Commencez

SnapCenter software

NetApp
January 09, 2026

Sommaire

Commencez

En savoir plus sur les logiciels SnapCenter

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 :

- Des sauvegardes sur disque rapides, compactes et cohérentes au niveau des applications
- Restauration rapide et détaillée et récupération cohérente avec les applications
- Un clonage rapide et compact

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 :
  - 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
  - Les données qui se trouvent sur les systèmes principaux et secondaires ONTAP ASA r2
- Sur site dans un cloud hybride pour protéger les éléments suivants :
  - 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
  - Les données qui se trouvent sur un système Azure NetApp Files primaire (Oracle, Microsoft SQL et SAP HANA)

Fonctionnalités clés

SnapCenter offre les principales fonctionnalités suivantes :

- Protection des données centralisée et cohérente au niveau des applications de différentes applications

  La protection des données est prise en charge pour les bases de données Microsoft Exchange Server, Microsoft SQL Server, Oracle sous Linux ou AIX, SAP HANA Database, IBM DB2, PostgreSQL, MySQL et Windows Host Filesystem exécutées sur des systèmes ONTAP. SnapCenter prend également en charge la protection d'applications telles que MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Sauvegardes basées sur des règles

  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 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 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

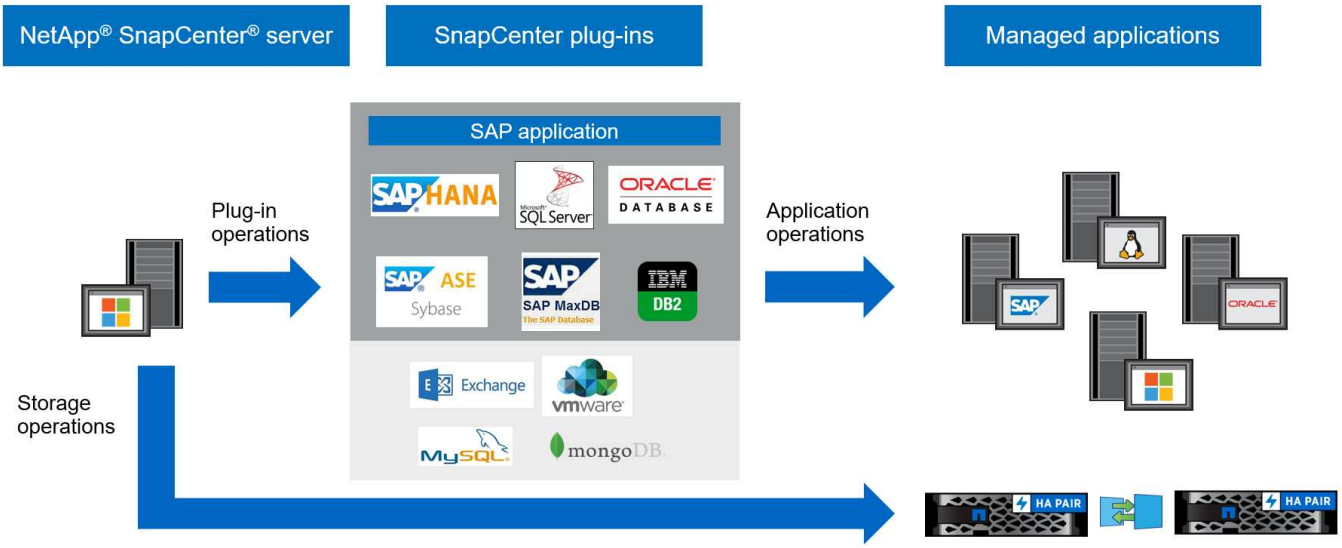
  SnapCenter fournit des API REST pour la plupart des fonctionnalités pour l'intégration avec n'importe quel logiciel d'orchestration et l'utilisation des cmdlets Windows PowerShell et de l'interface de ligne de commandes.

