance dans AD FS. Pour activer MFA dans SnapCenter, vous aurez besoin des métadonnées AD FS.

Pour plus d'informations sur l'activation de l'authentification multifacteur, voir"Activer l'authentification multifacteur" .

Contrôle d'accès basé sur les rôles dans SnapCenter

Le contrôle d'accès basé sur les rôles (RBAC) de SnapCenter et les autorisations ONTAP permettent aux administrateurs de 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 des environnements délégués.

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

Types de RBAC dans SnapCenter

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

- SnapCenter RBAC
- RBAC au niveau de l'application
- Plug-in SnapCenter pour VMware vSphere RBAC

- Autorisations ONTAP

SnapCenter RBAC

SnapCenter dispose de rôles prédéfinis et vous pouvez attribuer des utilisateurs ou des groupes d'utilisateurs à ces rôles. Les rôles prédéfinis sont :

- Rôle d'administrateur SnapCenter
- Rôle d'administrateur de sauvegarde et de clonage d'applications
- Rôle de visionneuse de sauvegarde et de clonage
- Rôle d'administrateur d'infrastructure

Lorsque vous attribuez un rôle à un utilisateur, seules les tâches pertinentes pour cet utilisateur sont visibles dans la page Tâches, sauf si vous avez attribué le rôle SnapCenterAdmin.

Vous pouvez également créer de nouveaux rôles et gérer les autorisations et les utilisateurs. 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 pouvez attribuer des autorisations RBAC aux utilisateurs et aux 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 des forêts.

Si vous créez un rôle personnalisé, il doit contenir toutes les autorisations du rôle SnapCenterAdmin. Si vous copiez uniquement certaines des autorisations, par exemple, l'ajout ou la suppression d'un hôte, vous ne pouvez pas effectuer ces opérations.

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

RBAC au niveau de l'application

SnapCenter utilise les informations d'identification pour vérifier que les utilisateurs SnapCenter autorisés disposent également d'autorisations au niveau de l'application.

Par exemple, si vous souhaitez effectuer des opérations de protection des données dans un environnement SQL Server, vous devez définir les informations d'identification avec les informations d'identification Windows ou SQL appropriées. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une ou l'autre méthode. Si vous souhaitez effectuer des opérations de protection des données dans un environnement de système de fichiers Windows sur le stockage ONTAP , le rôle d'administrateur SnapCenter doit disposer de privilèges d'administrateur 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 (OS) est désactivée dans l'hôte de la base de données, vous devez définir les informations d'identification avec les informations d'identification de la base de données Oracle ou 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.

SnapCenter Plug-in for VMware vSphere RBAC

Si vous utilisez le plug-in SnapCenter VMware pour une protection des données cohérente avec la machine virtuelle, vCenter Server fournit un niveau supplémentaire de RBAC. Le plug-in SnapCenter VMware prend en charge vCenter Server RBAC et ONTAP RBAC. "En savoir plus"

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

Autorisations ONTAP

Vous devez créer un compte vsadmin avec les autorisations requises pour accéder au système de stockage."En savoir plus"

Autorisations attribuées aux rôles SnapCenter prédéfinis

Lorsque vous ajoutez un utilisateur à un rôle, vous devez attribuer soit l'autorisation StorageConnection pour activer la communication de la machine virtuelle de stockage (SVM), soit attribuer une SVM à l'utilisateur pour activer l'autorisation d'utiliser la SVM. L'autorisation Connexion de stockage permet aux utilisateurs de créer des connexions SVM.

Par exemple, un utilisateur doté du rôle d'administrateur SnapCenter peut créer des connexions SVM et les attribuer à un utilisateur doté du rôle d'administrateur de sauvegarde et de clonage d'applications, qui, par défaut, n'a pas l'autorisation de créer ou de modifier des connexions SVM. Sans connexion SVM, les utilisateurs ne peuvent effectuer aucune opération de sauvegarde, de clonage ou de restauration.

