Commencer

NetApp Backup and Recovery

NetApp
February 11, 2026

Sommaire

Commencer

En savoir plus sur NetApp Backup and Recovery

NetApp Backup and Recovery est un service de données qui fournit une protection des données efficace, sécurisée et rentable pour toutes vos charges de travail ONTAP , y compris les volumes, les bases de données, les machines virtuelles et les charges de travail Kubernetes.

La prise en charge de la sauvegarde et de la récupération est déjà intégrée à tous les systèmes ONTAP , il n'est donc pas nécessaire de recourir à du matériel supplémentaire, à des licences logicielles ou à des passerelles multimédias. Cela rend les opérations de sauvegarde simples et rentables. La NetApp Console simplifie la mise en œuvre de toute stratégie de sauvegarde, y compris toute la gamme des variantes de sauvegarde 3-2-1, sans nécessiter plusieurs gestionnaires de ressources ou du personnel spécialisé.

> La documentation sur la protection des charges de travail VMware, KVM, Hyper-V et Kubernetes est fournie sous forme d'aperçu technologique. Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Ce que vous pouvez faire avec NetApp Backup and Recovery

Utilisez NetApp Backup and Recovery pour atteindre les objectifs suivants :

- * Charges de travail de volume ONTAP * :
  - Créez des instantanés locaux, répliquez-les vers un stockage secondaire et sauvegardez les volumes ONTAP à partir des systèmes ONTAP locaux ou Cloud Volumes ONTAP vers le stockage d'objets dans votre compte cloud public ou privé.
  - Créez des sauvegardes incrémentielles permanentes au niveau des blocs qui sont stockées sur un autre cluster ONTAP et dans un stockage d'objets dans le cloud.
  - Utilisez NetApp Backup and Recovery avec SnapCenter.
  - Se référer à"Protéger les volumes ONTAP" .
- **Charges de travail Microsoft SQL Server**:
  - Sauvegardez les instances et bases de données Microsoft SQL Server à partir ONTAP sur site, de Cloud Volumes ONTAP ou Amazon FSx for NetApp ONTAP.
  - Restaurer les bases de données Microsoft SQL Server.
  - Cloner des bases de données Microsoft SQL Server.
  - Utilisez NetApp Backup and Recovery sans SnapCenter.
  - Se référer à"Protégez les charges de travail Microsoft SQL Server" .
- **Charges de travail VMware (Aperçu avec nouvelle interface utilisateur sans SnapCenter Plug-in for VMware vSphere)**:
  - Protégez vos machines virtuelles et banques de données VMware avec NetApp Backup and Recovery.
  - Sauvegardez les charges de travail VMware sur Amazon Web Services S3 ou StorageGRID (pour l'aperçu).
  - Restaurez les données VMware du cloud vers le vCenter local.

- Vous pouvez restaurer la machine virtuelle exactement au même emplacement à partir duquel la sauvegarde a été effectuée ou vers un autre emplacement.
- Utilisez NetApp Backup and Recovery sans SnapCenter Plug-in for VMware vSphere.
- Se référer à"Protégez les charges de travail VMware" .

- **Charges de travail VMware (avec SnapCenter Plug-in for VMware vSphere)** :
  - Sauvegardez les machines virtuelles et les banques de données sur Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform et StorageGRID et restaurez les machines virtuelles sur l'hôte SnapCenter Plug-in for VMware vSphere sur site.
  - Restaurez les données de la machine virtuelle depuis le cloud vers le vCenter local avec NetApp Backup and Recovery. Vous pouvez restaurer la machine virtuelle exactement au même emplacement à partir duquel la sauvegarde a été effectuée ou vers un autre emplacement.
  - Utilisez NetApp Backup and Recovery avec le SnapCenter Plug-in for VMware vSphere.
  - Se référer à"Protégez les charges de travail VMware" .
- **Charges de travail KVM (Aperçu)**:
  - Sauvegarder et restaurer des machines virtuelles
  - Sauvegarder les pools de stockage KVM
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Se référer à"Protégez les charges de travail KVM" .
- **Charges de travail Hyper-V (Aperçu)**:
  - Sauvegarder et restaurer des machines virtuelles
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Se référer à"Protégez les charges de travail Hyper-V" .
- **Charges de travail Oracle Database (Preview)**:
  - Sauvegarder et restaurer les bases de données et les journaux
  - Utiliser des groupes de protection pour gérer les tâches de sauvegarde
  - Créer des politiques pour gérer les sauvegardes de bases de données et de journaux
  - Protéger une base de données avec une architecture de sauvegarde 3-2-1
  - Configurer la conservation des sauvegardes
  - Monter et démonter les sauvegardes ARCHIVELOG
  - Se référer à "Protégez les charges de travail Oracle Database".
- **Charges de travail Kubernetes (Aperçu)**:
  - Gérez et protégez vos applications et ressources Kubernetes en un seul endroit.
  - Utilisez des politiques de protection pour structurer vos sauvegardes incrémentielles.
  - Restaurez les applications et les ressources sur les mêmes clusters et espaces de noms ou sur des clusters et espaces de noms différents.
  - Utilisez NetApp Backup and Recovery sans SnapCenter.
  - Se référer à"Protégez les charges de travail Kubernetes" .

Avantages de l'utilisation de NetApp Backup and Recovery

NetApp Backup and Recovery offre les avantages suivants :

- **Efficace** : NetApp Backup and Recovery effectue une réplication incrémentielle permanente au niveau des blocs, ce qui réduit considérablement la quantité de données répliquées et stockées. Cela permet de minimiser le trafic réseau et les coûts de stockage.
- **Sécurisé** : NetApp Backup and Recovery crypte les données en transit et au repos, et utilise des protocoles de communication sécurisés pour protéger vos données.
- **Rentable** : NetApp Backup and Recovery utilise les niveaux de stockage les moins chers disponibles dans votre compte cloud, ce qui contribue à réduire les coûts.
- **Automatisé** : NetApp Backup and Recovery génère automatiquement des sauvegardes selon une planification prédéfinie, ce qui contribue à garantir la protection de vos données.
- **Flexible** : NetApp Backup and Recovery vous permet de restaurer des données sur le même système ou sur un système différent, ce qui offre une flexibilité dans la récupération des données.

Coût

NetApp ne vous facture pas l'utilisation de la version d'essai. Cependant, vous êtes responsable des coûts associés aux ressources cloud que vous utilisez, tels que les coûts de stockage et de transfert de données.

Il existe deux types de coûts associés à l'utilisation de la fonctionnalité de sauvegarde sur objet de NetApp Backup and Recovery avec les systèmes ONTAP :

- Frais de ressources
- Frais de service

La création d'instantanés ou de volumes répliqués est gratuite, hormis l'espace disque nécessaire à leur stockage.

Frais de ressources

Des frais de ressources sont payés au fournisseur de cloud pour la capacité de stockage d'objets et pour l'écriture et la lecture de fichiers de sauvegarde dans le cloud.

- Pour la sauvegarde sur un stockage d'objets, vous payez votre fournisseur de cloud pour les coûts de stockage d'objets.

  Étant donné que NetApp Backup and Recovery préserve l'efficacité du stockage du volume source, vous payez au fournisseur de cloud les coûts de stockage d'objets pour les données *après* l'efficacité ONTAP (pour la plus petite quantité de données après l'application de la déduplication et de la compression).

- Pour restaurer des données à l'aide de la recherche et de la restauration, certaines ressources sont provisionnées par votre fournisseur de cloud et un coût par Tio est associé à la quantité de données analysées par vos demandes de recherche. (Ces ressources ne sont pas nécessaires pour parcourir et restaurer.)
  - Dans AWS, "Amazone Athéna" et "Colle AWS" les ressources sont déployées dans un nouveau bucket S3.
  - Dans Azure, un "Espace de travail Azure Synapse" et "Stockage Azure Data Lake" sont provisionnés dans votre compte de stockage pour stocker et analyser vos données.
  - Dans Google, un nouveau bucket est déployé et le "Services Google Cloud BigQuery" sont

provisionnés au niveau du compte/projet.

- Si vous prévoyez de restaurer des données de volume à partir d'un fichier de sauvegarde qui a été déplacé vers un stockage d'objets d'archivage, des frais de récupération par Gio et des frais par demande supplémentaires sont facturés par le fournisseur de cloud.
- Si vous prévoyez d'analyser un fichier de sauvegarde à la recherche de ransomwares pendant le processus de restauration des données du volume (si vous avez activé DataLock et Ransomware Resilience pour vos sauvegardes cloud), vous devrez également supporter des frais de sortie supplémentaires auprès de votre fournisseur cloud.

Frais de service

Pour les charges de travail de volume ONTAP , vous n'êtes facturé que pour les volumes protégés sur le stockage objet. Les frais sont basés sur la capacité logique utilisée des volumes ONTAP source avant application des gains d'efficacité, également appelée téraoctets frontaux (FETB).

Pour les charges de travail Kubernetes, vous êtes facturé en fonction de la taille combinée de tous les volumes persistants.

Pour toutes les autres charges de travail, la facturation porte sur les ressources protégées sur au moins une cible de stockage secondaire ou objet. Les frais sont calculés en fonction de la taille logique de la charge de travail source. Pour les bases de données, cela correspond à la taille de la base de données ; pour les machines virtuelles, à la taille de la machine virtuelle.