- 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
- Une base de données de référentiel intégrée haute disponibilité pour stocker toutes les métadonnées de sauvegarde
- Installation automatisée des plug-ins
- Haute disponibilité
- Reprise après incident
- SnapLock "En savoir plus"

- Synchronisation active SnapMirror (initialement lancée sous la forme SnapMirror Business Continuity [SM-BC])
- La 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 divers composants d'infrastructure et d'applications.

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 HTML5 centralisée, des applets de commande PowerShell, des API REST et le référentiel SnapCenter.

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

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 SnapCenter pour Microsoft SQL Server	Package de plug-ins pour Windows	Plug-in pour Windows	Hôte SQL Server	Répertoires de base
Plug-in SnapCenter pour Windows	Package de plug-ins pour Windows		Hôte Windows	Répertoires de base

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 SnapCenter pour Microsoft Exchange Server	Package de plug-ins pour Windows	Plug-in pour Windows	Hôte Exchange Server	Répertoires de base
Plug-in SnapCenter pour Oracle Database	Package de plug-ins pour Linux et package de plug-ins pour AIX	Plug-in pour UNIX	Hôte Oracle	Linux ou AIX
Plug-in SnapCenter pour base de données SAP HANA	Package de plug-ins pour Linux et package 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	Package de plug-ins pour Linux et package 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	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte PostgreSQL	Linux ou Windows
Plug-in SnaoCenter pour MySQL	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte MySQL	Linux ou Windows
Plug-in SnapCenter pour MongoDB	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte MongoDB	Linux ou Windows
Plug-in SnapCenter pour ORASCPM (applications Oracle)	Package de plug-ins pour Linux et package 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	Package de plug-ins pour Linux et package 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	Requiert d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour SAP MaxDB	Package de plug-ins pour Linux et package 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	Package de plug-ins pour Linux et package 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 plug-in SnapCenter pour 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 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 de SnapCenter

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).
- Prend en charge les algorithmes de sécurité conformes à la norme FIPS (Federal information Processing Standard).
- Prend en charge l'utilisation des certificats CA autorisés fournis par le client.
- Prend en charge TLS 1.3 (transport Layer Security) 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. "En savoir plus >>".
- 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.
- 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 des 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 dans SnapCenter

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

Vous devez créer ou modifier des rôles et ajouter un accès aux ressources aux utilisateurs. Lors de la configuration de SnapCenter pour la première fois, ajoutez des utilisateurs ou des groupes Active Directory aux rôles et attribuez des ressources à ces utilisateurs ou groupes.

SnapCenter ne crée pas de comptes d'utilisateur ou de groupe. Créez des comptes d'utilisateur ou de groupe dans l'Active Directory du système d'exploitation ou de la base de données.

Types de RBAC dans SnapCenter

SnapCenter prend en charge les types de contrôle d'accès basé sur les rôles suivants :

- RBAC SnapCenter
- RBAC au niveau des applications
- Plug-in SnapCenter pour VMware vSphere RBAC
- Autorisations ONTAP

RBAC SnapCenter

SnapCenter dispose de rôles prédéfinis et vous pouvez attribuer des utilisateurs ou des groupes à ces rôles.

- 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 attribuez un rôle à un utilisateur, SnapCenter affiche les tâches pertinentes pour cet utilisateur sur la page Tâches, sauf si l’utilisateur dispose du 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 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.

Lorsque vous créez un rôle personnalisé, assurez-vous qu’il inclut toutes les autorisations du rôle SnapCenterAdmin. Si vous copiez uniquement certaines autorisations, SnapCenter vous empêche d’effectuer toutes les opérations.

Les utilisateurs doivent s’authentifier lors de la connexion via l’interface utilisateur ou les applets de commande PowerShell. Si les utilisateurs ont plusieurs rôles, ils sélectionnent un rôle après s’être connectés. L’authentification est également requise pour exécuter les 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, pour effectuer des opérations de protection des données dans un environnement SQL Server, définissez les informations d’identification Windows ou SQL appropriées. 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 sur 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.

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 VMware prend en charge le RBAC vCenter Server et ONTAP RBAC. "En savoir plus"

REMARQUE : NetApp vous 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, attribuez soit l'autorisation StorageConnection pour activer la communication de la machine virtuelle de stockage (SVM), soit une SVM à l'utilisateur pour lui accorder l'autorisation d'utiliser la SVM. L'autorisation Connexion de stockage permet aux utilisateurs de créer des connexions SVM.

