



Sécurité et chiffrement des données

Cloud Volumes ONTAP

NetApp

January 04, 2023

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-cloud-volumes-ontap/gcp/task-encrypting-volumes.html> on January 04, 2023. Always check docs.netapp.com for the latest.

Table des matières

- Sécurité et chiffrement des données 1
 - Cryptage de volumes grâce aux solutions de cryptage NetApp 1
 - Gérez les clés à l’aide du service Cloud Key Management de Google 1
 - Renforcer la protection contre les attaques par ransomware 3

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.

NAE est activé sur les nouveaux agrégats par défaut après avoir configuré un gestionnaire de clés externe. NVE est activé par défaut sur les nouveaux volumes qui ne font pas partie d'un agrégat NAE (par exemple, si des agrégats existants ont été créés avant de configurer un gestionnaire de clés externe).

Cloud Volumes ONTAP ne prend pas en charge la gestion intégrée des clés.

Ce dont vous avez besoin

Votre système Cloud Volumes ONTAP doit être enregistré auprès du support NetApp. Une licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp.

- ["Ajout de comptes du site de support NetApp à BlueXP"](#)
- ["Enregistrement des systèmes de paiement à l'utilisation"](#)



BlueXP n'installe pas la licence NVE sur les systèmes qui résident dans la région Chine.

Étapes

1. Consultez la liste des gestionnaires de clés pris en charge dans le ["Matrice d'interopérabilité NetApp"](#).



Recherchez la solution **gestionnaires de clés**.

2. ["Connectez-vous à l'interface de ligne de commandes de Cloud Volumes ONTAP"](#).
3. Configurez la gestion externe des clés.
 - Google Cloud : ["Service Google Cloud Key Management"](#)

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.

Lorsque vous utilisez le KMS, notez que, par défaut, une LIF de data SVM est utilisée 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.

Prérequis

- Cloud Volumes ONTAP doit exécuter la version 9.10.1 ou ultérieure
- Licence VE (Volume Encryption) installée
- 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 :

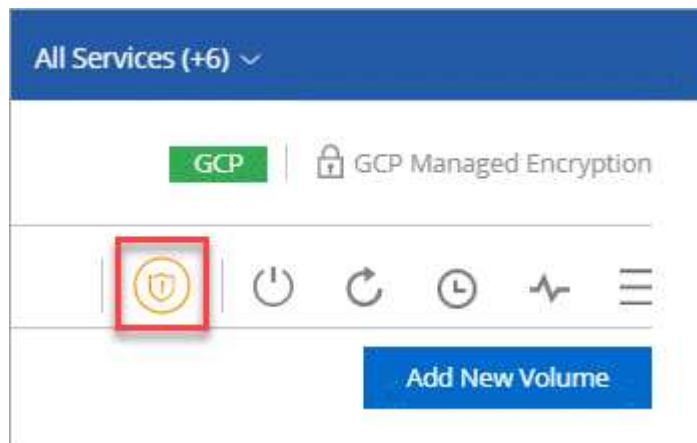
1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

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 la solution NetApp pour ransomware. Elle fournit des outils efficaces pour la visibilité, la détection et la résolution de problèmes.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **ransomware**.



2. Implémentez la solution NetApp en cas d'attaque par ransomware :
 - a. 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

Informations sur le copyright

Copyright © 2022 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.