Il existe trois façons de payer pour la sauvegarde et la restauration :

- La première option est de vous abonner auprès de votre fournisseur cloud, ce qui vous permet de payer par mois.
- La deuxième option consiste à souscrire un contrat annuel.
- La troisième option consiste à acheter des licences directement auprès de NetApp. Se référer à Licences section pour plus de détails.

Licences

NetApp Backup and Recovery propose un essai gratuit, vous permettant de l'utiliser sans clé de licence pendant une durée limitée.

Une licence de sauvegarde est uniquement requise pour les opérations de sauvegarde et de restauration impliquant le stockage d'objets. La création d'instantanés et de volumes répliqués ne nécessite pas de licence.

Vous pouvez choisir parmi trois options de licence :

- **Apportez votre propre licence (BYOL)** : Achetez une licence à durée déterminée (1, 2 ou 3 ans) et à capacité déterminée (par incréments de 1 Tio) auprès de NetApp. Saisissez le numéro de série fourni dans la NetApp Console pour activer le produit. La licence couvre tous les systèmes sources de votre organisation. Le renouvellement est requis lorsque la durée ou la limite de capacité est atteinte.
- **Paiement à l'utilisation (PAYGO)** : Abonnez-vous via la place de marché de votre fournisseur de cloud et payez par GiB de données sauvegardées, facturé mensuellement. Aucun paiement initial n'est requis. Un essai gratuit de 30 jours est disponible lors de votre première inscription. Pour plus d'informations, reportez-vous à "utiliser un abonnement NetApp Backup and Recovery PAYGO" .
- **Contrat annuel** : Disponible via les places de marché AWS et Azure pour 1, 2 ou 3 ans. Deux contrats annuels sont disponibles :

- **Sauvegarde dans le cloud** : Sauvegarde les données Cloud Volumes ONTAP et les données ONTAP sur site.
- **CVO Professional** : Regroupe Cloud Volumes ONTAP et NetApp Backup and Recovery, avec des sauvegardes illimitées pour les volumes Cloud Volumes ONTAP (la capacité de sauvegarde n'est pas décomptée de la licence).
  - Avec le forfait CVO Professional, il existe deux types de frais :
    - **Frais de ressources** : Basés sur l'utilisation du stockage. Pour plus d'informations, reportez-vous à "Licence pour Cloud Volumes ONTAP" .
    - **Frais de service** : Frais de NetApp Backup and Recovery. Toutefois, si le volume source se trouve dans un système de stockage utilisant le plan CVO Professional, NetApp Backup and Recovery est fourni gratuitement.

Lorsque vous utilisez Google Cloud Platform, demandez une offre privée à NetApp et sélectionnez votre forfait lors de l'activation sur Google Cloud Marketplace.

"Apprenez à configurer des licences".

Charges de travail, systèmes et cibles de sauvegarde pris en charge

Charges de travail prises en charge

NetApp Backup and Recovery protège les types de charges de travail suivants :

- Volumes ONTAP
- Instances et bases de données Microsoft SQL Server stockées sur disque physique et sur disque de machine virtuelle VMware (VMDK) via VMFS ou NFS
- Machines virtuelles et banques de données VMware
- Charges de travail KVM (Aperçu)
- Charges de travail Hyper-V (Aperçu)
- Charges de travail de base de données Oracle (Aperçu)
- Charges de travail Kubernetes (Aperçu)

Systèmes pris en charge

- SAN ONTAP sur site (protocole iSCSI) et NAS (utilisant les protocoles NFS et CIFS) avec ONTAP version 9.8 ou supérieure
- Cloud Volumes ONTAP 9.8 ou supérieur pour AWS (utilisant SAN et NAS)
- Cloud Volumes ONTAP 9.8 ou supérieur pour Google Cloud Platform (utilisant les protocoles NFS et CIFS)
- Cloud Volumes ONTAP 9.8 ou supérieur pour Microsoft Azure (utilisant SAN et NAS)
- Amazon FSx for NetApp ONTAP (charges de travail Microsoft SQL Server uniquement)

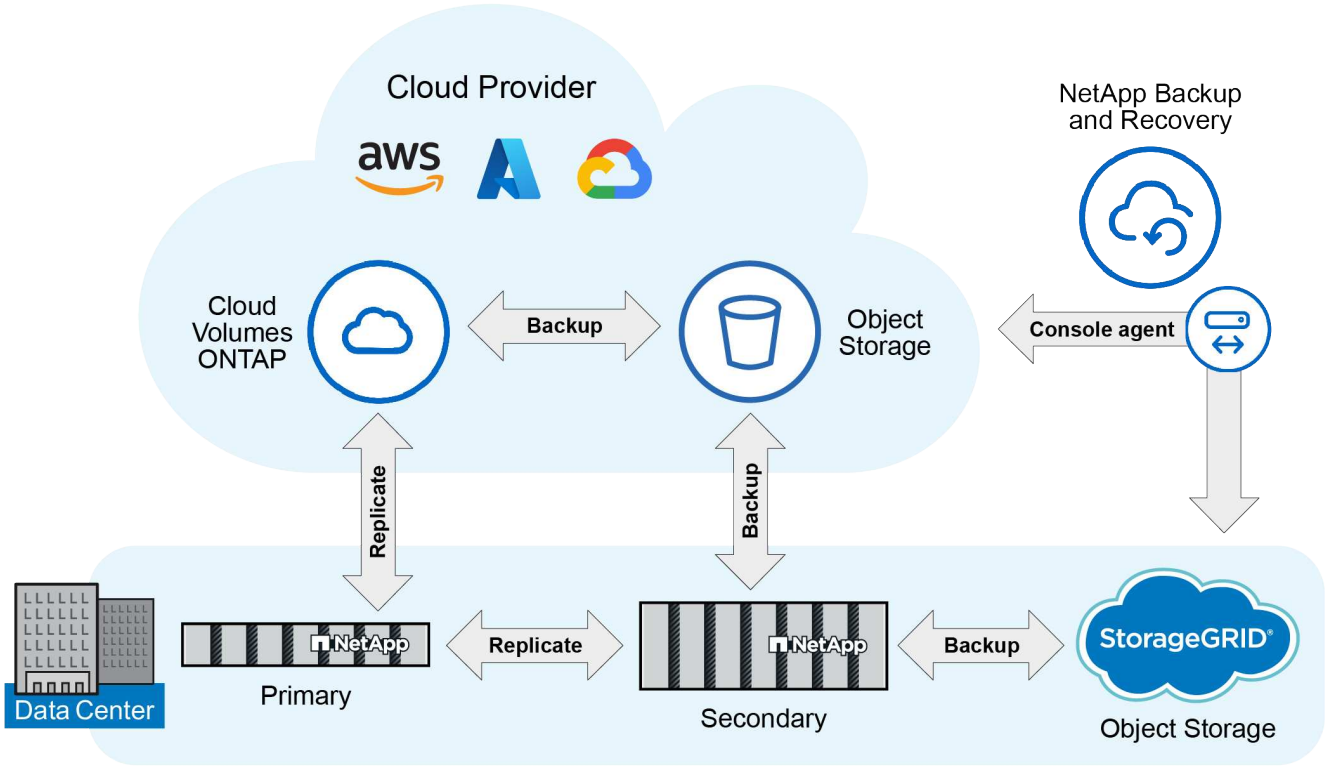
Cibles de sauvegarde prises en charge

- Amazon Web Services (AWS) S3
- Stockage Google Cloud
- Microsoft Azure Blob (non disponible pour les charges de travail VMware en version préliminaire)
- StorageGRID
- ONTAP S3 (non disponible pour les charges de travail VMware en version préliminaire)

Comment fonctionne la NetApp Backup and Recovery

Lorsque vous activez NetApp Backup and Recovery, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles. Cela permet de maintenir le trafic réseau à un minimum.

L'image suivante montre la relation entre les composants.



Le stockage primaire vers le stockage d'objets est également pris en charge, et pas seulement du stockage secondaire vers le stockage d'objets.

Où résident les sauvegardes dans les emplacements de stockage d'objets

Les copies de sauvegarde sont stockées dans un magasin d'objets que la NetApp Console crée dans votre compte cloud. Il existe un magasin d'objets par cluster ou système, et la console nomme le magasin d'objets comme suit : `netapp-backup-clusteruuid` . Assurez-vous de ne pas supprimer ce magasin d'objets.

- Dans AWS, la NetApp Console permet "Fonctionnalité d'accès public au bloc Amazon S3" sur le bucket S3.
- Dans Azure, la NetApp Console utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob. "bloque l'accès public à vos données blob" par défaut.
- Dans StorageGRID, la console utilise un compte de stockage existant pour le bucket de magasin d'objets.
- Dans ONTAP S3, la console utilise un compte utilisateur existant pour le bucket S3.

Les copies de sauvegarde sont associées à votre organisation NetApp Console

Les copies de sauvegarde sont associées à l'organisation de la NetApp Console dans laquelle réside l'agent

de la console. "En savoir plus sur l'identité et l'accès à la NetApp Console" .

Si vous disposez de plusieurs agents de console dans la même organisation de NetApp Console , chaque agent de console affiche la même liste de sauvegardes.

Termes qui pourraient vous aider avec NetApp Backup and Recovery

Il pourrait être utile de comprendre certains termes liés à la protection.

