# Chiffrement des données de volume avec NVE

ONTAP 9

NetApp
April 24, 2024

# Sommaire

# Chiffrement des données de volume avec NVE

## Chiffrement des données de volume avec NVE

Depuis ONTAP 9.7, le chiffrement de l'agrégat et du volume est activé par défaut lorsque vous disposez de la licence VE et de la gestion intégrée ou externe des clés. Pour ONTAP 9.6 et version antérieure, vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant. Vous devez avoir installé la licence VE et activé la gestion des clés avant de pouvoir activer le chiffrement de volume. NVE est conforme à la norme FIPS-140-2 de niveau 1.

## Chiffrement au niveau de l'agrégat avec licence VE

Depuis la version ONTAP 9.7, les nouveaux agrégats et volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE" et une gestion intégrée ou externe des clés. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes.

#### Description de la tâche

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Un agrégat activé pour le chiffrement au niveau de l'agrégat est appelé agrégat *NAE* (pour le chiffrement d'agrégat NetApp). Tous les volumes d'un agrégat NAE doivent être chiffrés avec un chiffrement NAE ou NVE. Grâce au chiffrement au niveau des agrégats, les volumes que vous créez dans l'agrégat sont chiffrés avec un chiffrement NAE par défaut. Vous pouvez remplacer le par défaut pour utiliser le chiffrement NVE.

Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

#### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

#### Étapes

1. Activer ou désactiver le chiffrement au niveau des agrégats :

| Pour… | Utilisez cette commande… |
|---|---|
| Créez un agrégat NAE avec ONTAP 9.7 ou version ultérieure | `storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* |
| Créez un agrégat NAE avec ONTAP 9.6 | `storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true` |

| | |
|---|---|
| Conversion d'un agrégat non-NAE en agrégat NAE | `storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true` |
| Conversion d'un agrégat NAE en agrégat non-NAE | `storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false` |

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

La commande suivante active le chiffrement au niveau de l'agrégat sur `aggr1`:

- ONTAP 9.7 ou version ultérieure :

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou version antérieure :

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Vérifier que l'agrégat est activé pour le chiffrement :

   `storage aggregate show -fields encrypt-with-aggr-key`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante vérifie que `aggr1` est activé pour le chiffrement :

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

**Une fois que vous avez terminé**

Exécutez le `volume create` commande permettant de créer les volumes chiffrés.

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

# Activer le chiffrement sur un nouveau volume

Vous pouvez utiliser le `volume create` commande permettant d'activer le chiffrement sur un nouveau volume.

**Description de la tâche**

Vous pouvez chiffrer les volumes à l'aide de NetApp Volume Encryption (NVE) et, à partir de ONTAP 9.6, NetApp Aggregate Encryption (NAE). Pour en savoir plus sur NAE et NVE, consultez le présentation du chiffrement de volume.

La procédure d'activation du chiffrement sur un nouveau volume dans ONTAP varie en fonction de la version de ONTAP que vous utilisez et de votre configuration spécifique :

- À partir de ONTAP 9.4, si vous l'activez `cc-mode` Lorsque vous configurez le gestionnaire de clés intégré, les volumes que vous créez avec le `volume create` la commande est automatiquement chiffrée, que vous spécifiez ou non `-encrypt true`.
- Dans ONTAP 9.6 et les versions antérieures, vous devez utiliser `-encrypt true` avec `volume create` commandes permettant d'activer le chiffrement (à condition que vous n'ayez pas activé `cc-mode`).
- Si vous voulez créer un volume NAE dans ONTAP 9.6, vous devez activer NAE au niveau des agrégats. Reportez-vous à la section Activation du chiffrement au niveau de l'agrégat avec la licence VE pour plus de détails sur cette tâche.
- Depuis la version ONTAP 9.7, les nouveaux volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE" et une gestion intégrée ou externe des clés. Par défaut, les nouveaux volumes créés dans un agrégat NAE seront de type NAE plutôt que NVE.
  - Dans ONTAP 9.7 et versions ultérieures, si vous ajoutez `-encrypt true` à la `volume create` Commande de création d'un volume dans un agrégat NAE, au lieu de NAE pour le volume le chiffrement NVE. Tous les volumes d'un agrégat NAE doivent être chiffrés avec NVE ou NAE.

> Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

**Étapes**

1. Créez un nouveau volume et spécifiez si le chiffrement est activé sur le volume. Si le nouveau volume se trouve dans un agrégat NAE, le volume en est par défaut un volume NAE :

| Pour créer… | Utilisez cette commande… |
|---|---|
| Volume NAE | `volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* |
| Un volume NVE | `volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true`<br><br>Dans les versions ONTAP 9.6 et antérieures, où NAE n'est pas pris en charge, `-encrypt true` Spécifie que le volume doit être chiffré avec NVE. Dans ONTAP 9.7 et versions ultérieures, où les volumes sont créés dans des agrégats NAE, `-encrypt true` Remplace le type de chiffrement par défaut de NAE pour créer un volume NVE. |

| | |
|---|---|
| Volume de texte brut | `volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false` |

Pour obtenir la syntaxe complète de la commande, reportez-vous à la page de référence de la commande LINK:https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[`volume create`^].

2. Vérifiez que les volumes sont activés pour le chiffrement :

   `volume show -is-encrypted true`

   Pour connaître la syntaxe complète de la commande, reportez-vous au "référence de commande".

**Résultat**

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP « transmet automatiquement » une clé de chiffrement au serveur lorsque vous chiffrez un volume.

= :allow-uri-read:

# Activez le chiffrement sur un volume existant

Vous pouvez utiliser le `volume move start` ou le `volume encryption conversion start` commande permettant d'activer le chiffrement sur un volume existant.

**Description de la tâche**

- Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement. Vous pouvez également utiliser le `volume move start` commande.
- Pour ONTAP 9.2 et les versions antérieures, vous pouvez utiliser uniquement le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant.

## Activez le chiffrement sur un volume existant à l'aide de la commande Volume Encryption conversion start

Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement.

Une fois que vous avez lancé une opération de conversion, elle doit être terminée. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption conversion pause` commande pour mettre l'opération en pause, et le `volume encryption conversion resume` commande pour reprendre l'opération.

> Vous ne pouvez pas utiliser `volume encryption conversion start` Pour convertir un volume SnapLock.

**Étapes**

1. Activer le chiffrement sur un volume existant :

`volume encryption conversion start -vserver SVM_name -volume volume_name`

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante active le chiffrement sur un volume existant `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

Le système crée une clé de chiffrement pour le volume. Les données du volume sont chiffrées.

2. Vérifiez l'état de l'opération de conversion :

   `volume encryption conversion show`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche le statut de l'opération de conversion :

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

**Résultat**

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

## Activez le chiffrement sur un volume existant à l'aide de la commande volume Move start

Vous pouvez utiliser le `volume move start` commande permettant d'activer le chiffrement en déplaçant un

volume existant. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Vous pouvez utiliser le même agrégat ou un autre agrégat.

**Description de la tâche**

- Vous pouvez utiliser ONTAP 9.8 depuis `volume move start` Pour activer le chiffrement sur un volume SnapLock ou FlexGroup.
- Depuis ONTAP 9.4, si vous activez « cc-mode » lors de la configuration du gestionnaire de clés intégré, les volumes que vous créez avec le système `volume move start` la commande est automatiquement chiffrée. Vous n'avez pas besoin de spécifier `-encrypt-destination true`.
- Depuis ONTAP 9.6, il est possible d'utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de déplacer les volumes. Un volume chiffré avec une clé unique est appelé *volume NVE* (ce qui signifie qu'il utilise le chiffrement de volume NetApp). Un volume chiffré avec une clé au niveau de l'agrégat est appelé un volume NAE_ (pour le chiffrement d'agrégat NetApp). Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.
- À partir de ONTAP 9.14.1, vous pouvez chiffrer un volume root SVM avec NVE. Pour plus d'informations, voir Configurer le chiffrement de volume NetApp sur un volume root SVM.

**Avant de commencer**

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

**Étapes**

1. Déplacez un volume existant et spécifiez si le chiffrement est activé sur le volume :

| Pour convertir… | Utilisez cette commande… |
|---|---|
| Volume en texte brut vers un volume NVE | `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true` |
| Un volume NVE ou en texte clair vers un volume NAE (en supposant que le chiffrement au niveau de l'agrégat est activé sur la destination) | `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true` |
| Un volume NAE vers un volume NVE | `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false` |
| Volume NAE en volume en texte brut | `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false` |

| | |
|---|---|
| Un volume NVE vers un volume en texte brut | `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false` |

Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante convertit un volume en texte brut nommé `vol1` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

En supposant que le chiffrement au niveau de l'agrégat soit activé sur la destination, la commande suivante convertit un volume NVE ou en texte brut nommé `vol1` Pour un volume NAE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

La commande suivante convertit un volume NAE nommé `vol2` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NAE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NVE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Afficher le type de chiffrement des volumes du cluster :

   `volume show -fields encryption-type none|volume|aggregate`

   Le `encryption-type` Ce champ est disponible dans ONTAP 9.6 et versions ultérieures.