Rôle d'administrateur SnapCenter

Le rôle d'administrateur SnapCenter dispose de toutes les autorisations activées. 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 sauvegarde et de clonage d'applications

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

Autorisations	Activé	Créer	Lire	Mise à jour	Supprimer
Groupe de ressources	Non Concerné	Oui	Oui	Oui	Oui
Politique	Non Concerné	Oui	Oui	Oui	Oui
Sauvegarde	Non Concerné	Oui	Oui	Oui	Oui
Hôte	Non Concerné	Oui	Oui	Oui	Oui
Connexion de stockage	Non Concerné	Non	Oui	Non	Non

Autorisations	Activé	Créer	Lire	Mise à jour	Supprimer
Cloner	Non Concerné	Oui	Oui	Oui	Oui
Disposition	Non Concerné	Non	Oui	Non	Non
Tableau de bord	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Rapports	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Restaurer	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Ressource	Oui	Oui	Oui	Oui	Oui
Installation/désinstallation du plug-in	Non	Non Concerné		Non Concerné	Non Concerné
Migration	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Monter	Oui	Oui	Non Concerné	Non Concerné	Non Concerné
Démonter	Oui	Oui	Non Concerné	Non Concerné	Non Concerné
Restauration complète du volume	Non	Non	Non Concerné	Non Concerné	Non Concerné
Protection secondaire	Non	Non	Non Concerné	Non Concerné	Non Concerné
Moniteur d'emploi	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné

Rôle de visionneuse de sauvegarde et de clonage

Le rôle Visualiseur de sauvegarde et de clonage dispose d'une vue en lecture seule de toutes les autorisations. Ce rôle dispose également d'autorisations activées pour la découverte, la création de rapports et l'accès au tableau de bord.

Autorisations	Activé	Créer	Lire	Mise à jour	Supprimer
Groupe de ressources	Non Concerné	Non	Oui	Non	Non
Politique	Non Concerné	Non	Oui	Non	Non

Autorisations	Activé	Créer	Lire	Mise à jour	Supprimer
Sauvegarde	Non Concerné	Non	Oui	Non	Non
Hôte	Non Concerné	Non	Oui	Non	Non
Connexion de stockage	Non Concerné	Non	Oui	Non	Non
Cloner	Non Concerné	Non	Oui	Non	Non
Disposition	Non Concerné	Non	Oui	Non	Non
Tableau de bord	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Rapports	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Restaurer	Non	Non	Non Concerné	Non Concerné	Non Concerné
Ressource	Non	Non	Oui	Oui	Non
Installation/désinstallation du plug-in	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Migration	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Monter	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Démonter	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Restauration complète du volume	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Protection secondaire	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Moniteur d'emploi	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné

Rôle d'administrateur d'infrastructure

Le rôle d'administrateur d'infrastructure dispose d'autorisations activées 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	Créer	Lire	Mise à jour	Supprimer
Groupe de ressources	Non Concerné	Oui	Oui	Oui	Oui
Politique	Non Concerné	Non	Oui	Oui	Oui
Sauvegarde	Non Concerné	Oui	Oui	Oui	Oui
Hôte	Non Concerné	Oui	Oui	Oui	Oui
Connexion de stockage	Non Concerné	Oui	Oui	Oui	Oui
Cloner	Non Concerné	Non	Oui	Non	Non
Disposition	Non Concerné	Oui	Oui	Oui	Oui
Tableau de bord	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Rapports	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Restaurer	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Ressource	Oui	Oui	Oui	Oui	Oui
Installation/désinstallation du plug-in	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Migration	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Monter	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Démonter	Non	Non Concerné	Non Concerné	Non Concerné	Non Concerné
Restauration complète du volume	Non	Non	Non Concerné	Non Concerné	Non Concerné
Protection secondaire	Non	Non	Non Concerné	Non Concerné	Non Concerné
Moniteur d’emploi	Oui	Non Concerné	Non Concerné	Non Concerné	Non Concerné

Reprise après sinistre dans SnapCenter

La fonctionnalité de récupération après sinistre (DR) de SnapCenter vous permet de récupérer après des sinistres tels que la corruption des ressources ou les pannes de serveur. Il permet de restaurer le référentiel SnapCenter , les planifications du serveur, les composants de configuration et le plug-in SnapCenter pour SQL Server et son stockage.