- **Protection** : La protection dans NetApp Backup and Recovery signifie garantir que les snapshots et les sauvegardes immuables se produisent régulièrement dans un domaine de sécurité différent à l'aide de politiques de protection.
- **Charge de travail** : une charge de travail dans NetApp Backup and Recovery peut inclure des volumes ONTAP , des instances et des bases de données Microsoft SQL Server ; des machines virtuelles et des banques de données VMware ; ou des clusters et des applications Kubernetes.

Conditions préalables à la NetApp Backup and Recovery

Commencez à utiliser NetApp Backup and Recovery en vérifiant l'état de préparation de votre environnement opérationnel, de l'agent NetApp Console et du compte NetApp Console . Pour utiliser NetApp Backup and Recovery, vous aurez besoin de ces prérequis.

Prérequis pour ONTAP 9.8 et versions ultérieures

Une licence ONTAP One doit être activée sur l'instance ONTAP locale.

Conditions préalables pour les sauvegardes sur le stockage d'objets

Pour utiliser le stockage d'objets comme cibles de sauvegarde, vous avez besoin d'un compte avec AWS S3, Microsoft Azure Blob, StorageGRID ou ONTAP et des autorisations d'accès appropriées configurées.

- "Protégez vos données de volume ONTAP"

Exigences pour la protection des charges de travail Microsoft SQL Server

Pour utiliser NetApp Backup and Recovery pour les charges de travail Microsoft SQL Server, vous avez besoin des prérequis suivants en matière de système hôte, d'espace et de dimensionnement.

Article	Exigences
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .
Versions de Microsoft SQL Server	Les versions 2012 et ultérieures sont prises en charge pour VMware Virtual Machine File System (VMFS) et VMware Virtual Machine Disk (VMDK) NFS.

Article	Exigences
Version du serveur SnapCenter	La version 5.0 ou supérieure de SnapCenter Server est requise si vous souhaitez importer vos données existantes de SnapCenter dans NetApp Backup and Recovery. Si vous disposez déjà de SnapCenter, vérifiez d'abord que vous avez rempli les conditions préalables avant d'importer depuis SnapCenter. Voir"Conditions préalables à l'importation de ressources depuis SnapCenter" .
RAM minimale pour le plug-in sur l'hôte SQL Server	1 Go
Espace minimum d'installation et de journalisation pour le plug-in sur l'hôte SQL Server	5 Go Allouez suffisamment d'espace disque et surveillez la consommation de stockage par le dossier des journaux. L'espace journal requis varie en fonction du nombre de sauvegardes effectuées et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace, les journaux ne seront pas créés pour les opérations.
Logiciels requis	• Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) • PowerShell 7.4.2 Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

Exigences pour la protection des charges de travail VMware

Vous avez besoin d'exigences spécifiques pour découvrir et protéger vos charges de travail VMware.

Support logiciel

- Les datastores NFS et VMFS sont pris en charge.
- Versions NFS prises en charge : NFS 3 et NFS 4.1
- Versions de VMware ESXi Server prises en charge : 7.0U1 et versions ultérieures
- Versions VMware vCenter vSphere prises en charge : 7.0U1 et supérieures
- Adresses IP : IPv4 et IPv6
- VMware TLS : 1.2, 1.3
- Stockage connecté pris en charge : ONTAP 9.13 ou version ultérieure

Exigences de connexion et de port pour la protection des charges de travail VMware

Type de port	Port préconfiguré
Port du serveur VMware ESXi	443 (HTTPS), bidirectionnel. La fonction de restauration de fichiers invités utilise ce port.
Cluster de stockage ou port de VM de stockage	443 (HTTPS), bidirectionnel. 80 (HTTP), bidirectionnel. Ce port est utilisé pour la communication entre l'appliance virtuelle et la machine virtuelle de stockage ou le cluster contenant la machine virtuelle de stockage.

Exigences de contrôle d'accès basé sur les rôles (RBAC) pour la protection des charges de travail VMware

Le compte administrateur vCenter doit disposer des privilèges vCenter requis.

Pour obtenir la liste des privilèges vCenter nécessaires, consultez "SnapCenter Plug-in for VMware vSphere privilèges vCenter requis" .

Exigences pour la protection des charges de travail KVM

Vous avez besoin d'exigences spécifiques pour découvrir et protéger les machines virtuelles KVM.

- Une distribution Linux moderne exécutant la version du noyau 5.14.0-503.22.1.el9_5.x86_64 (long terme) ou ultérieure
- Vos hôtes KVM et vos machines virtuelles doivent être gérés par une plateforme de gestion. NetApp Backup and Recovery prend en charge les plateformes de gestion suivantes :
  - Apache CloudStack 4.22.0.0
- Assurez-vous que le trafic réseau entrant sur le port 22 est autorisé depuis l'agent de console vers l'hôte KVM.
- Agent invité QEMU version 9.0.0 ou ultérieure
- libvirt version 10.5.0 ou ultérieure

Pour garantir la réussite des restaurations de charges de travail KVM, assurez-vous que le paramètre **Activer l'instantané cohérent avec la machine virtuelle** est actif dans la stratégie de protection que vous utilisez pour les sauvegardes KVM.

Pour activer la protection des machines virtuelles KVM administrées par des utilisateurs non root, procédez comme suit :

1. Montez le volume en tant que type NFS3 pour éviter l'utilisation de `nobody` utilisateur et groupe.
2. Utilisez la commande suivante pour ajouter un utilisateur non root à la liste `qemu` groupe tout en préservant leurs groupes existants :

```
usermod -aG qemu <non-root-user>
```

3. Utilisez la commande suivante pour accorder la propriété du chemin de montage à `qemu` utilisateur et groupe et modifier les autorisations du chemin de montage :

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Supprimez le répertoire NetApp_SnapCenter_Backups existant s'il existe.

Exigences relatives à la protection des charges de travail Oracle Database

Assurez-vous que votre environnement répond à des exigences spécifiques pour découvrir et protéger les ressources Oracle.

- Base de données Oracle :
  - Oracle 19C et 21C sont pris en charge dans un déploiement autonome.
  - La base de données Oracle doit être déployée dans un stockage NetApp ONTAP principal ou secondaire.
  - Prise en charge du système d'exploitation hôte : Red Hat Enterprise Linux 8 et 9
- Prise en charge du stockage d'objets :
  - Stockage d'objets Azure
  - Amazon AWS
  - NetApp StorageGRID
  - ONTAP S3

Exigences pour la protection des applications Kubernetes

Vous avez besoin d'exigences spécifiques pour découvrir les ressources Kubernetes et protéger vos applications Kubernetes.

Pour connaître les exigences de la NetApp Console , reportez-vous àDans la NetApp Console .

- Un système ONTAP principal (ONTAP 9.16.1 ou version ultérieure)
- Un cluster Kubernetes - Les distributions et versions Kubernetes prises en charge incluent :
  - Anthos On-Prem (VMware) et Anthos sur bare metal 1.16

- Kubernetes 1.27 - 1.33
- OpenShift 4.10 - 4.18
- Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
- Suse Rancher

- NetApp Trident 24.10 ou version ultérieure
- NetApp Trident Protect 25.07 ou version ultérieure (installé lors de la découverte de la charge de travail Kubernetes)
- NetApp Trident Protect Connector 25.07 ou version ultérieure (installé lors de la découverte de la charge de travail Kubernetes)
  - Assurez-vous que le port TCP 443 n'est pas filtré dans le sens sortant entre le cluster Kubernetes, le Trident Protect Connector et le Trident Protect proxy.

Exigences pour la protection des charges de travail Hyper-V

Assurez-vous que votre instance Hyper-V répond à des exigences spécifiques pour découvrir et protéger les machines virtuelles.

- Configuration logicielle requise pour l'hôte Windows Server Hyper-V :
  - Éditions Microsoft Hyper-V 2019, 2022 et 2025
  - Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs)
  - PowerShell 7.4.2 ou version ultérieure
  - Si des utilisateurs n'appartenant pas à un domaine d'administrateur doivent protéger des machines virtuelles Hyper-V, assurez-vous qu'ils disposent des autorisations suivantes :
    - Assurez-vous que l'utilisateur est membre du groupe des administrateurs locaux.
    - Assurez-vous que l'utilisateur fait partie de la stratégie de sécurité locale « Ouvrir une session en tant que service ».
  - Assurez-vous que le trafic HTTPS bidirectionnel est autorisé pour les ports suivants dans les paramètres du pare-feu Windows :
    - 8144 (plugin NetApp pour Hyper-V)
    - 8145 (plugin NetApp pour Windows)
- Configuration matérielle requise pour l'hôte Hyper-V :
  - Les hôtes autonomes et en cluster FCI sont pris en charge
  - 1 Go de RAM minimum pour le plug-in NetApp Hyper-V sur l'hôte Hyper-V
  - 5 Go minimum d'espace d'installation et de journal pour le plug-in sur l'hôte Hyper-V

> Assurez-vous d'allouer suffisamment d'espace disque sur l'hôte Hyper-V pour le dossier des journaux et surveillez régulièrement son utilisation. L'espace requis dépend de la fréquence des sauvegardes et des opérations de protection des données. S'il n'y a pas assez d'espace, les journaux ne seront pas générés.

- Configuration requise NetApp ONTAP :
  - Un système ONTAP principal (ONTAP 9.14.1 ou version ultérieure)
  - Pour les déploiements Hyper-V utilisant des partages CIFS pour stocker les données de la machine virtuelle, assurez-vous que la propriété de partage de disponibilité continue est activée sur le système

ONTAP . Reportez-vous à la "Documentation ONTAP" pour les instructions.

