



Sécurité et chiffrement des données

Cloud Volumes ONTAP

NetApp
April 23, 2024

Sommaire

- Sécurité et chiffrement des données 1
 - Cryptage de volumes grâce aux solutions de cryptage NetApp 1
 - Gérez les clés avec le service de gestion des clés AWS 1
 - Gérez les clés avec Azure Key Vault 2
 - Gérez les clés à l'aide du service Cloud Key Management de Google 10
 - Renforcer la protection contre les attaques par ransomware 12

Sécurité et chiffrement des données

Cryptage de volumes grâce aux solutions de cryptage NetApp

Cloud Volumes ONTAP prend en charge NetApp Volume Encryption (NVE) et NetApp Aggregate Encryption (NAE). NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos conforme à la norme FIPS 140-2. ["En savoir plus sur ces solutions de cryptage"](#).

NVE et NAE sont pris en charge par un gestionnaire de clés externe.

Gérez les clés avec le service de gestion des clés AWS

Vous pouvez utiliser ["Service de gestion des clés \(KMS\) d'AWS"](#) Pour protéger vos clés de chiffrement ONTAP dans une application déployée par AWS.

La gestion des clés avec le KMS AWS peut être activée via l'interface de ligne de commandes ou l'API REST ONTAP.

Lorsque vous utilisez le KMS, notez que par défaut la LIF d'un SVM de données est utilisée pour communiquer avec le terminal de gestion des clés cloud. Un réseau de gestion des nœuds permet de communiquer avec les services d'authentification d'AWS. Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Avant de commencer

- Cloud Volumes ONTAP doit exécuter la version 9.12.0 ou ultérieure
- Vous devez avoir installé la licence Volume Encryption (VE) et
- Vous devez avoir installé la licence MTEKM (Multi-tenant Encryption Key Management).
- Vous devez être un administrateur de cluster ou de SVM
- Vous devez disposer d'un abonnement AWS actif



Vous pouvez uniquement configurer les clés d'un SVM de données.

Configuration

AWS

1. Vous devez créer un ["octroi"](#) Il s'agit de la clé KMS AWS qui sera utilisée par le rôle IAM gérant le chiffrement. Le rôle IAM doit inclure une politique permettant les opérations suivantes :
 - DescribeKey
 - Encrypt
 - DecryptPour créer une subvention, reportez-vous à la section ["Documentation AWS"](#).
2. ["Ajouter une règle au rôle IAM approprié."](#) La politique devrait soutenir le DescribeKey, Encrypt, et Decrypt exploitation.

Cloud Volumes ONTAP

1. Passez à votre environnement Cloud Volumes ONTAP.
2. Basculer vers le niveau de privilège avancé :
`set -privilege advanced`
3. Activer le gestionnaire de clés AWS :
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Lorsque vous y êtes invité, entrez la clé secrète.
5. Vérifiez que le KMS AWS a été correctement configuré :
`security key-manager external aws show -vserver svm_name`

Gérez les clés avec Azure Key Vault

Vous pouvez utiliser ["Azure Key Vault \(AKV\)"](#) Afin de protéger vos clés de chiffrement ONTAP dans une application déployée dans Azure.

AKV peut être utilisé pour protéger ["Clés NetApp Volume Encryption \(NVE\)"](#) Uniquement pour les SVM de données.

La gestion des clés via AKV peut être activée via l'interface de ligne de commande ou l'API REST ONTAP.

Lorsque vous utilisez AKV, notez que par défaut une LIF de SVM de données permet de communiquer avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur de cloud (login.microsoftonline.com). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Avant de commencer

- Cloud Volumes ONTAP doit exécuter la version 9.10.1 ou ultérieure
- Licence Volume Encryption (VE) installée (la licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp).
- Vous devez disposer d'une licence MT_EK_MGMT (Multi-tenant Encryption Key Management)
- Vous devez être un administrateur de cluster ou de SVM
- Un abonnement Active Azure

Limites

- AKV ne peut être configuré que sur un SVM de données
- NAE ne peut pas être utilisé avec AKV. NAE nécessite un serveur KMIP externe pris en charge.