Par exemple, un administrateur SnapCenter peut créer des connexions SVM et les attribuer aux utilisateurs administrateurs de sauvegarde d'application et de clonage, qui ne peuvent pas créer ou modifier des connexions SVM. Sans connexion SVM, les utilisateurs ne peuvent pas effectuer d'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.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
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
Protection secondaire	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 Visionneuse 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	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

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
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
Protection secondaire	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.

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

Reprise après incident dans SnapCenter

La fonctionnalité de reprise après incident de SnapCenter vous permet de vous remettre en cas d'incidents tels que la corruption de ressources ou les pannes de serveur. Il permet de restaurer le référentiel SnapCenter, les planifications des serveurs, les composants de configuration, ainsi que le plug-in SnapCenter pour SQL Server et son stockage.

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 de SnapCenter sauvegarde le serveur SnapCenter à l'aide d'API REST. Voir "Workflows d'API REST pour la reprise après incident d'un serveur SnapCenter".
- Le fichier de configuration relatif 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 sur incident 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 "Reprise après incident du plug-in SnapCenter pour SQL Server".

SnapCenter utilise ONTAP SnapMirror pour répliquer les données qui peuvent être utilisées pour la reprise d'activité en synchronisant les données sur un site secondaire. Pour initier le basculement, interrompre la réplication SnapMirror. Pendant le retour arrière, inversez la synchronisation pour répliquer les données à partir du site de reprise sur incident 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 licence SnapCenter que vous installez dépend de votre environnement de stockage et des fonctionnalités que vous souhaitez utiliser.

Licence	Si nécessaire
Contrôleur SnapCenter standard	Requis pour FAS, AFF, ASA La licence standard SnapCenter est basée sur le contrôleur et est incluse dans NetApp ONTAP One. Si vous disposez de la licence SnapManager Suite, vous bénéficiez également des droits de licence SnapCenter Standard. Si vous souhaitez installer SnapCenter en version d'essai avec un système de stockage FAS, AFF ou ASA, vous pouvez obtenir une licence d'évaluation NetApp ONTAP One en contactant l'ingénieur commercial. Pour plus d'informations sur les licences incluses avec NetApp ONTAP One, reportez-vous à la section "Licences incluses avec NetApp ONTAP One". SnapCenter fait également partie du pack de protection des données. Si vous avez acheté 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	Indispensable pour restaurer et vérifier les sauvegardes. Sur les systèmes de stockage primaires • Indispensable sur les systèmes de destination SnapVault pour effectuer une vérification à distance et une restauration à partir d'une sauvegarde. • Nécessaire sur les systèmes de destination SnapMirror pour effectuer une vérification à distance.

Licence	Si nécessaire
FlexClone	Requises pour cloner les bases de données et les 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 secondaire à distance. • Requis sur les systèmes de destination SnapMirror pour créer des clones à partir d'une sauvegarde SnapMirror secondaire
Licences de protocoles	• Licence iSCSI ou FC pour LUN • Licence CIFS pour les partages SMB • Licence NFS pour VMDK de type NFS • Licence iSCSI ou FC pour les VMDK de type VMFS Indispensable sur les systèmes de destination SnapMirror pour transmettre les données en cas d'indisponibilité d'un volume source.
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. Une licence FlexClone est toutefois requise sur les destinations secondaires pour effectuer les opérations de clonage et de vérification.

Licence	Si nécessaire
Licences Single Mailbox Recovery (SMBR)	Si vous utilisez le plug-in SnapCenter pour Exchange pour gérer les bases de données Microsoft Exchange Server et SMBR (Single Mailbox Recovery), vous devez disposer d'une licence supplémentaire pour SMBR qui doit être achetée séparément selon la boîte aux lettres des utilisateurs. NetApp® Single Mailbox Recovery a pris fin le 12 mai 2023. Pour plus d'informations, reportez-vous à la section "CPC-00507". NetApp continuera d'assurer le support des clients ayant acheté une capacité de boîte aux lettres, des services de maintenance et un support via des références marketing introduites le 24 juin 2020, pendant la durée du support souscrit. 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 de support Ontrack PowerControls auprès d'Ontrack (jusqu'à licensingteam@ontrack.com) pour une récupération granulaire des boîtes aux lettres après la date de fin de disponibilité 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 nécessaires 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 l'ajout de licences, reportez-vous à la section "Ajout de licences SnapCenter standard basées sur le contrôleur".

