Sécurisez votre réseau

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/networking/configure_network_security_using_federal_information_processing_standards_fips.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Sécurisez votre réseau . . . 1
- Configurez la sécurité réseau ONTAP à l'aide de FIPS pour toutes les connexions SSL . . . 1
  - Activez FIPS . . . 2
  - Désactivez FIPS . . . 3
  - Affichez l'état de conformité FIPS . . . 3
- Configurer le chiffrement IPsec en vol . . . 4
  - Préparez-vous à utiliser la sécurité IP sur le réseau ONTAP . . . 4
  - Configurer la sécurité IP pour le réseau ONTAP . . . 8
- Configurer le chiffrement du réseau du cluster backend ONTAP . . . 13
  - Activer ou désactiver le chiffrement pour la communication réseau du cluster . . . 14
  - Gérer les certificats de chiffrement du réseau du cluster . . . 14
- Configuration des politiques de pare-feu pour les LIF du réseau ONTAP . . . 15
  - Politiques de pare-feu et LIF . . . 16
  - Configuration du service portmap . . . 17
  - Créer une politique de pare-feu et l'affecter à une LIF . . . 18
- Commandes ONTAP pour gérer le service et les politiques de pare-feu . . . 21

Sécurisez votre réseau

Configurez la sécurité réseau ONTAP à l'aide de FIPS pour toutes les connexions SSL

ONTAP est conforme aux normes fédérales de traitement de l'information (FIPS) 140-2 pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir les protocoles SSL globalement et désactiver les chiffrements faibles dans ONTAP.

Par défaut, SSL sur ONTAP est défini avec la conformité FIPS désactivée et les protocoles TLS suivants activés :

- TLSv1.3 (à partir de ONTAP 9.11.1)
- TLSv1.2

Les protocoles TLS suivants étaient activés par défaut dans les versions précédentes de ONTAP :

- TLSv1.1 (désactivé par défaut à partir de ONTAP 9.12.1)
- TLSv1 (désactivé par défaut à partir de ONTAP 9.8)

Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.

Si vous souhaitez que les comptes d'administrateur accèdent aux SVM avec une clé publique SSH, vous devez vous assurer que l'algorithme de clé hôte est pris en charge avant d'activer le mode SSL FIPS.

Remarque : la prise en charge de l'algorithme de clé hôte a changé dans ONTAP 9.11.1 et versions ultérieures.

Version de ONTAP	Types de clés pris en charge	Types de clés non pris en charge
9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge doivent être reconfigurés avec un type de clé pris en charge avant l'activation de FIPS, sinon l'authentification de l'administrateur échoue.

Pour plus d'informations, voir "Activez les comptes de clé publique SSH".

ONTAP 9.18.1 introduit la prise en charge des algorithmes cryptographiques post-quantiques ML-KEM, ML-DSA et SLH-DSA pour SSL, offrant une couche de sécurité supplémentaire contre les futures attaques

potentielles d'ordinateurs quantiques. Ces algorithmes ne sont disponibles que lorsqueLe système FIPS est désactivé. . Les algorithmes cryptographiques post-quantiques sont négociés lorsque FIPS est désactivé et que le pair les prend en charge.

Activez FIPS

Il est recommandé que tous les utilisateurs sécurisés ajustent leur configuration de sécurité immédiatement après l'installation ou la mise à niveau du système. Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.

Lorsque FIPS est activé, vous ne pouvez ni installer ni créer de certificat avec une clé RSA d'une longueur de 4096.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Activer FIPS :

   ```
   security config modify * -is-fips-enabled true
   ```

3. Lorsque vous êtes invité à continuer, entrez `y`
4. À partir d' ONTAP 9.9.1, le redémarrage n'est pas nécessaire. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster un par un.

Exemple

Si vous exécutez ONTAP 9.9.1 ou une version ultérieure, le message d'avertissement ne s'affiche pas.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Pour en savoir plus sur `security config modify` la configuration du mode SSL FIPS et sur le "Référence de commande ONTAP".

Désactivez FIPS

À partir d' ONTAP 9.18.1, SSL dans ONTAP prend en charge les algorithmes cryptographiques post-quantiques ML-KEM, ML-DSA et SLH-DSA. Ces algorithmes ne sont disponibles que lorsque FIPS est désactivé et que le système homologue les prend en charge.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Désactiver FIPS en tapant :

   ```
   security config modify -is-fips-enabled false
   ```

3. Lorsque vous êtes invité à continuer, entrez `y`.
4. À partir d' ONTAP 9.9.1, le redémarrage n'est pas nécessaire. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster.