Processus de configuration

La procédure décrite ci-dessus décrit comment enregistrer votre configuration Cloud Volumes ONTAP avec Azure et comment créer un coffre-fort de clés Azure et des clés. Si vous avez déjà effectué ces étapes, vérifiez que vous disposez des paramètres de configuration corrects, notamment dans [Créez un coffre-fort de clés Azure](#), puis passer à [Configuration Cloud Volumes ONTAP](#).

- [Inscription aux applications Azure](#)
- [Créez le secret du client Azure](#)

- [Créez un coffre-fort de clés Azure](#)
- [Créez une clé de chiffrement](#)
- [Création d'un terminal Azure Active Directory \(HA uniquement\)](#)
- [Configuration Cloud Volumes ONTAP](#)

Inscription aux applications Azure

1. Vous devez d'abord enregistrer votre application dans l'abonnement Azure que vous souhaitez que Cloud Volumes ONTAP utilise pour accéder au coffre-fort de clés Azure. Dans le portail Azure, sélectionnez **enregistrements d'applications**.
2. Sélectionnez **Nouvelle inscription**.
3. Indiquez un nom pour votre application et sélectionnez un type d'application pris en charge. Le locataire unique par défaut suffit pour l'utilisation d'Azure Key Vault. Sélectionnez **Enregistrer**.
4. Dans la fenêtre Présentation d'Azure, sélectionnez l'application que vous avez enregistrée. Copiez l'ID de l'application (client) **et l'ID du répertoire** (locataire)** dans un emplacement sécurisé. Elles seront requises plus tard dans le processus d'inscription.

Créez le secret du client Azure

1. Sur le portail Azure pour l'enregistrement de votre application Azure Key Vault, sélectionnez le volet **Certificats & secrets**.
2. Sélectionnez **Nouveau secret client**. Entrez un nom significatif pour votre secret client. NetApp recommande une période d'expiration de 24 mois. Cependant, vos règles de gouvernance cloud peuvent varier.
3. Cliquez sur **Ajouter** pour créer le secret client. Copiez la chaîne secrète répertoriée dans la colonne **valeur** et stockez-la dans un emplacement sécurisé pour une utilisation ultérieure dans [Configuration Cloud Volumes ONTAP](#). La valeur secrète ne s'affiche plus après avoir navigué loin de la page.

Créez un coffre-fort de clés Azure

1. Si vous disposez déjà d'un coffre-fort de clés Azure, vous pouvez le connecter à votre configuration Cloud Volumes ONTAP. Toutefois, vous devez adapter les règles d'accès aux paramètres de ce processus.
2. Dans le portail Azure, accédez à la section **Key Vaults**.
3. Cliquez sur **+Créer** et entrez les informations requises, notamment le groupe de ressources, la région et le niveau de prix. De plus, entrez le nombre de jours de conservation des coffres-forts supprimés et sélectionnez **Activer la protection de purge** sur le coffre-fort de clés.
4. Sélectionnez **Suivant** pour choisir une stratégie d'accès.
5. Sélectionnez les options suivantes :
 - a. Sous **Configuration d'accès**, sélectionnez la stratégie d'accès au coffre-fort **.
 - b. Sous **accès aux ressources**, sélectionnez **Azure Disk Encryption pour le chiffrement de volume**.
6. Sélectionnez **+Créer** pour ajouter une stratégie d'accès.
7. Sous **configurer à partir d'un modèle**, cliquez sur le menu déroulant, puis sélectionnez le modèle **Key, Secret et Certificate Management**.
8. Choisissez chacun des menus déroulants d'autorisations (clé, secret, certificat), puis **Sélectionner tout** en haut de la liste des menus pour sélectionner toutes les autorisations disponibles. Vous devez avoir :
 - **Autorisations clés** : 20 sélectionnées
 - **Autorisations secrètes** : 8 sélectionnées

- **Autorisations de certificat:** 16 sélectionné

Create an access policy



- 1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Cryptographic Operations

- ☒ Select all
- ☒ Decrypt
- ☒ Encrypt
- ☒ Unwrap Key
- ☒ Wrap Key
- ☒ Verify
- ☒ Sign