Dans la NetApp Console

Assurez-vous que la NetApp Console répond aux exigences suivantes.

- Un utilisateur de la console doit disposer du rôle et des privilèges requis pour effectuer des opérations sur les charges de travail Microsoft SQL Server et Kubernetes. Pour découvrir les ressources, vous devez disposer du rôle NetApp Backup and Recovery de Super administrateur. Voir"Accès aux fonctionnalités de NetApp Backup and Recovery basé sur les rôles" pour plus de détails sur les rôles et les autorisations requis pour effectuer des opérations dans NetApp Backup and Recovery.
- Une organisation de console avec au moins un agent de console actif qui se connecte aux clusters ONTAP locaux ou à Cloud Volumes ONTAP.
- Au moins un système de console avec un cluster NetApp sur site ONTAP ou Cloud Volumes ONTAP .
- Un agent de console

  Se référer à "Apprenez à configurer un agent de console" et "exigences standard de la NetApp Console" .

  - La version d'aperçu nécessite le système d'exploitation Ubuntu 22.04 LTS pour l'agent de console.

Configurer la NetApp Console

L'étape suivante consiste à configurer la console et la NetApp Backup and Recovery.

Revoir "exigences standard de la NetApp Console" .

Créer un agent de console

Vous devez contacter votre équipe produit NetApp pour essayer la sauvegarde et la récupération. Ensuite, lorsque vous utilisez l'agent de console, il inclura les fonctionnalités appropriées pour le service.

Pour créer un agent de console dans la NetApp Console avant d'utiliser le service, reportez-vous à la documentation de la console qui décrit "comment créer un agent de console" .

Où installer l'agent de console

Pour terminer une opération de restauration, l'agent de console peut être installé aux emplacements suivants :

- Pour Amazon S3, l'agent de console peut être déployé sur vos locaux.
- Pour Azure Blob, l'agent de console peut être déployé sur vos locaux.
- Pour StorageGRID, l'agent de console doit être déployé dans vos locaux ; avec ou sans accès Internet.
- Pour ONTAP S3, l'agent de console peut être déployé dans vos locaux (avec ou sans accès Internet) ou dans un environnement de fournisseur de cloud

Les références aux « systèmes ONTAP sur site » incluent les systèmes FAS et AFF .

Configurer les licences pour NetApp Backup and Recovery

Vous pouvez obtenir une licence NetApp Backup and Recovery en achetant un abonnement payant à l'utilisation (PAYGO) ou un abonnement annuel à * NetApp Intelligent Services* auprès de votre fournisseur de cloud, ou en achetant une licence

BYOL (Bring Your Own License) auprès de NetApp. Une licence valide est requise pour activer NetApp Backup and Recovery sur un système, pour créer des sauvegardes de vos données de production et pour restaurer les données de sauvegarde sur un système de production.

Quelques notes avant de poursuivre votre lecture :

- Si vous êtes déjà abonné à l'abonnement à la carte (PAYGO) sur la place de marché de votre fournisseur de cloud pour un système Cloud Volumes ONTAP , vous êtes également automatiquement abonné à NetApp Backup and Recovery . Vous n'aurez pas besoin de vous abonner à nouveau.
- La licence BYOL (Bring Your Own License) de NetApp Backup and Recovery est une licence flottante que vous pouvez utiliser sur tous les systèmes associés à votre organisation ou compte NetApp Console . Ainsi, si vous disposez d'une capacité de sauvegarde suffisante à partir d'une licence BYOL existante, vous n'aurez pas besoin d'acheter une autre licence BYOL.
- Si vous utilisez une licence BYOL, il est recommandé de souscrire également à un abonnement PAYGO. Si vous sauvegardez plus de données que ce qui est autorisé par votre licence BYOL, ou si la durée de votre licence expire, la sauvegarde continue via votre abonnement à la carte - il n'y a aucune interruption de service.
- Lors de la sauvegarde des données ONTAP sur site sur StorageGRID, vous avez besoin d'une licence BYOL, mais il n'y a aucun coût pour l'espace de stockage du fournisseur cloud.

"En savoir plus sur les coûts liés à l'utilisation de NetApp Backup and Recovery."

Essai gratuit de 30 jours

Un essai gratuit de 30 jours de NetApp Backup and Recovery est disponible si vous souscrivez à un abonnement à la carte sur la place de marché de votre fournisseur de cloud pour * NetApp Intelligent Services*. L'essai gratuit commence au moment où vous vous abonnez à la liste du marché. Notez que si vous payez l'abonnement Marketplace lors du déploiement d'un système Cloud Volumes ONTAP , puis démarrez votre essai gratuit de NetApp Backup and Recovery 10 jours plus tard, il vous restera 20 jours pour utiliser l'essai gratuit.

Une fois l'essai gratuit terminé, vous passerez automatiquement à l'abonnement PAYGO sans interruption. Si vous décidez de ne pas continuer à utiliser NetApp Backup and Recovery,"désinscrire NetApp Backup and Recovery du système" avant la fin de l'essai et vous ne serez pas facturé.

Mettre fin à l'essai gratuit

Si vous souhaitez continuer à utiliser NetApp Backup and Recovery après la fin de la période d'essai gratuite, vous devez configurer un abonnement payant. Vous pouvez le faire à partir de l'interface de la NetApp Console en accédant à la section de facturation et en sélectionnant un plan d'abonnement adapté à vos besoins. Si vous ne souhaitez pas continuer à utiliser NetApp Backup and Recovery, vous pouvez mettre fin à l'essai gratuit.

Lorsque vous mettez fin à l'essai gratuit sans souscrire à un forfait payant, vos données sont automatiquement supprimées 60 jours après la fin de l'essai gratuit. Vous pouvez éventuellement demander au système de supprimer immédiatement vos données.

Étapes

1. Depuis la page d'accueil de NetApp Backup and Recovery , sélectionnez **Afficher l'essai gratuit**.
2. Sélectionnez **Terminer l'essai gratuit**.

3. Sélectionnez **Supprimer les données immédiatement après la fin de mon essai gratuit** pour supprimer vos données immédiatement.
4. Tapez **fin de l'essai** dans la case.
5. Sélectionnez **Fin** pour confirmer.

Utiliser un abonnement NetApp Backup and Recovery PAYGO

Pour le paiement à l'utilisation, vous paierez à votre fournisseur de cloud les coûts de stockage d'objets et les coûts de licence de sauvegarde NetApp sur une base horaire dans un seul abonnement. Vous devez vous abonner à * NetApp Intelligent Services* sur la Marketplace même si vous disposez d'un essai gratuit ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit qu'il n'y aura aucune interruption de service après la fin de votre essai gratuit. Une fois la période d'essai terminée, vous serez facturé toutes les heures en fonction de la quantité de données que vous sauvegardez.
- Si vous sauvegardez plus de données que ce qui est autorisé par votre licence BYOL, les opérations de sauvegarde et de restauration des données se poursuivent via votre abonnement à la carte. Par exemple, si vous disposez d'une licence BYOL de 10 Tio, toute capacité au-delà de 10 Tio est facturée via l'abonnement PAYGO.

Vous ne serez pas facturé sur votre abonnement prépayé pendant votre essai gratuit ou si vous n'avez pas dépassé votre licence BYOL.

Il existe quelques plans PAYGO pour NetApp Backup and Recovery:

- Un package « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un package « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour le système Cloud Volumes ONTAP à l'aide de la licence (la capacité de sauvegarde n'est pas comptabilisée dans la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

  Notez que cette option nécessite également un abonnement PAYGO de sauvegarde et de récupération, mais aucun frais ne sera facturé pour les systèmes Cloud Volumes ONTAP éligibles.

"En savoir plus sur ces packages de licences basés sur la capacité".

Utilisez ces liens pour vous abonner à NetApp Backup and Recovery depuis la place de marché de votre fournisseur de cloud :

- AWS : "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." .
- Azuré: "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." .
- Google Cloud : "Accédez à l'offre Marketplace pour les NetApp Intelligent Services pour connaître les détails des tarifs." .

Utiliser un contrat annuel

Payez NetApp Backup and Recovery annuellement en achetant un contrat annuel. Ils sont disponibles pour des durées de 1, 2 ou 3 ans.

Si vous disposez d'un contrat annuel auprès d'une place de marché, toute consommation de NetApp Backup and Recovery est facturée sur ce contrat. Vous ne pouvez pas combiner un contrat de marché annuel avec un BYOL.

Lorsque vous utilisez AWS, deux contrats annuels sont disponibles auprès du "Page AWS Marketplace" pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement depuis la page Marketplace puis "associer l'abonnement à vos informations d'identification AWS" . Notez que vous devrez également payer vos systèmes Cloud Volumes ONTAP à l'aide de cet abonnement contractuel annuel, car vous ne pouvez attribuer qu'un seul abonnement actif à vos informations d'identification AWS dans la console.

- Un plan « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour le système Cloud Volumes ONTAP à l'aide de la licence (la capacité de sauvegarde n'est pas comptabilisée dans la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

  Voir le "Sujet sur les licences Cloud Volumes ONTAP" pour en savoir plus sur cette option de licence.

  Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lors de la création d'un système Cloud Volumes ONTAP et la console vous invite à vous abonner à AWS Marketplace.