Synchronisation active SnapMirror dans SnapCenter

La synchronisation active SnapMirror assure la continuité des services, même en cas de défaillance complète d'un site. Les applications peuvent ainsi basculer en toute transparence au moyen d'une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

Pour plus d'informations sur la synchronisation active SnapMirror, reportez-vous àla section "Présentation de la synchronisation active SnapMirror".

Pour la synchronisation active SnapMirror, assurez-vous que vous répondez aux différentes exigences en matière de matériel, de logiciels et de configuration du système. Pour plus d'informations, reportez-vous à "Prérequis"

Les plug-ins pris en charge pour cette fonctionnalité sont le plug-in SnapCenter pour SQL Server, le plug-in SnapCenter pour Windows, le plug-in SnapCenter pour Oracle Database, le plug-in SnapCenter pour SAP HANA, le plug-in SnapCenter pour Microsoft Exchange Server et le plug-in SnapCenter pour Unix.

Après avoir installé SnapCenter Server et les plug-ins, vous devez activer l'API REST pour SnapCenter afin de détecter les relations de synchronisation actives de SnapMirror .

- Sur l'hôte du serveur SnapCenter , modifiez le fichier *C:\Program Files\ NetApp\SMCore\SMCoreServiceHost.dll.config* pour modifier la valeur du paramètre *IsRestEnabledForStorageConnection* sur *true*, puis redémarrez le service SnapCenter SMCore.
- Sur les hôtes du plug-in Windows :
  - Modifiez le fichier *C:\Program Files\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config* pour modifier la valeur du paramètre *IsRestEnabledForStorageConnection* sur *true*.
  - Modifiez le fichier *C:\Program Files\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config* pour modifier la valeur du paramètre *IsRestEnabledForStorageConnection* sur *true*.
  - Redémarrez le service SnapCenter SMCore.

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

Cas d'utilisation non pris en charge par SnapCenter :

- Si vous convertissez les charges de travail de synchronisation active SnapMirror asymétriques en charges de travail symétriques en modifiant la règle sur les relations de synchronisation active SnapMirror de *automatedfailover* à *automatefailoverduplex* dans ONTAP, cette règle n'est pas prise en charge dans SnapCenter.
- En cas de sauvegardes d'un groupe de ressources (déjà protégé dans SnapCenter), puis de modification de la règle de stockage sur les relations de synchronisation active SnapMirror entre *automatedfailover* et *failetedoverduplex* dans ONTAP, cette règle n'est pas prise en charge dans SnapCenter.

Concepts clés de la protection des données

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

Ressources

Les ressources comprennent les bases de données, les systèmes de fichiers Windows ou les 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, potentiellement provenant 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 ou des groupes individuels.

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

Utilisez les plug-ins appropriés pour sauvegarder des ressources spécifiques : plug-ins de base de données pour bases de données, plug-ins de système de fichiers pour systèmes de fichiers et plug-in SnapCenter pour VMware vSphere pour les VM et les datastores.

Stratégies

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

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

Un groupe de ressources définit ce qui doit être protégé et quand il doit être protégé en termes de jour et d'heure. Une politique décrit comment la protection sera effectuée. 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 comprenant toutes les bases de données ou tous les systèmes de fichiers de l'hôte peut être créé. Deux politiques pourraient alors être associées au groupe de ressources : une politique quotidienne et une politique horaire.

Lors de la création du groupe de ressources et de l'association des stratégies, 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 prescripteurs et des scripts d'appel 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 peut automatiquement signaler les échecs ou les avertissements de la tâche de protection des données. Il est essentiel de comprendre les exigences de création de ces scripts avant de configurer des prescripteurs et des scripts d'exécution.