Privileged Key Operations

- ☒ Select all
- ☒ Purge
- ☒ Release

Rotation Policy Operations

- ☒ Select all
- ☒ Rotate
- ☒ Get Rotation Policy
- ☒ Set Rotation Policy

Secret permissions

Secret Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Set
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Privileged Secret Operations

- ☒ Select all
- ☒ Purge

Certificate permissions

Certificate Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore
- ☒ Manage Contacts
- ☒ Manage Certificate Authorities
- ☒ Get Certificate Authorities
- ☒ List Certificate Authorities
- ☒ Set Certificate Authorities
- ☒ Delete Certificate Authorities

Privileged Certificate Operations

- ☒ Select all
- ☒ Purge

Previous

Next

9. Cliquez sur **Suivant** pour sélectionner l'application **principal** Azure enregistrée dans [Inscription aux applications Azure](#). Sélectionnez **Suivant**.



Un seul principal peut être affecté par police.

Create an access policy

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Selected item

No item selected

Previous **Next**

10. Cliquez sur **Suivant** deux fois jusqu'à votre arrivée à **Revue et créer**. Cliquez ensuite sur **Créer**.
11. Sélectionnez **Suivant** pour passer aux options **mise en réseau**.
12. Choisissez la méthode d'accès au réseau appropriée ou sélectionnez **tous les réseaux** et **Revue + Créer** pour créer le coffre-fort de clés. (La méthode d'accès au réseau peut être prescrite par une gouvernance ou par votre équipe de sécurité cloud.)
13. Enregistrez l'URI du coffre-fort de clés : dans le coffre-fort de clés que vous avez créé, accédez au menu Aperçu et copiez l'URI du coffre-fort ** dans la colonne de droite. Vous en avez besoin pour une étape ultérieure.

Créez une clé de chiffrement

1. Dans le menu du coffre-fort de clés créé pour Cloud Volumes ONTAP, accédez à l'option **touches**.
2. Sélectionnez **générer/importer** pour créer une nouvelle clé.
3. Laissez l'option par défaut sur **générer**.
4. Fournissez les informations suivantes :

- Nom de la clé de chiffrement
- Type de clé : RSA
- Taille de la clé RSA : 2048
- Activé : Oui

5. Sélectionnez **Créer** pour créer la clé de cryptage.
6. Revenez au menu **touches** et sélectionnez la touche que vous venez de créer.
7. Sélectionnez l'ID de clé sous **version actuelle** pour afficher les propriétés de la clé.
8. Repérez le champ **Key identifier**. Copiez l'URI vers mais sans inclure la chaîne hexadécimale.

Création d'un terminal Azure Active Directory (HA uniquement)

1. Ce processus n'est requis que si vous configurez Azure Key Vault pour un environnement de travail Cloud Volumes ONTAP haute disponibilité.
2. Dans le portail Azure, accédez à **réseaux virtuels**.
3. Sélectionnez le réseau virtuel sur lequel vous avez déployé l'environnement de travail Cloud Volumes ONTAP et sélectionnez le menu **sous-réseaux** sur le côté gauche de la page.
4. Sélectionnez dans la liste le nom de sous-réseau de votre déploiement Cloud Volumes ONTAP.
5. Naviguez jusqu'à l'en-tête **points d'extrémité du service**. Dans le menu déroulant, sélectionnez les options suivantes :
 - **Microsoft.AzureActiveDirectory**
 - **Microsoft.KeyVault**
 - **Microsoft.Storage** (facultatif)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. Sélectionnez **Enregistrer** pour capturer vos paramètres.