Si vous devez utiliser le protocole SSLv3, vous devez désactiver FIPS en suivant la procédure ci-dessus. SSLv3 ne peut être activé que lorsque FIPS est désactivé.

Vous pouvez activer SSLv3 avec la commande suivante. Si vous utilisez ONTAP 9.9.1 ou une version ultérieure, vous ne verrez pas le message d'avertissement.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Affichez l'état de conformité FIPS

Vous pouvez vérifier si le cluster entier exécute les paramètres de configuration de sécurité actuels.

Étapes

1. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster un par un.
2. Afficher le statut de conformité actuel :

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

Pour en savoir plus, `security config show` consultez le "Référence de commande ONTAP".

Informations associées

- "FIPS 203 : Norme relative au mécanisme d'encapsulation de clés basé sur un réseau de modules (ML-KEM)"
- "FIPS 204 : Norme de signature numérique basée sur un réseau de modules (ML-DSA)"
- "FIPS 205 : Norme de signature numérique sans état basée sur le hachage (SLH-DSA)"

Configurer le chiffrement IPsec en vol

Préparez-vous à utiliser la sécurité IP sur le réseau ONTAP

À partir de ONTAP 9.8, vous avez la possibilité d'utiliser la sécurité IP (IPSec) pour protéger votre trafic réseau. IPSec est l'une des nombreuses options de chiffrement de données en mouvement ou à la volée disponibles avec ONTAP. Vous devez vous préparer à configurer IPsec avant de l'utiliser dans un environnement de production.

Mise en œuvre de la sécurité IP dans ONTAP

IPSec est une norme Internet gérée par l'IETF. Il assure le cryptage et l'intégrité des données ainsi que l'authentification du trafic circulant entre les terminaux réseau au niveau IP.

Avec ONTAP, IPSec sécurise l'ensemble du trafic IP entre ONTAP et les différents clients, notamment les protocoles NFS, SMB et iSCSI. En plus de la confidentialité et de l'intégrité des données, le trafic réseau est protégé contre plusieurs attaques, telles que les attaques par réexécution et les attaques de l'homme du milieu. ONTAP utilise l'implémentation du mode de transport IPsec. Il s'appuie sur le protocole Internet Key Exchange (IKE) version 2 pour négocier le matériel clé entre ONTAP et les clients utilisant IPv4 ou IPv6.

Lorsque la fonctionnalité IPSec est activée sur un cluster, le réseau requiert une ou plusieurs entrées de la base de données SPD (Security Policy Database) de ONTAP correspondant aux différentes caractéristiques de trafic. Ces entrées sont mappées aux détails de protection spécifiques nécessaires au traitement et à l'envoi des données (par exemple, suite de chiffrement et méthode d'authentification). Une entrée SPD correspondante est également nécessaire pour chaque client.

Pour certains types de trafic, une autre option de chiffrement des données en mouvement peut être préférable. Par exemple, pour le chiffrement du trafic NetApp SnapMirror et de peering de cluster, le protocole TLS (transport Layer Security) est généralement recommandé à la place d'IPsec. En effet, TLS offre de meilleures performances dans la plupart des situations.

Informations associées

- "Internet Engineering Task Force"
- "RFC 4301 : Architecture de sécurité pour le protocole Internet"

Évolution de l'implémentation ONTAP IPsec

IPsec a été introduit pour la première fois avec ONTAP 9.8. Son implémentation a continué d'évoluer dans les versions ultérieures ONTAP , comme décrit ci-dessous.

ONTAP 9.18.1

La prise en charge du déchargement matériel IPsec est étendue au trafic IPv6.

ONTAP 9.17.1

La prise en charge du déchargement matériel IPsec est étendue à "groupes d'agrégation de liens" . "Clés pré-partagées postquantiques (PPK)" sont pris en charge pour l'authentification par clés pré-partagées IPsec (PSK).

ONTAP 9.16.1

Plusieurs opérations cryptographiques, telles que le cryptage et les contrôles d'intégrité, peuvent être déchargées sur une carte NIC prise en charge. Voir Fonctionnalité de déchargement matériel IPsec pour plus d'informations.

ONTAP 9.12.1

La prise en charge du protocole hôte IPSec frontal est disponible dans les configurations MetroCluster IP et MetroCluster FAS. La prise en charge IPsec fournie avec les clusters MetroCluster est limitée au trafic hôte frontal et n'est pas prise en charge sur les LIF intercluster MetroCluster.

ONTAP 9.10.1

Les certificats peuvent être utilisés pour l'authentification IPsec en plus des clés PSK. Avant ONTAP 9.10.1, seules les clés PSK étaient prises en charge pour l'authentification.