Groupe de cohérence (CG)

Un groupe de cohérence est un ensemble de volumes gérés comme une seule unité. Les CG sont synchronisés pour assurer la cohérence des données entre les unités de stockage et les volumes. Dans ONTAP, ils offrent une gestion facile et une garantie de protection pour une charge de travail applicative couvrant plusieurs volumes. En savoir plus sur "groupes de cohérence" .

Utilisation des prescripteurs et des postscripts

Les prescripteurs personnalisés et les postscripts peuvent automatiser vos tâches de protection des données avant ou après le travail. Par exemple, vous pouvez ajouter un script pour vous informer des échecs de travaux ou des avertissements. Avant de les configurer, assurez-vous de bien comprendre les exigences 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 prescripteurs et scripts postscripts exécutés dans le cadre des opérations SnapCenter sur les systèmes de stockage non virtualisés et 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 démarre, 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.

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 pour NetApp ONTAP

Amazon FSx for NetApp ONTAP prend en charge la mémoire non volatile express (NVMe) via le protocole TCP (Transport Control Protocol).

Pour plus d'informations sur Amazon FSX pour NetApp ONTAP, consultez "Documentation Amazon FSX pour NetApp ONTAP".

- Systèmes NetApp ASA r2 exécutant NetApp ONTAP 9.16.1 et versions ultérieures

  Vous devez utiliser ONTAP 9.17.1 si vous utilisez SnapCenter Server 6.2 et les plug-ins SnapCenter 6.2.

Applications et bases de données prises en charge

SnapCenter prend en charge la protection de différentes applications et bases de données.

SnapCenter prend en charge la protection des charges de travail Oracle et Microsoft SQL dans le cloud VMware sur les environnements SDDC (Software-Defined Data Center) Amazon Web Services (AWS). "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 pour qu'ils puissent exécuter 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. L'authentification SnapCenter s'effectue sans configuration supplémentaire. Vous avez besoin d'informations d'identification Windows pour ajouter des hôtes, installer des modules de plug-in et planifier des travaux.

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 avec SnapCenter.

Authentification locale du groupe de travail

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

Authentification SQL Server

La méthode d'authentification SQL s'authentifie par rapport à une instance SQL Server. Cela signifie qu'une instance SQL Server doit être découverte dans SnapCenter. Par conséquent, avant d'ajouter un identifiant SQL, vous devez ajouter un hôte, installer des modules 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 par rapport à un hôte Linux. Vous avez besoin d'une authentification Linux au cours de la première étape de l'ajout de l'hôte Linux et de l'installation du module SnapCenter Plug-ins Package 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. L'authentification AIX doit être effectuée lors de l'étape initiale de l'ajout de l'hôte AIX et de l'installation du module plug-ins SnapCenter pour AIX à distance à partir de l'interface utilisateur graphique SnapCenter.

Authentification de la base de données Oracle

La méthode d'authentification de la base de données Oracle s'authentifie par rapport à une base de données Oracle. Une authentification de base de données Oracle est nécessaire pour effectuer des opérations sur la base de données Oracle si l'authentification du système d'exploitation 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 sysdba Privileges.

Authentification Oracle ASM

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

Authentification du catalogue RMAN

La méthode d'authentification du catalogue RMAN s'authentifie par rapport à 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 de catalogue, vous devez ajouter l'authentification de catalogue RMAN.

Opérations SnapCenter prises en charge pour les systèmes ASA r2

Les systèmes de stockage ASA r2 sont pris en charge à partir de SnapCenter 6.1. "En savoir plus sur les systèmes ASA r2" .

SnapCenter prend en charge la protection primaire et secondaire des applications exécutées sur des systèmes physiques et sur des systèmes de fichiers de machines virtuelles (VMFS). SnapCenter utilise les API REST pour toutes les opérations sur les systèmes ASA r2. Les systèmes ASA r2 ne prennent pas en charge les ZAPI.