Cette section explique les deux types de DR dans SnapCenter:

Restauration après sinistre du serveur SnapCenter

- Les données du serveur SnapCenter sont sauvegardées et peuvent être récupérées sans aucun plug-in ajouté ou géré par le 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 après sinistre de SnapCenter Server, fermez tous les onglets du navigateur et rouvrez un navigateur pour vous reconnecter. Cela effacera les cookies de session existants ou actifs et mettra à jour les données de configuration correctes.
- La fonctionnalité de récupération après sinistre de SnapCenter utilise les API REST pour sauvegarder le serveur SnapCenter . Voir "Workflows de l'API REST pour la reprise après sinistre de SnapCenter Server" .
- Le fichier de configuration lié aux paramètres d'audit n'est pas sauvegardé dans la sauvegarde DR 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 sinistre du stockage

DR est disponible uniquement pour le plug-in SnapCenter pour SQL Server. Si le plug-in est en panne, passez à un autre hôte SQL et récupérez les données en suivant quelques étapes. Voir "Récupération après sinistre du plug-in SnapCenter pour SQL Server" .

SnapCenter utilise ONTAP SnapMirror pour répliquer les données, qui peuvent être utilisées pour la reprise après sinistre en gardant les données synchronisées sur un site secondaire. Pour lancer le basculement, interrompez la réplication SnapMirror . Lors de la reprise après sinistre, inversez la synchronisation pour répliquer les données du site DR vers l'emplacement principal.

Licences requises par SnapCenter

SnapCenter nécessite plusieurs licences pour permettre la protection des données des applications, des bases de données, des systèmes de fichiers et des machines virtuelles. Le type de licences SnapCenter que vous installez dépend de votre environnement de stockage et des fonctionnalités que vous souhaitez utiliser.

Licence	Si nécessaire
Contrôleur standard SnapCenter	Obligatoire pour FAS, AFF, ASA La licence SnapCenter Standard est une licence basée sur un contrôleur et est incluse dans le cadre de NetApp ONTAP One. Si vous disposez de la licence SnapManager Suite, vous bénéficiez également du droit de licence SnapCenter Standard. Si vous souhaitez installer SnapCenter à titre d'essai avec le stockage FAS, AFF ou ASA , vous pouvez obtenir une licence d'évaluation NetApp ONTAP One en contactant le représentant commercial. Pour plus d'informations sur les licences incluses avec NetApp ONTAP One, reportez-vous à "Licences incluses avec NetApp ONTAP One" . SnapCenter est également proposé dans le cadre d'un pack de protection des données. Si vous avez acheté l'A400 ou une version ultérieure, vous devez acheter le pack de protection des données.
SnapMirror ou SnapVault	ONTAP Une licence SnapMirror ou SnapVault est requise si la réplication est activée dans SnapCenter.
SnapRestore	Nécessaire pour restaurer et vérifier les sauvegardes. Sur les systèmes de stockage primaires • Requis sur les systèmes de destination SnapVault pour effectuer une vérification à distance et restaurer à partir d'une sauvegarde. • Requis sur les systèmes de destination SnapMirror pour effectuer une vérification à distance.

Licence	Si nécessaire
FlexClone	Nécessaire pour cloner des bases de données et des opérations de vérification. Sur les systèmes de stockage primaires et secondaires • Requis sur les systèmes de destination SnapVault pour créer des clones à partir d'une sauvegarde de coffre-fort secondaire. • Requis sur les systèmes de destination SnapMirror pour créer des clones à partir d'une sauvegarde SnapMirror secondaire.
Licences de protocole	• Licence iSCSI ou FC pour les LUN • Licence CIFS pour les actions SMB • Licence NFS pour les VMDK de type NFS • Licence iSCSI ou FC pour les VMDK de type VMFS Requis sur les systèmes de destination SnapMirror pour diffuser des données si un volume source n'est pas disponible.
Licences SnapCenter Standard (en option)	Destinations secondaires Il est recommandé, mais pas obligatoire, d'ajouter des licences SnapCenter Standard aux destinations secondaires. Si les licences SnapCenter Standard ne sont pas activées sur les destinations secondaires, vous ne pouvez pas utiliser SnapCenter pour sauvegarder les ressources sur la destination secondaire après avoir effectué une opération de basculement. Cependant, une licence FlexClone est requise sur les destinations secondaires pour effectuer des opérations de clonage et de vérification.