ONTAP 9.9.1

Les algorithmes de chiffrement utilisés par IPsec sont validés par la norme FIPS 140-2-2. Ces algorithmes sont traités par le module cryptographique NetApp de ONTAP, qui est certifié FIPS 140-2-2.

ONTAP 9.8

La prise en charge d'IPsec devient initialement disponible en fonction de l'implémentation du mode de transport.

Fonctionnalité de déchargement matériel IPsec

Si vous utilisez ONTAP 9.16.1 ou une version ultérieure, vous avez la possibilité de transférer certaines opérations à forte intensité de calcul, telles que le cryptage et les contrôles d'intégrité, vers une carte de contrôleur d'interface réseau (NIC) installée sur le nœud de stockage. Le débit pour les opérations déchargées sur la carte NIC est d'environ 5 % ou moins. Cela peut considérablement améliorer les performances et le débit du trafic réseau protégé par IPsec.

Exigences et recommandations

Vous devez tenir compte de plusieurs exigences avant d'utiliser la fonction de déchargement matériel IPsec.

Cartes Ethernet prises en charge

Vous devez installer et utiliser uniquement des cartes Ethernet compatibles. Les cartes Ethernet suivantes sont prises en charge à partir d' ONTAP 9.16.1 :

- X50131A (contrôleur Ethernet 2p, 40G/100G/200G/400G)
- X60132A (contrôleur Ethernet 4p, 10G/25G)

ONTAP 9.17.1 ajoute la prise en charge des cartes Ethernet suivantes :

- X50135A (contrôleur Ethernet 2p, 40G/100G)
- X60135A (contrôleur Ethernet 2p, 40G/100G)

Les cartes X50131A et X50135A sont prises en charge sur les plates-formes suivantes :

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Les cartes X60132A et X60135A sont prises en charge sur les plates-formes suivantes :

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Voir le "NetApp Hardware Universe" pour plus d'informations sur les plateformes et cartes prises en charge.

Étendue du cluster

La fonction de déchargement matériel IPSec est configurée globalement pour le cluster. Et ainsi, par exemple, la commande `security ipsec config` s'applique à tous les nœuds du cluster.

Configuration cohérente

Les cartes NIC prises en charge doivent être installées sur tous les nœuds du cluster. Si une carte NIC prise en charge n'est disponible que sur certains nœuds, vous pouvez constater une dégradation importante des performances après un basculement si certaines LIF ne sont pas hébergées sur une carte réseau prenant en charge le déchargement.

Désactiver l'anti-relecture

Vous devez désactiver la protection anti-relecture IPSec sur ONTAP (configuration par défaut) et les clients IPsec. Si elle n'est pas désactivée, la fragmentation et le multi-chemin (route redondante) ne sont pas pris en

charge.

Si la configuration IPSec de ONTAP a été modifiée par défaut pour activer la protection anti-replay, utilisez cette commande pour la désactiver :

```
security ipsec config modify -replay-window 0
```

Vous devez vous assurer que la protection anti-relecture IPSec est désactivée sur votre client. Reportez-vous à la documentation IPsec de votre client pour désactiver la protection anti-replay.

Limites

Vous devez tenir compte de plusieurs limitations avant d'utiliser la fonction de déchargement matériel IPsec.

IPv6

À partir d' ONTAP 9.18.1, IPv6 est pris en charge pour la fonction de déchargement matériel IPsec. Avant ONTAP 9.18.1, le déchargement matériel IPsec ne prend pas en charge IPv6.

Numéros de séquence étendus

Les numéros de séquence étendus IPsec ne sont pas pris en charge avec la fonction de déchargement matériel. Seuls les numéros de séquence 32 bits normaux sont utilisés.

Agrégation de liens

À partir d' ONTAP 9.17.1, vous pouvez utiliser la fonction de déchargement matériel IPsec avec un "groupe d'agrégation de liens" .

Avant la version 9.17.1, la fonctionnalité de déchargement matériel IPsec ne prenait pas en charge l'agrégation de liens. Elle ne pouvait pas être utilisée avec une interface ou un groupe d'agrégation de liens administrés via le `network port ifgrp` commandes sur l'interface CLI ONTAP .

Prise en charge de la configuration dans l'interface de ligne de commandes ONTAP

Trois commandes CLI existantes sont mises à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec comme décrit ci-dessous. Voir également "Configurer la sécurité IP dans ONTAP"pour plus d'informations.