Lorsque vous utilisez Azure, deux contrats annuels sont disponibles auprès du "Page de la place de marché Azure" pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan « Cloud Backup » qui vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement depuis la page Marketplace puis "associer l'abonnement à vos informations d'identification Azure" . Notez que vous devrez également payer vos systèmes Cloud Volumes ONTAP à l'aide de cet abonnement contractuel annuel, car vous ne pouvez attribuer qu'un seul abonnement actif à vos informations d'identification Azure dans la console.

- Un plan « CVO Professional » qui vous permet de regrouper Cloud Volumes ONTAP et NetApp Backup and Recovery. Cela inclut des sauvegardes illimitées pour le système Cloud Volumes ONTAP à l'aide de la licence (la capacité de sauvegarde n'est pas comptabilisée dans la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

  Voir le "Sujet sur les licences Cloud Volumes ONTAP" pour en savoir plus sur cette option de licence.

  Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lors de la création d'un système Cloud Volumes ONTAP et lorsque la console vous invite à vous abonner à Azure Marketplace.

Lorsque vous utilisez GCP, contactez votre représentant commercial NetApp pour acheter un contrat annuel. Le contrat est disponible sous forme d'offre privée sur Google Cloud Marketplace.

Une fois que NetApp vous aura communiqué l'offre privée, vous pourrez sélectionner le forfait annuel lors de votre inscription sur Google Cloud Marketplace au moment de l'activation de NetApp Backup and Recovery .

Utiliser une licence BYOL NetApp Backup and Recovery

Les licences Bring Your Own de NetApp offrent des durées de 1, 2 ou 3 ans. Vous ne payez que pour les données que vous protégez, calculées par la capacité logique utilisée (avant toute efficacité) des volumes ONTAP sources qui sont sauvegardés. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

La licence BYOL NetApp Backup and Recovery est une licence flottante où la capacité totale est partagée entre tous les systèmes associés à votre organisation ou compte NetApp Console . Pour les systèmes ONTAP , vous pouvez obtenir une estimation approximative de la capacité dont vous aurez besoin en exécutant la commande CLI `volume show -fields logical-used-by-afs` pour les volumes que vous prévoyez de sauvegarder.

Si vous ne disposez pas d'une licence BYOL NetApp Backup and Recovery , cliquez sur l'icône de chat en bas à droite de la console pour en acheter une.

En option, si vous disposez d'une licence basée sur un nœud non attribué pour Cloud Volumes ONTAP que vous n'utiliserez pas, vous pouvez la convertir en une licence NetApp Backup and Recovery avec la même équivalence en dollars et la même date d'expiration. "Cliquez ici pour plus de détails" .

Vous utilisez la NetApp Console pour gérer les licences BYOL. Vous pouvez ajouter de nouvelles licences, mettre à jour les licences existantes et afficher l'état des licences à partir de la console.

"En savoir plus sur l'ajout de licences".

Configurer des certificats de sécurité pour StorageGRID et ONTAP dans NetApp Backup and Recovery

Créez un certificat de sécurité pour activer la communication entre NetApp Backup and Recovery et StorageGRID ou ONTAP.

Créer un certificat de sécurité pour StorageGRID

Si la communication entre les conteneurs NetApp Backup and Recovery et StorageGRID doit vérifier le certificat StorageGRID , procédez comme suit.

Le certificat généré doit avoir un CN et un nom alternatif du sujet comme nom fourni dans NetApp Backup and Recovery lorsque vous avez activé la sauvegarde.

Étapes

1. Suivez les étapes de la documentation StorageGRID pour créer le certificat StorageGRID .

   "Informations StorageGRID sur la configuration des certificats"

2. Mettez à jour StorageGRID avec le certificat si vous ne l'avez pas déjà fait.
3. Connectez-vous à l'agent de la console en tant qu'utilisateur root. Courir:

   ```
   sudo su
   ```

4. Obtenez le volume Docker NetApp Backup and Recovery (Cloud Backup Service). Courir:

```
docker volume ls | grep cbs
```

Exemple de sortie :

```
local service-manager-2_cloudmanager_cbs_volume"
```

Le nom du volume diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple utilise le mode Standard. Se référer à "Modes de déploiement de la NetApp Console" .

5. Recherchez le point de montage du volume NetApp Backup and Recovery . Courir:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Exemple de sortie :

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data"
```

Le point de montage diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

6. Accédez au répertoire MountPoint. Courir:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

7. Si le certificat de StorageGRID est signé par l'autorité de certification racine et une autorité de certification intermédiaire, ajoutez le `pem` fichiers des deux dans un seul fichier nommé `sgws.crt` à l'emplacement actuel. N'ajoutez pas le certificat feuille à ce fichier.

Étapes pour le conteneur cloudmanager_cbs

Vous devrez activer la vérification du certificat du serveur StorageGRID dans NetApp Backup and Recovery (Cloud Backup Service).

1. Modifiez les répertoires vers le volume Docker obtenu lors des étapes précédentes.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Changez de répertoire vers le répertoire de configuration.

```
cd cbs_config
```

3. Créez et enregistrez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Sortez du conteneur. Courir:

```
exit
```

5. Redémarrage `cloudmanager_cbs` . Courir:

```
docker restart cloudmanager_cbs
```

Étapes pour le conteneur cloudmanager_cbs_catalog

Ensuite, vous devrez activer la vérification du certificat du serveur StorageGRID pour le service de catalogage.

1. Changer les répertoires du volume Docker :

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Configurer le catalogue. Courir:

```
cd cbs_catalog_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration du catalogue

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Redémarrer le catalogue. Courir:

```
docker restart cloudmanager_cbs_catalog
```

Mettre à jour le certificat de l'agent de console avec le certificat StorageGRID en fonction du système d'exploitation de l'agent

Ubuntu

1. Copiez le certificat SGWS sur `/usr/local/share/ca-certificates` . Voici un exemple :

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

   où `sgws.crt` est le certificat CA racine.

2. Mettez à jour les certificats d'hôte avec le certificat StorageGRID . Courir

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Copiez le certificat SGWS sur `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

où `sgws.crt` est le certificat CA racine.

2. Mettez à jour les certificats d'hôte avec le certificat StorageGRID .

```
update-ca-trust extract
```

3. Mettre à jour le `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Pour vérifier si les certificats sont présents, exécutez la commande suivante :

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Créer un certificat de sécurité pour ONTAP

Si la communication entre les conteneurs NetApp Backup and Recovery et ONTAP doit valider le certificat ONTAP , procédez comme suit.

NetApp Backup and Recovery utilise l'IP de gestion de cluster pour se connecter à ONTAP. Saisissez l'adresse IP du cluster dans les noms alternatifs du sujet du certificat. Spécifiez cette étape lorsque vous générez la CSR à l'aide de l'interface utilisateur du gestionnaire système.

Utilisez la documentation du gestionnaire de système pour créer un nouveau certificat CA pour ONTAP.

- "Gérer les certificats avec System Manager"
- "Comment gérer les certificats SSL ONTAP avec System Manager"

Étapes

1. Connectez-vous à l'agent de la console en tant que root. Courir:

```
sudo su
```

2. Obtenez le volume Docker de NetApp Backup and Recovery . Courir:

```
docker volume ls | grep cbs
```

Exemple de sortie :

```
local service-manager-2_cloudmanager_cbs_volume
```

Le nom du volume diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

3. Obtenez le support pour le volume. Courir:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

Exemple de sortie :

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

Le point de montage diffère selon les modes de déploiement Standard, Privé et Restreint. Cet exemple montre un déploiement cloud standard. Se référer à "Modes de déploiement de la NetApp Console" .

4. Accédez au répertoire du point de montage. Courir:

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

5. Effectuez l'une des étapes suivantes :
   - Si le certificat ONTAP est signé par l'autorité de certification racine et une autorité de certification intermédiaire, ajoutez le `pem` fichiers des deux dans un seul fichier nommé `ontap.crt` à l'emplacement actuel.
   - Si le certificat ONTAP est signé par une seule autorité de certification, renommez-le `pem` déposer comme `ontap.crt` et copiez-le à l'emplacement actuel. N'ajoutez pas le certificat feuille à ce fichier.

Étapes pour le conteneur cloudmanager_cbs

Ensuite, activez la vérification du certificat du serveur ONTAP dans NetApp Backup and Recovery (Cloud Backup Service).