Opérations prises en charge par SnapCenter pour les systèmes ASA r2

- Création de sauvegardes primaires d'applications
- Déplacement des instantanés de groupe de cohérence hiérarchique vers un système de stockage secondaire
- Restauration des sauvegardes des systèmes de stockage principal et secondaire vers l'hôte d'origine ou

alternatif

- Restauration sur place à partir des systèmes de stockage principaux et secondaires à l'aide de VMware vMotion
- Connectez et copiez la restauration à partir des systèmes de stockage principal et secondaire

- Clonage des sauvegardes sur l'hôte d'origine ou sur l'hôte alternatif
- RDM (Raw Device Mapping)
- Protection des volumes d'application pour Oracle
- Protection de SAP HANA NDV
- LockVault
- Provisionnement secondaire du répertoire de journaux de l'hôte du plug-in SQL

SnapCenter découvre ou crée des groupes de cohérence ONTAP . Il configure les relations SnapMirror sur le cluster de destination pour une protection secondaire. "En savoir plus sur les groupes de cohérence ONTAP" .

> Après la mise à niveau vers SnapCenter 6.2 (serveur et plug-ins) et ONTAP 9.17.1, SnapCenter modifie les groupes de cohérence plats en groupes de cohérence hiérarchiques lors de la première sauvegarde planifiée.

Pour savoir comment activer la protection secondaire sur les systèmes ASA r2 pour votre application, consultez :

- "Activer la protection secondaire pour les ressources Microsoft SQL Server"
- "Activer la protection secondaire pour les ressources SAP HANA"
- "Activer la protection secondaire pour les ressources Oracle"
- "Activer la protection secondaire pour les systèmes de fichiers Windows"
- "Activer la protection secondaire pour les ressources IBM Db2"
- "Activer la protection secondaire pour les ressources PostgreSQL"
- "Activer la protection secondaire pour les ressources MySQL"
- "Activer la protection secondaire pour les systèmes de fichiers Unix"

Opérations non prises en charge par SnapCenter pour les systèmes ASA r2

- Des snapshots inviolables
- Volumes FlexGroup
- Migration des systèmes de stockage ASA, AFF ou FAS vers les systèmes de stockage ASA r2
- Protection des bases de données avec un mélange de ressources ASA, AFF ou FAS et de ressources ASA r2
- Modification du nom des snapshots
- Provisionnement des ressources Windows
- Protection secondaire en cas de basculement de synchronisation active SnapMirror
- Protocole NVMe (Nonvolatile Memory Express) si SnapMirror Active Sync est activé
- Protection des applications exécutées sur AIX
- Mise à jour technologique

- Récupération après sinistre des ressources Microsoft SQL

Démarrage rapide du logiciel SnapCenter

Le guide de démarrage rapide décrit les étapes de base pour installer et configurer le logiciel SnapCenter.

1 Préparation de l'installation du serveur SnapCenter

Vous devez vous assurer que toutes les conditions requises pour installer le serveur SnapCenter sont remplies.

- "De formation"
- "Inscrivez-vous pour accéder au logiciel SnapCenter"
- "Activez l'authentification multifacteur"

2 Installez le serveur SnapCenter

Le serveur SnapCenter peut être installé sur des hôtes Windows ou Linux. Téléchargez le package d'installation du serveur SnapCenter à partir du "Site de support NetApp" et exécutez le programme d'installation.

- "Installez SnapCenter Server sous Windows"
- "Installez SnapCenter Server sous Linux"

3 Configurer le serveur SnapCenter

Après avoir installé le serveur SnapCenter, vous devez le configurer en fonction de votre environnement.

4 Installez le plug-in pour votre application

Assurez-vous que toutes les conditions d'installation du plug-in spécifique à l'application sont remplies en fonction de l'application utilisée, puis procédez à l'installation du plug-in correspondant.

5 Protégez votre application

Après avoir installé le serveur SnapCenter et les plug-ins nécessaires, vous pouvez lancer la création de sauvegardes d'applications. Ces sauvegardes peuvent ensuite être utilisées à des fins de restauration et de clonage lorsque cela est nécessaire.

Informations sur le copyright

Informations sur les marques commerciales