Licence	Si nécessaire
Licences de récupération de boîte aux lettres unique (SMBR)	Si vous utilisez SnapCenter Plug-in pour Exchange pour gérer les bases de données Microsoft Exchange Server et Single Mailbox Recovery (SMBR), vous aurez besoin d'une licence supplémentaire pour SMBR qui doit être achetée séparément en fonction de la boîte aux lettres de l'utilisateur. NetApp® Single Mailbox Recovery est arrivé en fin de disponibilité (EOA) le 12 mai 2023. Pour plus d'informations, reportez-vous à"CPC-00507" . NetApp continuera à prendre en charge les clients qui ont acheté la capacité, la maintenance et le support de la boîte aux lettres via les numéros de référence marketing introduits le 24 juin 2020, pendant toute la durée du droit de support. NetApp Single Mailbox Recovery est un produit partenaire fourni par Ontrack. Ontrack PowerControls offre des fonctionnalités similaires à celles de NetApp Single Mailbox Recovery. Les clients peuvent se procurer de nouvelles licences logicielles Ontrack PowerControls et des renouvellements de maintenance et d'assistance Ontrack PowerControls auprès d'Ontrack (via licensingteam@ontrack.com) pour une récupération granulaire des boîtes aux lettres après la date EOA du 12 mai 2023.

Les licences SnapCenter Advanced et SnapCenter NAS File Services sont obsolètes et ne sont plus disponibles. La licence standard et la licence basée sur la capacité ne sont plus requises pour Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP et Azure NetApp Files.

Vous devez installer une ou plusieurs licences SnapCenter . Pour plus d'informations sur la façon d'ajouter des licences, voir"Ajouter des licences basées sur le contrôleur SnapCenter Standard" .

Synchronisation active SnapMirror dans SnapCenter

La synchronisation active SnapMirror permet aux services professionnels de continuer à fonctionner même en cas de panne totale du site, en prenant en charge le basculement transparent des applications à l'aide d'une copie secondaire. Aucune intervention manuelle ni script supplémentaire n'est requis pour déclencher un basculement avec la synchronisation active SnapMirror .

Pour plus d'informations sur SnapMirror Active Sync, reportez-vous à "Présentation de la synchronisation active de SnapMirror" .

Pour la synchronisation active de SnapMirror , assurez-vous d'avoir respecté les différentes exigences matérielles, logicielles et de configuration système. Pour plus d'informations, reportez-vous à "Prérequis"

Les plug-ins pris en charge pour cette fonctionnalité sont SnapCenter Plug-in pour SQL Server, SnapCenter Plug-in pour Windows, SnapCenter Plug-in pour la base de données Oracle, SnapCenter Plug-in pour la base de données SAP HANA, SnapCenter Plug-in pour Microsoft Exchange Server et SnapCenter Plug-in pour Unix.

Pour prendre en charge la proximité de l'initiateur hôte dans SnapCenter, sa valeur, la source ou la destination, doit être définie dans ONTAP.

Les cas d'utilisation non pris en charge dans SnapCenter:

- Si vous convertissez les charges de travail de synchronisation active SnapMirror asymétriques existantes en symétriques en modifiant la stratégie sur les relations de synchronisation active SnapMirror de *automatedfailover* à *automatedfailoverduplex* dans ONTAP, cette même stratégie n'est pas prise en charge dans SnapCenter.
- S'il existe des sauvegardes d'un groupe de ressources (déjà protégé dans SnapCenter) et que la politique de stockage est modifiée sur les relations de synchronisation active SnapMirror de *automatedfailover* à *automatedfailoverduplex* dans ONTAP, cette même opération n'est pas prise en charge dans SnapCenter.

Concepts clés de la protection des données

Avant d'utiliser SnapCenter, comprenez les concepts clés de la sauvegarde, du clonage et de la restauration.

Ressources

Les ressources incluent des bases de données, des systèmes de fichiers Windows ou des partages de fichiers sauvegardés ou clonés avec SnapCenter. Selon votre environnement, les ressources peuvent également être des instances de base de données, des groupes de disponibilité SQL Server, des bases de données Oracle, des bases de données RAC ou des groupes d'applications personnalisés.