1. Modifiez les répertoires vers le volume Docker obtenu lors des étapes précédentes.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Accédez au répertoire de configuration. Courir:

```
cd cbs_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Sortez du conteneur. Courir:

```
exit
```

5. Redémarrez NetApp Backup and Recovery. Courir:

```
docker restart cloudmanager_cbs
```

Étapes pour le conteneur cloudmanager_cbs_catalog

Activez la vérification du certificat du serveur ONTAP pour le service de catalogage.

1. Changez les répertoires vers le volume Docker. Courir:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Courir:

```
cd cbs_catalog_config
```

3. Créez un fichier de configuration comme indiqué ci-dessous avec l'un des noms suivants en fonction de votre environnement de déploiement :

   - `production-customer.json`Utilisé pour les déploiements en mode standard et en mode restreint.
   - `darksite-customer.json`Utilisé pour les déploiements en mode privé.

   Se référer à "Modes de déploiement de la NetApp Console" .

   Fichier de configuration

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Redémarrez NetApp Backup and Recovery. Courir:

```
docker restart cloudmanager_cbs_catalog
```

Créer un certificat pour ONTAP et StorageGRID

Si vous devez activer le certificat pour ONTAP et StorageGRID, le fichier de configuration ressemble à ceci :

Fichier de configuration pour ONTAP et StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Configurez les destinations de sauvegarde avant d'utiliser NetApp Backup and Recovery

Avant d'utiliser NetApp Backup and Recovery, effectuez quelques étapes pour configurer les destinations de sauvegarde.

Avant de commencer, révisez"prérequis" pour garantir que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez une ou plusieurs des destinations de sauvegarde suivantes :

- StorageGRID NetApp .

  Se référer à "Découvrez StorageGRID" .

  Se référer à "Documentation de StorageGRID" pour plus de détails sur StorageGRID.

- Services Web Amazon. Se référer à "Documentation Amazon S3" .

  Procédez comme suit pour préparer AWS comme destination de sauvegarde :

  - Configurez un compte dans AWS.
  - Configurez les autorisations S3 dans AWS, répertoriées dans la section suivante.
  - Pour plus de détails sur la gestion de votre stockage AWS dans la console, reportez-vous à "Gérez vos buckets Amazon S3" .
- Microsoft Azure.
  - Se référer à "Documentation Azure NetApp Files" .
  - Configurez un compte dans Azure.

- Configure "Autorisations Azure" dans Azure.
- Pour plus de détails sur la gestion de votre stockage Azure dans la console, reportez-vous à "Gérez vos comptes de stockage Azure" .

Après avoir configuré les options dans la destination de sauvegarde elle-même, vous la configurerez ultérieurement comme destination de sauvegarde dans NetApp Backup and Recovery. Pour plus de détails sur la configuration de la destination de sauvegarde dans NetApp Backup and Recovery, reportez-vous à"Découvrir les cibles de sauvegarde" .

Configurer les autorisations S3

Vous devrez configurer deux ensembles d'autorisations AWS S3 :

- Autorisations permettant à l'agent de console de créer et de gérer le compartiment S3.
- Autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire des données dans le bucket S3.

Étapes

1. Assurez-vous que l'agent de la console dispose des autorisations requises. Pour plus de détails, voir "Autorisations de stratégie de la NetApp Console" .

   Lors de la création de sauvegardes dans les régions AWS Chine, vous devez modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* dans les politiques IAM de « aws » à « aws-cn » ; par exemple `arn:aws-cn:s3:::netapp-backup-*` .

2. Lorsque vous activez le service, l'assistant de sauvegarde vous invite à saisir une clé d'accès et une clé secrète. Ces informations d'identification sont transmises au cluster ONTAP afin ONTAP puisse sauvegarder et restaurer les données dans le bucket S3. Pour cela, vous devrez créer un utilisateur IAM avec les autorisations suivantes.

   Reportez-vous à la "Documentation AWS : Création d'un rôle pour déléguer des autorisations à un utilisateur IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Connectez-vous à NetApp Backup and Recovery

Vous utilisez la NetApp Console pour vous connecter à NetApp Backup and Recovery.

NetApp Backup and Recovery utilise la gestion des identités et des accès pour contrôler ce que chaque utilisateur peut faire.

Pour plus de détails sur les actions que chaque rôle peut effectuer, voir"Rôles utilisateur de NetApp Backup and Recovery" .

Pour vous connecter à la NetApp Console, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion à la NetApp Console à l'aide de votre adresse e-mail et d'un mot de passe. "En savoir plus sur la connexion" .

Rôle de NetApp Console requis Rôle de super administrateur de sauvegarde et de récupération ou d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Pour ajouter un agent de console, vous devez disposer du rôle de super administrateur de sauvegarde et de récupération.

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console" .

   La page de connexion à la NetApp Console s'affiche.

2. Connectez-vous à la console.
3. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
   - Si c'est la première fois que vous vous connectez à Backup and Recovery et que vous n'avez pas encore ajouté de système à la page **Systèmes**, Backup and Recovery affiche la page d'accueil « Bienvenue sur le nouveau NetApp Backup and Recovery» avec une option permettant d'ajouter un système. Pour plus d'informations sur l'ajout d'un système à la page **Systèmes**, veuillez consulter "Prise en main du mode standard de la NetApp Console".
   - Si vous vous connectez à Backup and Recovery pour la première fois et que vous avez un système dans la console mais aucune ressource découverte, la page *Bienvenue sur le nouveau NetApp Backup and Recovery* apparaît avec une option pour **Découvrir les ressources**.
4. Si vous ne l'avez pas déjà fait, sélectionnez l'option **Découvrir et gérer**.
   - Pour les charges de travail Microsoft SQL Server, reportez-vous à"Découvrez les charges de travail Microsoft SQL Server" .
   - Pour les charges de travail VMware, reportez-vous à"Découvrez les charges de travail VMware" .
   - Pour les charges de travail KVM, reportez-vous à"Découvrez les charges de travail KVM" .
   - Pour les charges de travail Oracle Database, consultez "Découvrez les charges de travail Oracle Database".
   - Pour les charges de travail Hyper-V, reportez-vous à"Découvrez les charges de travail Hyper-V" .
   - Pour les charges de travail Kubernetes, reportez-vous à"Découvrez les charges de travail Kubernetes" .

Découvrez les cibles de sauvegarde hors site dans NetApp Backup and Recovery

Suivez quelques étapes pour découvrir ou ajouter manuellement des cibles de sauvegarde hors site dans NetApp Backup and Recovery.

Découvrir une cible de sauvegarde

Configurez vos cibles de sauvegarde (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID) avant d'utiliser NetApp Backup and Recovery.

Vous pouvez découvrir ces cibles automatiquement ou les ajouter manuellement.

Fournissez les informations d'identification pour accéder au compte de stockage. NetApp Backup and Recovery utilise ces informations d'identification pour découvrir les charges de travail que vous souhaitez sauvegarder.

Avant de commencer

Vous devez découvrir au moins une charge de travail avant de pouvoir ajouter une cible de sauvegarde hors site.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'onglet **Cibles de sauvegarde hors site**.
3. Sélectionnez **Découvrir la cible de sauvegarde**.
4. Sélectionnez l'un des types de cibles de sauvegarde : **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* ou * ONTAP S3*.
5. Dans la section **Choisir l'emplacement des informations d'identification**, choisissez l'emplacement où résident les informations d'identification, puis choisissez comment associer les informations d'identification.
6. Sélectionnez **Suivant**.
7. Saisissez les informations d'identification. Elles varient selon le type de cible de sauvegarde sélectionné et l'emplacement des informations d'identification choisi.
   - Pour AWS :
     - **Nom d'identification** : saisissez le nom d'identification AWS.
     - **Clé d'accès** : Saisissez le secret AWS.
     - **Clé secrète** : saisissez la clé secrète AWS.
   - Pour Azure :
     - **Nom des informations d'identification** : saisissez le nom des informations d'identification du stockage d'objets blob Azure.
     - **Secret client** : saisissez le secret client du stockage d'objets blob Azure.
     - **ID d'application (client)** : sélectionnez l'ID d'application Azure Blob Storage.
     - **ID de locataire du répertoire** : saisissez l'ID de locataire du stockage d'objets blob Azure.
   - Pour StorageGRID:
     - **Nom d'identification** : saisissez le nom d'identification StorageGRID .

- **Nom de domaine complet du nœud de passerelle** : saisissez un nom de domaine complet pour StorageGRID.
- **Port**: saisissez le numéro de port pour StorageGRID.
- **Clé d'accès** : saisissez la clé d'accès StorageGRID S3.
- **Clé secrète** : saisissez la clé secrète StorageGRID S3.

◦ Pour ONTAP S3 :

- **Nom d'identification** : saisissez le nom d'identification ONTAP S3.
- **Nom de domaine complet du nœud de passerelle** : saisissez un nom de domaine complet pour ONTAP S3.
- **Port** : saisissez le numéro de port pour ONTAP S3.
- **Clé d'accès** : Saisissez la clé d'accès ONTAP S3.
- **Clé secrète** : Saisissez la clé secrète ONTAP S3.

8. Sélectionnez **Découvrir**.

Ajouter un bucket pour une cible de sauvegarde

Plutôt que de laisser NetApp Backup and Recovery découvrir automatiquement les buckets, vous pouvez ajouter manuellement un bucket à une cible de sauvegarde hors site.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions*** icône et sélectionnez ***Ajouter un bucket**.
4. Saisissez les informations du bucket. Les informations diffèrent selon le type de cible de sauvegarde que vous avez sélectionné.

◦ Pour AWS :

- **Nom du bucket** : saisissez le nom du bucket S3. Le préfixe « netapp-backup » est un préfixe obligatoire et est automatiquement ajouté au nom que vous fournissez.
- **Compte AWS** : saisissez le nom du compte AWS.
- **Région du bucket** : saisissez la région AWS du bucket.