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche le type de cryptage des volumes dans `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Vérifiez que les volumes sont activés pour le chiffrement :

   `volume show -is-encrypted true`

   Pour la syntaxe complète de la commande, reportez-vous à la page man de la commande.

   La commande suivante affiche les volumes chiffrés sur `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

**Résultat**

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP transmet automatiquement une clé de chiffrement au serveur lorsque vous chiffrez un volume.

# Configurer le chiffrement de volume NetApp sur un volume root SVM

À partir de la version ONTAP 9.14.1, vous pouvez activer NetApp Volume Encryption (NVE) sur un volume racine de machine virtuelle de stockage (SVM). Avec NVE, le volume racine est chiffré avec une clé unique, pour renforcer la sécurité au niveau du SVM.

**Description de la tâche**

NVE sur un volume root SVM ne peut être activé qu'une fois le SVM créé.

**Avant de commencer**

- Le volume racine du SVM ne doit pas se trouver sur un agrégat chiffré avec le chiffrement d'agrégat NetApp (NAE).
- Vous devez avoir activé le chiffrement avec Onboard Key Manager ou un gestionnaire de clés externe.
- Vous devez exécuter ONTAP 9.14.1 ou une version ultérieure.
- Pour migrer un SVM contenant un volume racine chiffré avec NVE, vous devez convertir le volume racine du SVM en volume texte brut une fois la migration terminée, puis re-chiffrer le volume racine du SVM.

    - Si l'agrégat de destination de la migration du SVM utilise NAE, le volume racine hérite de NAE par défaut.
- Si la SVM est dans une relation de SVM DR :
    - Les paramètres de chiffrement d'un SVM en miroir ne sont pas copiés vers la destination. Si vous activez NVE sur la source ou la destination, vous devez activer NVE séparément sur le volume racine du SVM en miroir.
    - Si tous les agrégats du cluster de destination utilisent NAE, le volume racine du SVM utilisera NAE.

**Étapes**

Vous pouvez activer NVE sur un volume root SVM via l'interface de ligne de commandes ONTAP ou System Manager.

**CLI**

Vous pouvez activer NVE sur le volume racine du SVM sans déplacement ou en déplaçant le volume entre les agrégats.

**Chiffrez le volume racine sur place**

1. Convertir le volume root en volume chiffré :

   `volume encryption conversion start -vserver` *`svm_name`* `-volume` *`volume`*

2. Confirmez que le chiffrement a réussi. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

**Chiffrer le volume root du SVM en le déplaçant**

1. Lancer un déplacement de volume :

   `volume move start -vserver` *`svm_name`* `-volume` *`volume`* `-destination-aggregate` *`aggregate`* `-encrypt-with-aggr-key false -encrypt-destination true`

   Pour plus d'informations sur `volume move`, voir Déplacer un volume.

2. Confirmez le `volume move` l'opération a réussi avec le `volume move show` commande. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

**System Manager**

1. Accédez à **stockage** > **volumes**.
2. En regard du nom du volume root du SVM à chiffrer, sélectionner ⋮ Puis **Modifier**.
3. Sous l'en-tête **stockage et optimisation**, sélectionnez **Activer le cryptage**.
4. Sélectionnez **Enregistrer**.

# Activer le chiffrement de volume racine de nœud

Depuis ONTAP 9.8, vous pouvez utiliser NetApp Volume Encryption pour protéger le volume racine de votre nœud.

**Description de la tâche**

Cette procédure s'applique au volume racine du nœud. Elle ne s'applique pas aux volumes root du SVM. Les volumes root des SVM peuvent être protégés via le chiffrement au niveau des agrégats et À partir de ONTAP 9.14.1, NVE.

Une fois le chiffrement du volume racine démarré, il doit être terminé. Vous ne pouvez pas interrompre l'opération. Une fois le cryptage terminé, vous ne pouvez pas attribuer de nouvelle clé au volume racine et vous ne pouvez pas effectuer de suppression sécurisée.

**Avant de commencer**

- Votre système doit utiliser une configuration haute disponibilité.
- Le volume racine du nœud doit déjà être créé.
- Votre système doit disposer d'un gestionnaire de clés intégré ou d'un serveur de gestion des clés externe à l'aide du protocole KMIP (Key Management Interoperability Protocol).

**Étapes**

1. Chiffrer le volume root :

   `volume encryption conversion start -vserver SVM_name -volume root_vol_name`

2. Vérifiez l'état de l'opération de conversion :

   `volume encryption conversion show`

3. Une fois l'opération de conversion terminée, vérifiez que le volume est crypté :

   `volume show -fields`

   Voici un exemple de sortie pour un volume chiffré.

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver    volume is-encrypted
---------- ------ ------------
xyz        vol0   true
```