Groupe de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte ou un cluster, provenant potentiellement de plusieurs hôtes et clusters. Les opérations effectuées sur un groupe de ressources s'appliquent à toutes ses ressources en fonction de la planification spécifiée. Vous pouvez effectuer des sauvegardes à la demande ou planifiées pour des ressources individuelles ou des groupes.

Si un hôte d'un groupe de ressources partagées entre en mode maintenance, toutes les opérations planifiées pour ce groupe seront suspendues sur tous les hôtes.

Utilisez des plug-ins pertinents pour sauvegarder des ressources spécifiques : plug-ins de base de données pour les bases de données, plug-ins de système de fichiers pour les systèmes de fichiers et SnapCenter Plug-in for VMware vSphere pour les machines virtuelles et les banques de données.

Politiques

Les politiques spécifient la fréquence de sauvegarde, la conservation des copies, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Une ou plusieurs politiques peuvent être sélectionnées lors de la création d'un groupe de ressources ou lors de l'exécution d'une sauvegarde à la demande.

Un groupe de ressources définit ce qui doit être protégé et quand cela doit être protégé en termes de jour et d'heure. Une politique décrit comment la protection sera mise en œuvre. Par exemple, si la sauvegarde de toutes les bases de données ou de tous les systèmes de fichiers d'un hôte est nécessaire, un groupe de ressources incluant toutes les bases de données ou tous les systèmes de fichiers de l'hôte peut être créé. Deux politiques pourraient alors être attachées au groupe de ressources : une politique quotidienne et une politique horaire.

Lors de la création du groupe de ressources et de l'association des politiques, il est possible de le configurer pour effectuer une sauvegarde complète quotidienne et une autre planification pour les sauvegardes de journaux toutes les heures.

Des prescripts et postscripts personnalisés peuvent être utilisés dans les opérations de protection des données. Ces scripts permettent l'automatisation avant ou après le travail de protection des données. Par exemple, un script pourrait automatiquement notifier les échecs ou les avertissements d'une tâche de protection des données. Il est essentiel de comprendre les exigences de création de ces scripts avant de configurer les prescripts et les postscripts.

Utilisation des prescripts et des postscripts

Les prescripts et postscripts personnalisés peuvent automatiser vos tâches de protection des données avant ou après le travail. Par exemple, vous pouvez ajouter un script pour vous avertir des échecs ou des avertissements de tâches. Avant de les configurer, assurez-vous de bien comprendre les exigences relatives à ces scripts.

Types de scripts pris en charge

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

- Fichiers batch
- Scripts PowerShell
- Scripts Perl

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

- Scripts Perl
- Scripts Python
- Scripts shell

> En plus du 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 préscripts et postscripts 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 être situés sur l'hôte du plug-in.

> Le chemin des prescripts ou des postscripts ne doit pas inclure de lecteurs ou de partages. Le chemin doit être relatif à SCRIPTS_PATH.

- Les scripts UNIX doivent être situés sur l'hôte du plug-in.

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

Où spécifier les scripts

Les scripts sont spécifiés dans les politiques de sauvegarde. Lorsqu'une tâche de sauvegarde démarre, la politique associe automatiquement le script aux ressources en cours de sauvegarde. Lorsque vous créez une politique de sauvegarde, vous pouvez spécifier les arguments prescript et postscript.

Vous ne pouvez pas spécifier plusieurs scripts.

Délais d'expiration des scripts

Le délai d'expiration est défini sur 60 secondes par défaut. Vous pouvez modifier la valeur du délai d'attente.

Sortie du script

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

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

Systèmes de stockage et applications pris en charge par SnapCenter

Vous devez connaître les systèmes de stockage, les applications et les bases de données pris en charge par SnapCenter.

Systèmes de stockage pris en charge

- NetApp ONTAP 9.12.1 et versions ultérieures
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Prend en charge la mémoire non volatile express (NVMe) via le protocole de contrôle de transport (TCP).

  Pour plus d'informations sur Amazon FSx for NetApp ONTAP, consultez "Documentation Amazon FSx for NetApp ONTAP" .

- Systèmes NetApp ASA r2 exécutant NetApp ONTAP 9.16.1.