- **Activer le verrouillage d'objet S3** : sélectionnez cette option pour activer le verrouillage d'objet S3 pour le bucket. S3 Object Lock empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.
  - **Mode de gouvernance** : sélectionnez cette option pour activer le mode de gouvernance pour le bucket S3 Object Lock. Le mode de gouvernance vous permet de protéger les objets contre la suppression ou l'écrasement par la plupart des utilisateurs, mais permet à certains utilisateurs de modifier les paramètres de conservation.
  - **Mode de conformité** : sélectionnez cette option pour activer le mode de conformité pour le compartiment S3 Object Lock. Le mode de conformité empêche tout utilisateur, y compris l'utilisateur root, de modifier les paramètres de conservation ou de supprimer des objets jusqu'à l'expiration de la période de conservation.
- **Versioning** : sélectionnez cette option pour activer le contrôle de version pour le bucket S3. Le

contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.

- **Tags** : sélectionnez les balises pour le bucket S3. Les balises sont des paires clé-valeur qui peuvent être utilisées pour organiser et gérer vos ressources S3.
- **Cryptage** : sélectionnez le type de cryptage pour le compartiment S3. Les options sont soit des clés gérées par AWS S3, soit des clés AWS Key Management Service. Si vous sélectionnez des clés AWS Key Management Service, vous devez fournir l'ID de clé.

◦ Pour Azure :

- **Abonnement** : sélectionnez le nom du conteneur de stockage d'objets blob Azure.
- **Groupe de ressources** : sélectionnez le nom du groupe de ressources Azure.
- **Détails de l'instance**:
  - **Nom du compte de stockage** : saisissez le nom du conteneur de stockage d'objets blob Azure.
  - **Région Azure** : saisissez la région Azure du conteneur.
  - **Type de performance** : sélectionnez le type de performance Standard ou Premium pour le conteneur de stockage d'objets blob Azure indiquant le niveau de performance requis.
  - **Chiffrement** : sélectionnez le type de chiffrement pour le conteneur de stockage d'objets blob Azure. Les options sont soit des clés gérées par Microsoft, soit des clés gérées par le client. Si vous sélectionnez des clés gérées par le client, vous devez fournir le nom du coffre de clés et le nom de la clé.

◦ Pour StorageGRID:

- **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket StorageGRID .
- **Nom du bucket** : saisissez le nom du bucket StorageGRID .
- **Région** : saisissez la région StorageGRID pour le bucket.
- **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket StorageGRID . Le contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.
- **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le bucket StorageGRID . Le verrouillage des objets empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.
- **Capacité** : saisissez la capacité du bucket StorageGRID . Il s'agit de la quantité maximale de données pouvant être stockée dans le bucket.

◦ Pour ONTAP S3 :

- **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket ONTAP S3.
- **Nom de la cible du bucket** : saisissez le nom du bucket ONTAP S3.
- **Capacité** : saisissez la capacité du bucket ONTAP S3. Il s'agit de la quantité maximale de données pouvant être stockée dans le bucket.
- **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket ONTAP S3. Le contrôle de version vous permet de conserver plusieurs versions d'objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de récupération.
- **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le compartiment ONTAP S3. Le verrouillage des objets empêche la suppression ou l'écrasement des

objets pendant une période de conservation spécifiée, offrant ainsi une couche supplémentaire de protection des données. Vous ne pouvez activer cette option que lorsque vous créez un bucket et vous ne pouvez pas la désactiver ultérieurement.

5. Sélectionnez **Ajouter**.

Modifier les informations d'identification pour une cible de sauvegarde

Saisissez les informations d'identification nécessaires pour accéder à la cible de sauvegarde.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions*** icône et sélectionnez *Modifier les informations d'identification**.
4. Saisissez les nouvelles informations d'identification pour la cible de sauvegarde. Les informations diffèrent selon le type de cible de sauvegarde que vous avez sélectionné.
5. Sélectionnez **Terminé**.

Basculer vers différentes charges de travail de NetApp Backup and Recovery

Vous pouvez basculer entre les différentes charges de travail de NetApp Backup and Recovery .

Passer à une charge de travail différente

Vous pouvez basculer vers une charge de travail différente dans l'interface utilisateur de NetApp Backup and Recovery .

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Dans le coin supérieur droit de la page, sélectionnez la liste déroulante **Changer de charge de travail**.
3. Sélectionnez la charge de travail vers laquelle vous souhaitez basculer.

   La page s'actualise et affiche la charge de travail sélectionnée.

Configurer les paramètres de NetApp Backup and Recovery

Après avoir configuré la NetApp Console, configurez les paramètres de sauvegarde et de récupération. Ajoutez des informations d'identification pour les ressources de l'hôte, importez des ressources SnapCenter , configurez les répertoires de journaux et définissez les paramètres VMware vCenter. Effectuez ces étapes avant de sauvegarder ou de récupérer des données.

- Ajouter des informations d'identification pour les ressources de l'hôte pour tous les hôtes Windows, Microsoft SQL Server, Oracle Database ou Linux avec lesquels NetApp Backup and Recovery doit s'authentifier. Cela inclut les informations d'identification du système d'exploitation invité Windows utilisées

lors de la restauration des fichiers ou dossiers invités.

- Maintenir les paramètres VMware vCenter.
- Importer et gérer les ressources de l'hôte SnapCenter. (charges de travail Microsoft SQL Server uniquement)
- Ajouter une plateforme de gestion KVM. (Charges de travail KVM uniquement)
- Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows.
- Créer un modèle de hook d'exécution pour exécuter des scripts avant et après les tâches de sauvegarde. (Charges de travail Kubernetes uniquement)

Rôle de NetApp Console requis Super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services" .

Ajouter des informations d'identification pour les ressources de l'hôte

Ajouter les informations d'identification pour les ressources hôtes. NetApp Backup and Recovery utilise ces informations d'identification pour découvrir les charges de travail et appliquer les politiques de sauvegarde.

Si vous ne disposez pas d'informations d'identification, créez-les avec des autorisations pour accéder aux charges de travail de l'hôte et les gérer.

Vous devez configurer les types d'informations d'identification suivants :

- Informations d'identification Microsoft SQL Server
- Informations d'identification de l'hôte Windows SnapCenter
- Informations d'identification du système d'exploitation invité Windows utilisées lors de la restauration des fichiers ou dossiers invités
- Identifiants de base de données Oracle
- Identifiants de l'hôte Linux

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour **Informations d'identification**.
3. Sélectionnez **Ajouter de nouvelles informations d'identification**.
4. Saisissez les informations d'identification. Les champs affichés varient selon le mode d'authentification sélectionné. Passez votre souris sur l'icône d'information **i** pour obtenir plus d'informations sur les champs.
    - **Nom des informations d'identification** : saisissez un nom pour les informations d'identification.
    - **Mode d'authentification** : Sélectionnez **Windows**, **Microsoft SQL**, **Oracle Database** ou **Linux**.

Pour les charges de travail Microsoft SQL Server, vous devez saisir des informations d'identification à la fois pour Windows et pour Microsoft SQL Server ; vous devrez donc ajouter deux ensembles d'informations d'identification.

Windows

i. Si vous avez sélectionné **Windows** :

- **Agents** : Sélectionnez un agent de console dans la liste.
- **Domaine et nom d'utilisateur** : saisissez le nom de domaine complet NetBIOS ou du domaine et le nom d'utilisateur pour les informations d'identification.
- **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.

Microsoft SQL Server

i. Si vous avez sélectionné **Microsoft SQL Server** :

- **Domaine et nom d'utilisateur** : saisissez le nom de domaine complet NetBIOS ou du domaine et le nom d'utilisateur pour les informations d'identification.
- **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
- **Hôtes** : Sélectionnez une adresse d'hôte SQL Server détectée.
- **Instance SQL Server** : sélectionnez une instance SQL Server découverte.

Base de données Oracle

i. Si vous avez sélectionné **Oracle Database** :

- **Agents** : Sélectionnez un agent de console dans la liste.
- **Nom d'utilisateur** : Veuillez saisir le nom d'utilisateur pour les identifiants.
- **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.

Linux

i. Si vous avez sélectionné **Linux** :

- **Agents** : Sélectionnez un agent de console dans la liste.
- **Nom d'utilisateur** : Veuillez saisir le nom d'utilisateur pour les identifiants.
- **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.

5. Sélectionnez **Ajouter**.

Modifier les informations d'identification pour les ressources de l'hôte

Vous pourrez modifier ultérieurement le mot de passe de tous les identifiants que vous avez créés.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Informations d'identification**.
3. Sélectionnez l'icône Actions ••• > **Modifier les informations d'identification**.
   - **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
4. Sélectionnez **Enregistrer**.

Maintenir les paramètres VMware vCenter

Fournissez les informations d'identification VMware vCenter pour découvrir les charges de travail à

sauvegarder. Si vous ne disposez pas d'informations d'identification, créez-les avec des autorisations pour accéder et gérer les charges de travail VMware vCenter Server.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **VMware vCenter**.
3. Sélectionnez **Ajouter vCenter**.
4. Saisissez les informations du serveur VMware vCenter.
   - **VCenter FQDN ou adresse IP** : saisissez un nom de domaine complet ou l'adresse IP du serveur VMware vCenter.
   - **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur VMware vCenter.