Configuration Cloud Volumes ONTAP

1. Connectez-vous à la LIF de gestion du cluster avec votre client SSH préféré.
2. Entrez le mode de privilège avancé dans ONTAP :

```
set advanced -con off
```

3. Identifier le SVM de données souhaité et vérifier sa configuration DNS :

```
vserver services name-service dns show
```

- a. Si une entrée DNS pour le SVM de données souhaité existe et qu'elle contient une entrée pour le DNS Azure, aucune action n'est requise. Si ce n'est pas le cas, ajoutez une entrée de serveur DNS pour le SVM de données qui pointe vers le DNS Azure, le DNS privé ou le serveur sur site. Ceci doit correspondre à l'entrée pour le SVM admin du cluster :

```
vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address
```

- b. Vérifier que le service DNS a été créé pour le SVM de données :

```
vserver services name-service dns show
```

4. Activez le coffre-fort de clés Azure à l'aide de l'ID client et de l'ID locataire enregistrés après l'enregistrement de l'application :

```
security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI
```



Le `_full_key_URI` la valeur doit utiliser le `<https:// <key vault host name>/keys/<key label>` format.

5. Une fois Azure Key Vault correctement installé, entrez dans le `client secret value` lorsque vous y êtes invité.

6. Vérifier le statut du gestionnaire de clés :

`security key-manager external azure check` Le résultat sera le suivant :

```
::*> security key-manager external azure check
```

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekvip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

Si le `service_reachability` l'état n'est pas OK, La SVM ne peut pas atteindre le service Azure Key Vault avec toutes les connectivités et autorisations requises. Assurez-vous que vos stratégies réseau et votre routage Azure ne bloquent pas votre vnet privé d'atteindre le point de terminaison public Azure

KeyVault. Dans ce cas, envisagez d'utiliser un terminal privé Azure pour accéder au coffre-fort de clés à partir du vnet. Vous devrez peut-être aussi ajouter une entrée d'hôtes statiques sur votre SVM pour résoudre l'adresse IP privée de votre nœud final.

Le `kms_wrapped_key_status` rapports UNKNOWN lors de la configuration initiale. Son statut devient OK une fois le premier volume crypté.

7. FACULTATIF : créez un volume de test pour vérifier le fonctionnement de NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

S'il est correctement configuré, Cloud Volumes ONTAP crée automatiquement le volume et active le chiffrement de volume.

8. Confirmez que le volume a été créé et chiffré correctement. Si c'est le cas, le `-is-encrypted` le paramètre s'affiche comme `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

Gérez les clés à l'aide du service Cloud Key Management de Google

Vous pouvez utiliser "[Service de gestion des clés \(KMS cloud\) de Google Cloud Platform](#)" Pour protéger vos clés de chiffrement ONTAP dans une application déployée sur Google Cloud Platform.

La gestion des clés via le serveur Cloud KMS peut être activée via l'interface de ligne de commande ou l'API REST de ONTAP.

Lors de l'utilisation de Cloud KMS, notez que la LIF d'un SVM de données est utilisée par défaut pour communiquer avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur de cloud (`oauth2.googleapis.com`). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Avant de commencer

- Cloud Volumes ONTAP doit exécuter la version 9.10.1 ou ultérieure
- Licence VE (Volume Encryption) installée
- Licence MTEKM (Encryption Key Management) mutualisée installée, à partir de Cloud Volumes ONTAP 9.12.1 GA.
- Vous devez être un administrateur de cluster ou de SVM
- Un abonnement actif à Google Cloud Platform

Limites

- Cloud KMS peut uniquement être configuré sur un SVM de données

Configuration

Google Cloud

1. Dans votre environnement Google Cloud, "[Créez une clé et une clé GCP symétriques](#)".

2. Créez un rôle personnalisé pour votre compte de service Cloud Volumes ONTAP.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Attribuez le rôle personnalisé à la clé KMS cloud et au compte de service Cloud Volumes ONTAP :

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Télécharger la clé JSON du compte de service :

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. Connectez-vous à la LIF de gestion du cluster avec votre client SSH préféré.

2. Basculer vers le niveau de privilège avancé :

```
set -privilege advanced
```

3. Créer un DNS pour le SVM de données.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. Créer une entrée CMEK :

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

5. Lorsque vous y êtes invité, entrez la clé JSON de compte de service de votre compte GCP.

6. Confirmer que le processus activé a réussi :

```
security key-manager external gcp check -vserver svm_name
```

7. FACULTATIF : créez un volume pour tester le chiffrement vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G

Résoudre les problèmes

Si vous avez besoin d'effectuer un dépannage, vous pouvez consulter les journaux d'API REST bruts dans les deux dernières étapes ci-dessus :

1. set d

2. systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log

Renforcer la protection contre les attaques par ransomware









Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. BlueXP vous permet d'implémenter deux solutions NetApp pour les attaques par ransomware : protection contre les extensions de fichiers classiques et protection anti-ransomware autonome (ARP). Ces solutions fournissent des outils efficaces de visibilité, de détection et de résolution des problèmes.