Applications et bases de données prises en charge

SnapCenter prend en charge la protection de différentes applications et bases de données. Pour des informations détaillées sur les applications et bases de données prises en charge, consultez "Outil de matrice d'interopérabilité NetApp" .

SnapCenter prend en charge la protection des charges de travail Oracle et Microsoft SQL dans les environnements VMware Cloud on Amazon Web Services (AWS) Software-Defined Data Center (SDDC). "En

savoir plus" .

Méthodes d’authentification pour les informations d’identification SnapCenter

Les informations d’identification utilisent différentes méthodes d’authentification selon l’application ou l’environnement. Les informations d’identification authentifient les utilisateurs afin qu’ils puissent effectuer des opérations SnapCenter . Vous devez créer un ensemble d’informations d’identification pour l’installation des plug-ins et un autre pour les opérations de protection des données.

Authentification Windows

La méthode d’authentification Windows s’authentifie auprès d’Active Directory. Pour l’authentification Windows, Active Directory est configuré en dehors de SnapCenter. SnapCenter s’authentifie sans configuration supplémentaire. Vous avez besoin d’informations d’identification Windows pour ajouter des hôtes, installer des packages de plug-ins et planifier des tâches.

Authentification de domaine non fiable

SnapCenter permet aux utilisateurs et aux groupes appartenant à des domaines non approuvés de créer des informations d’identification Windows. Pour que l’authentification réussisse, vous devez enregistrer les domaines non approuvés auprès de SnapCenter.

Authentification du groupe de travail local

SnapCenter permet la création d’informations d’identification Windows avec des utilisateurs et des groupes de travail locaux. L’authentification Windows pour les utilisateurs et les groupes de travail locaux ne se produit pas lors de la création des informations d’identification Windows, mais est différée jusqu’à ce que l’enregistrement de l’hôte et d’autres opérations de l’hôte soient effectués.

Authentification SQL Server

La méthode d’authentification SQL s’authentifie auprès d’une instance SQL Server. Cela signifie qu’une instance SQL Server doit être découverte dans SnapCenter. Par conséquent, avant d’ajouter des informations d’identification SQL, vous devez ajouter un hôte, installer des packages de plug-in et actualiser les ressources. Vous avez besoin de l’authentification SQL Server pour effectuer des opérations telles que la planification sur SQL Server ou la découverte de ressources.

Authentification Linux

La méthode d’authentification Linux s’authentifie auprès d’un hôte Linux. Vous avez besoin d’une authentification Linux lors de l’étape initiale d’ajout de l’hôte Linux et d’installation du package de plug-ins SnapCenter pour Linux à distance à partir de l’interface graphique SnapCenter .

Authentification AIX

La méthode d’authentification AIX s’authentifie auprès d’un hôte AIX. Vous avez besoin d’une authentification AIX lors de l’étape initiale d’ajout de l’hôte AIX et d’installation du package de plug-ins SnapCenter pour AIX à distance à partir de l’interface graphique SnapCenter .

Authentification de la base de données Oracle

La méthode d'authentification de base de données Oracle s'authentifie auprès d'une base de données Oracle. Vous avez besoin d'une authentification de base de données Oracle pour effectuer des opérations sur la base de données Oracle si l'authentification du système d'exploitation (OS) est désactivée sur l'hôte de la base de données. Par conséquent, avant d'ajouter des informations d'identification de base de données Oracle, vous devez créer un utilisateur Oracle dans la base de données Oracle avec des privilèges sysdba.

Authentification Oracle ASM

La méthode d'authentification Oracle ASM s'authentifie auprès d'une instance Oracle Automatic Storage Management (ASM). L'authentification Oracle ASM est requise si vous devez accéder à une instance Oracle ASM et que l'authentification du système d'exploitation est désactivée sur l'hôte de la base de données. Avant d'ajouter des informations d'identification Oracle ASM, créez un utilisateur Oracle avec des privilèges système dans l'instance ASM.

Authentification du catalogue RMAN

La méthode d'authentification du catalogue RMAN s'authentifie auprès de la base de données du catalogue Oracle Recovery Manager (RMAN). Si vous avez configuré un mécanisme de catalogue externe et enregistré votre base de données dans la base de données du catalogue, vous devez ajouter l'authentification du catalogue RMAN.

Informations sur le copyright

Informations sur les marques commerciales