Sécurité et chiffrement des données

Cloud Volumes ONTAP

NetApp
December 09, 2022

Table des matières

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.
   - AWS : "Pour obtenir des instructions, consultez la documentation ONTAP"
     - Azure : "Azure Key Vault (AKV)"
     - Google Cloud : "Service Google Cloud Key Management"

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.

Prérequis

- 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).
- Licence MTEKM (Multi-tenant Encryption Key Management) installée
- 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

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. Dans le portail Azure de votre application Cloud Volumes ONTAP, sélectionnez le volet **Ceritificats & secrets**.
2. Sélectionnez **Nouveau secret client** Entrez un nom significatif pour votre secret client. NetApp recommande une période d'expiration de 24 mois. Toutefois, vos règles de gouvernance cloud peuvent nécessiter un paramétrage différent.

3. Sélectionnez **Ajouter** pour enregistrer le secret client. Copiez immédiatement la valeur ** du secret et stockez-la quelque part en toute sécurité pour une configuration future. La valeur secrète ne s'affiche pas lorsque vous vous éloignez 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, mais vous devez adapter les règles d'accès aux paramètres de ce processus.
2. Dans le portail Azure, accédez à la section **Key Vaults**.
3. Sélectionnez **Créer**. Entrez les informations requises, y compris le groupe de ressources, la région et le niveau de prix, et effectuez des sélections pour les jours de conservation des coffres-forts supprimés et si la protection de purge est activée ou non. Les valeurs par défaut sont suffisantes pour cette configuration. Toutefois, vos règles de gouvernance de cloud peuvent nécessiter des paramètres différents.
4. Sélectionnez **Suivant** pour choisir une stratégie d'accès.
5. Sélectionnez **chiffrement de disque Azure** pour l'option de chiffrement de volume et **politique d'accès au coffre-fort** pour le modèle d'autorisation.
6. Sélectionnez **Ajouter une stratégie d'accès**.
7. Sélectionnez le point adjacent au champ **configurer à partir du modèle (facultatif)**. Sélectionnez ensuite **Key, Secret, & Certification 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** : 19 sélectionnées
   - **Autorisations secrètes**: 8 sélectionnées
   - **Autorisations de certificat**: 16 sélectionné
9. Sélectionnez **Ajouter** pour créer la stratégie d'accès.
10. Sélectionnez **Suivant** pour passer aux options **mise en réseau**.
11. 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.)
12. 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 aurez 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 **Microsoft.AzureActiveDirectory** dans la liste.
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` *`Azure_key_name`* `-key-id` *`Azure_key_ID`*
5. Vérifiez la configuration du gestionnaire de clés :
   `security key-manager external azure show`
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: ekmip_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. 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.

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
- Licence MTEKM (Multi-tenant Encryption Key Management) 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 queue 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.