   - **Port** : saisissez le numéro de port du serveur VMware vCenter.
   - **Protocole** : Sélectionnez **HTTP** ou **HTTPS**.
5. Sélectionnez **Ajouter**.

Importer et gérer les ressources de l'hôte SnapCenter

Si vous avez déjà utilisé SnapCenter pour sauvegarder vos ressources, vous pouvez importer et gérer ces ressources dans NetApp Backup and Recovery. Cette option vous permet d'importer les informations du serveur SnapCenter pour enregistrer plusieurs serveurs SnapCenter et découvrir les charges de travail de la base de données.

Il s'agit d'un processus en deux parties :

- Importer l'application SnapCenter Server et les ressources de l'hôte
- Gérer les ressources hôtes SnapCenter sélectionnées

Importer l'application SnapCenter Server et les ressources de l'hôte

Cette première étape importe les ressources de l'hôte depuis SnapCenter et affiche ces ressources dans la page Inventaire de NetApp Backup and Recovery . À ce stade, les ressources ne sont pas encore gérées par NetApp Backup and Recovery.

Une fois les ressources de l'hôte SnapCenter importées, NetApp Backup and Recovery ne prend pas en charge la gestion de la protection. Pour ce faire, vous devez choisir explicitement de gérer ces ressources dans NetApp Backup and Recovery.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Importer depuis SnapCenter**.
3. Sélectionnez **Importer depuis SnapCenter** pour importer les ressources SnapCenter .
4. Saisissez * les informations d'identification de l'application SnapCenter * :
   a. * Adresse FQDN ou IP de SnapCenter * : saisissez le FQDN ou l'adresse IP de l'application SnapCenter elle-même.
   b. **Port** : saisissez le numéro de port du serveur SnapCenter .

c. **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur SnapCenter .

d. **Agent de console** : sélectionnez l'agent de console pour SnapCenter.

5. Saisissez * les informations d'identification de l'hôte du serveur SnapCenter * :

a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Entrez le nom des informations d'identification.

b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter existantes, vous pouvez en ajouter de nouvelles. Saisissez le nom des informations d'identification, le mode d'authentification, le nom d'utilisateur et le mot de passe.

6. Sélectionnez **Importer** pour valider vos entrées et enregistrer le serveur SnapCenter .

Si le serveur SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche les ressources SnapCenter importées.

Gérer les ressources de l'hôte SnapCenter

Après avoir importé les ressources SnapCenter , gérez ces ressources hôtes dans NetApp Backup and Recovery. Une fois que vous avez choisi de gérer ces ressources importées, NetApp Backup and Recovery peut sauvegarder et récupérer les ressources que vous importez depuis SnapCenter. Vous n'avez plus besoin de gérer ces ressources dans SnapCenter Server.

Étapes

1. Après avoir importé les ressources SnapCenter , sur la page Inventaire qui s'affiche, sélectionnez les ressources SnapCenter que vous avez importées et que vous souhaitez que NetApp Backup and Recovery gère désormais.
2. Sélectionnez l'icône Actions ••• > **Gérer** pour gérer les ressources.
3. Sélectionnez **Gérer dans la NetApp Console**.

   La page Inventaire affiche **Géré** sous le nom d'hôte pour indiquer que les ressources d'hôte sélectionnées sont désormais gérées par NetApp Backup and Recovery.

Modifier les ressources SnapCenter importées

Vous pouvez ensuite réimporter les ressources SnapCenter ou modifier les ressources SnapCenter importées pour mettre à jour les détails d'enregistrement.

Vous ne pouvez modifier que les détails du port et du mot de passe pour le serveur SnapCenter .

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour **Importer depuis SnapCenter**.

   La page Importer depuis SnapCenter affiche toutes les importations précédentes.

3. Sélectionnez l'icône Actions ••• > **Modifier** pour mettre à jour les ressources.

4. Mettez à jour le mot de passe et les détails du port SnapCenter , si nécessaire.
5. Sélectionnez **Importer**.

Ajouter une plateforme de gestion KVM

Si vous utilisez la plateforme de gestion Apache CloudStack pour gérer les ressources KVM, vous devez l'intégrer à NetApp Backup and Recovery afin que ce dernier puisse détecter et protéger les hôtes et les machines virtuelles KVM gérés.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Plateforme de gestion**.
3. Sélectionnez **Ajouter les informations d'identification de la plateforme de gestion**.
4. Saisissez les informations suivantes :
   - **Adresse IP ou nom de domaine complet de la plateforme de gestion** : Saisissez l'adresse IP ou le nom de domaine complet de la plateforme de gestion.
   - **Clé API** : Saisissez la clé API à utiliser pour authentifier les requêtes API.
   - **Clé secrète** : Saisissez la clé secrète à utiliser pour authentifier les requêtes API.
   - **Port** : Saisissez le port à utiliser pour la communication entre la sauvegarde et la restauration et la plateforme de gestion.
   - **Agents** : Sélectionnez un agent de console à utiliser pour faciliter la communication entre la sauvegarde et la restauration et la plateforme de gestion.
5. Une fois terminé, sélectionnez **Ajouter**.

Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows

Avant de créer des stratégies pour les hôtes Windows, vous devez configurer les répertoires de journaux dans les instantanés pour les hôtes Windows. Les répertoires de journaux sont utilisés pour stocker les journaux générés pendant le processus de sauvegarde.

Étapes

1. Dans le menu NetApp Backup and Recovery , sélectionnez **Inventaire**.
2. Depuis la page Inventaire, sélectionnez une charge de travail, puis sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
3. Dans la page Détails de l'inventaire affichant Microsoft SQL Server, sélectionnez l'onglet Hôtes.
4. Depuis la page Détails de l'inventaire, sélectionnez un hôte et sélectionnez l'icône Actions ••• > **Configurer le répertoire des journaux**.
5. Parcourez ou entrez le chemin d'accès au répertoire du journal.
6. Sélectionnez **Enregistrer**.

Créer un modèle de hook d'exécution

Vous pouvez créer un modèle de hook d'exécution personnalisé que vous pouvez utiliser pour effectuer des actions avant ou après une opération de protection des données sur une application.

Les modèles que vous créez ici ne sont utilisables que lors de la protection des charges de travail Kubernetes.

Étapes

1. Dans la console, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Paramètres**.
3. Développez la section **Modèle de hook d'exécution**.
4. Sélectionnez **Créer un modèle de hook d'exécution**.
5. Entrez un nom pour le hook d'exécution.
6. Vous pouvez également choisir un type de hook. Par exemple, un hook post-restauration est exécuté une fois l'opération de restauration terminée.
7. Dans la zone de texte **Script**, saisissez le script shell exécutable que vous souhaitez exécuter dans le cadre du modèle de hook d'exécution. Vous pouvez également sélectionner **Télécharger le script** pour télécharger un fichier de script à la place.
8. Sélectionnez **Créer**.

   Une fois le modèle créé, il apparaît dans la liste des modèles dans la section **Modèle de hook d'exécution**.

Configurez le contrôle d'accès basé sur les rôles dans NetApp Backup and Recovery

Pour renforcer la sécurité et contrôler l'accès aux ressources, configurez le contrôle d'accès basé sur les rôles pour NetApp Backup and Recovery. La NetApp Console prend en charge le contrôle d'accès basé sur les rôles (RBAC) pour certaines charges de travail de Backup and Recovery. Vous pouvez attribuer des rôles d'administrateur ou de visionneur spécifiques à ces charges de travail. Les autres charges de travail qui ne prennent pas encore en charge le contrôle d'accès basé sur les rôles restent accessibles à tous les utilisateurs disposant de rôles Backup and Recovery jusqu'à ce que l'association au niveau du projet soit prise en charge.

Suivez ces étapes pour contrôler l'accès aux ressources de votre organisation. Apportez les modifications nécessaires dans la page **Administration > Identité et accès** du menu NetApp Console.

Ces étapes supposent que vous disposez du rôle Organization Admin dans la Console.

Étapes

1. Créez la structure du projet d'identité et de contrôle d'accès.

   En tant qu'administrateur de l'organisation, configurez le dossier Identity and access ainsi que la structure du projet où résideront les charges de travail.

2. Attribuez des rôles aux utilisateurs.

   a. Option principale :

      Ajoutez des utilisateurs à chaque projet désigné pour les charges de travail et attribuez-leur le rôle

approprié. Par exemple :

- **Organization admin** et **Backup and Recovery super admin** : Un utilisateur disposant de ces rôles peut voir toutes les ressources de toutes les organisations, découvrir les workloads Backup and Recovery et les affecter à des projets (par exemple, US East ou US West).
- **Folder or project admin** et **Backup and Recovery super admin** : Un utilisateur disposant de ces rôles ne peut voir que les ressources du dossier ou du projet pour lequel il dispose des autorisations, mais peut découvrir les workloads NetApp Backup and Recovery et les affecter à ce projet.

b. Option alternative :

Au lieu d'accorder à un utilisateur un accès complet d'administrateur Backup and Recovery, vous pouvez vous attribuer le rôle de super administrateur Backup and Recovery et découvrir directement les workloads.

3. Découvrez les charges de travail dans Backup and Recovery.

Les administrateurs de l'organisation, du dossier ou du projet découvrent les charges de travail disponibles et sélectionnent le projet approprié (par exemple, US East ou US West). Chaque charge de travail est automatiquement associée au projet sélectionné.

4. Ajouter des utilisateurs aux projets.

Les administrateurs d'organisation ou de dossier/projet ajoutent des utilisateurs de Console aux projets avec des workloads. Attribuez aux utilisateurs le rôle de viewer de l'Organization et un rôle de Backup and Recovery en fonction de leurs besoins d'accès. Les utilisateurs disposant du bon rôle de Backup and Recovery auront automatiquement accès aux nouveaux workloads dans ces projets.

Informations connexes

- "Découvrez la gestion des identités et des accès de la NetApp Console".
- "Rôles de NetApp Backup and Recovery dans la NetApp Console".