Protection contre les extensions de fichiers ransomware courantes

Disponible via BlueXP, le paramètre de protection contre les ransomwares vous permet d'utiliser la fonctionnalité ONTAP FPolicy pour vous prémunir contre les types d'extension de fichiers ransomware courants.

Étapes

1. Sur la page Canvas, double-cliquez sur le nom du système que vous configurez pour la protection contre les ransomware.
2. Dans l'onglet vue d'ensemble, cliquez sur le panneau fonctionnalités, puis cliquez sur l'icône en forme de crayon en regard de **protection contre les ransomware**.

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access 	
Instance Type		m5.xlarge 
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration		Not Registered 
CIFs Setup		

3. Implémentez la solution NetApp en cas d'attaque par ransomware :

- Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

La technologie Snapshot de NetApp offre la meilleure solution du secteur pour résoudre les problèmes liés aux attaques par ransomware. Le mieux pour réussir la récupération est d'effectuer une restauration à partir de sauvegardes non infectées. Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

- b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations de fichiers en fonction de l'extension d'un fichier.

Cette solution préventive améliore la protection contre les attaques par ransomware en bloquant les types de fichiers généralement utilisés.

Les fichiers de blocs d'étendue FPolicy par défaut qui possèdent les extensions suivantes :

micro, chiffré, verrouillé, crypto, crypt, Crinf, r5a, XRNT, XTBL, R16M01D05, Pzdc, Good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, enciphed, LeChiffre



BlueXP crée ce périmètre lorsque vous activez FPolicy sur Cloud Volumes ONTAP. La liste est basée sur les types de fichiers ransomware les plus courants. Vous pouvez personnaliser les extensions de fichiers bloqués en utilisant les commandes `vserver fpolicy policy scope` à partir de l'interface de ligne de commande Cloud Volumes ONTAP.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

Protection autonome contre les ransomwares

Cloud Volumes ONTAP prend en charge la fonctionnalité de protection anti-ransomware autonome (ARP), qui effectue des analyses sur les workloads pour détecter de manière proactive les activités anormales et vous avertir d'une attaque de ransomware.

Séparer des protections d'extension de fichier fournies par le "[paramètre de protection contre les ransomware](#)", La fonction ARP utilise l'analyse de la charge de travail pour alerter l'utilisateur sur les attaques potentielles en fonction de l'activité anormale détectée. Vous pouvez combiner la configuration de protection contre les ransomware et la fonctionnalité ARP pour bénéficier d'une protection complète contre les ransomware.

La fonctionnalité ARP est disponible uniquement pour les licences BYOL (d'une durée de 1 à 36 mois), sur les modèles de licence basés sur les nœuds et la capacité. Vous devez contacter votre représentant commercial NetApp pour acheter une nouvelle licence d'extension séparée à utiliser avec la fonctionnalité ARP de Cloud

Volumes ONTAP.

La licence ARP est considérée comme une licence « flottante », ce qui signifie qu'elle n'est pas liée à une seule instance Cloud Volumes ONTAP et peut être appliquée à plusieurs environnements Cloud Volumes ONTAP.



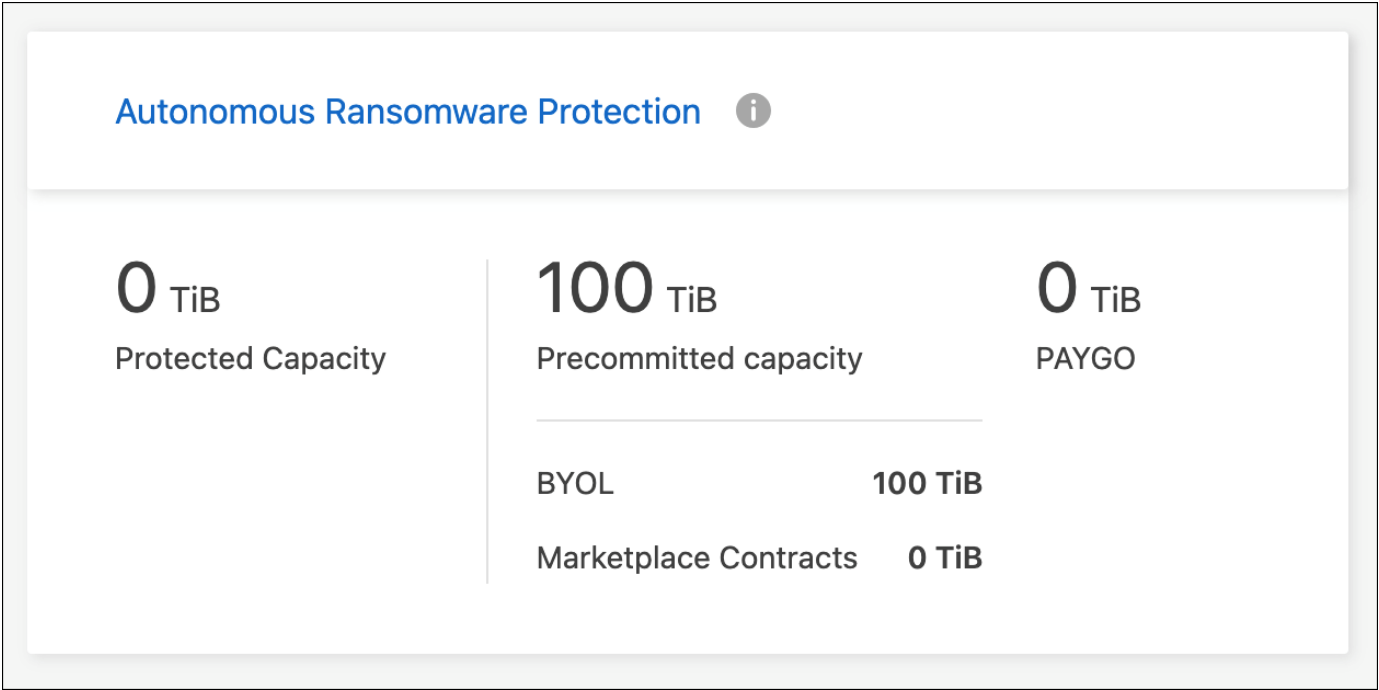
L'utilisation de la fonction ARP avec les licences Cloud Volumes ONTAP basées sur les nœuds n'est pas actuellement reflétée dans le portefeuille digital. La possibilité d'afficher l'utilisation du protocole ARP basé sur les nœuds sera disponible dans une prochaine version sous le portefeuille digital.

Lors de l'achat d'une licence complémentaire et de son ajout au portefeuille digital, vous pouvez activer le protocole ARP par volume avec Cloud Volumes ONTAP. Le chargement du protocole ARP est mesuré au niveau du volume, en fonction de la capacité totale provisionnée des volumes pour lesquels la fonctionnalité ARP est activée. La capacité minimale de licence est de 1 To. Cependant, il n'y a pas de charge de capacité minimale pour la fonction ARP.

Les volumes ARP activés ont un état désigné « mode apprentissage » ou « actif ». Tout volume dont l'état ARP est « désactivé » est exclu de la charge. Par exemple, un environnement Cloud Volumes ONTAP avec 30 Tio de capacité provisionnée peut choisir d'avoir uniquement un sous-ensemble de volumes de 15 Tio avec ARP activé.

La configuration du protocole ARP pour les volumes s'effectue via ONTAP System Manager et l'interface de ligne de commande ONTAP.

Pour plus d'informations sur l'activation d'ARP avec ONTAP System Manager et l'interface de ligne de commande, reportez-vous à la section "[Activation de la protection autonome contre les ransomwares](#)".



L'assistance n'est pas disponible pour l'utilisation des fonctions sous licence sans licence.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.