Commande ONTAP	Mise à jour
`security ipsec config show`	Le paramètre booléen `Offload Enabled` indique l'état actuel du déchargement de la carte réseau.
`security ipsec config modify`	Le paramètre `is-offload-enabled` peut être utilisé pour activer ou désactiver la fonction de déchargement de carte réseau.
`security ipsec config show-ipsecsa`	Quatre nouveaux compteurs ont été ajoutés pour afficher le trafic entrant et sortant en octets et en paquets.

Prise en charge de la configuration dans l'API REST ONTAP

Deux terminaux d'API REST existants sont mis à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec, comme décrit ci-dessous.

Terminal REST	Mise à jour
`/api/security/ipsec`	Le paramètre `offload_enabled` a été ajouté et est disponible avec la méthode PATCH.
`/api/security/ipsec/security_association`	Deux nouvelles valeurs de compteur ont été ajoutées pour suivre le nombre total d'octets et de paquets traités par la fonction de déchargement.

Pour en savoir plus sur l'API REST ONTAP, y compris "Nouveautés de l'API REST ONTAP", consultez la documentation sur l'automatisation ONTAP. Vous devez également consulter la documentation sur l'automatisation ONTAP pour plus de détails sur "Noeuds finaux IPsec".

Informations associées

- "sécurité ipsec"

Configurer la sécurité IP pour le réseau ONTAP

Plusieurs tâches sont nécessaires pour configurer et activer le chiffrement à la volée IPsec sur votre cluster ONTAP.

Vérifiez "Préparez-vous à utiliser la sécurité IP" avant de configurer IPsec. Par exemple, vous devrez peut-être décider d'utiliser la fonction de déchargement matériel IPSec disponible à partir de ONTAP 9.16.1.

Activez IPsec sur le cluster

Vous pouvez activer IPsec sur le cluster pour vous assurer que les données sont chiffrées en continu et sécurisées pendant le transit.

Étapes

1. Découvrez si IPSec est déjà activé :

   ```
   security ipsec config show
   ```

   Si le résultat inclut `IPsec Enabled: false`, passez à l'étape suivante.

2. Activer IPsec :

   ```
   security ipsec config modify -is-enabled true
   ```

   Vous pouvez activer la fonction de déchargement matériel IPsec à l'aide du paramètre booléen `is-offload-enabled` .

3. Exécutez à nouveau la commande de découverte :

   ```
   security ipsec config show
   ```

   Le résultat inclut maintenant `IPsec Enabled: true`.

Préparez la création de stratégies IPsec avec l'authentification par certificat

Vous pouvez ignorer cette étape si vous utilisez uniquement des clés prépartagées (PSK) pour l'authentification et que vous n'utilisez pas l'authentification par certificat.

Avant de créer une stratégie IPSec qui utilise des certificats pour l'authentification, vous devez vérifier que les conditions préalables suivantes sont remplies :

- ONTAP et le client doivent avoir installé le certificat CA de l'autre partie afin que les certificats de l'entité finale (ONTAP ou le client) soient vérifiables des deux côtés
- Un certificat est installé pour la LIF de ONTAP qui participe à la politique

> Les LIF ONTAP peuvent partager des certificats. Un mappage un-à-un entre les certificats et les LIFs n'est pas nécessaire.

Étapes

1. Installez tous les certificats de l'autorité de certification utilisés lors de l'authentification mutuelle, y compris les autorités de certification côté ONTAP et côté client, dans la gestion des certificats ONTAP, sauf s'il est déjà installé (comme c'est le cas pour une autorité de certification racine auto-signée ONTAP).

   Commande exemple
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Pour vous assurer que l'autorité de certification installée se trouve dans le chemin de recherche de l'autorité de certification IPSec lors de l'authentification, ajoutez les autorités de certification de gestion de certificat ONTAP au module IPSec à l'aide du `security ipsec ca-certificate add` commande.

   Commande exemple
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Créez et installez un certificat pour une utilisation par le LIF ONTAP. L'autorité de certification de l'émetteur de ce certificat doit déjà être installée sur ONTAP et ajoutée à IPsec.

   Commande exemple
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

Pour plus d'informations sur les certificats dans ONTAP, consultez les commandes de certificat de sécurité dans la documentation de ONTAP 9.

Définir la base de données de règles de sécurité (SPD)

IPSec requiert une entrée SPD avant d'autoriser le trafic à circuler sur le réseau. Ceci est vrai si vous utilisez un PSK ou un certificat pour l'authentification.

Étapes

1. Utilisez le `security ipsec policy create` commande pour :
   a. Sélectionnez l'adresse IP ONTAP ou le sous-réseau d'adresses IP pour participer au transport IPsec.
   b. Sélectionnez les adresses IP des clients qui se connectent aux adresses IP ONTAP.

Le client doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec une clé pré-partagée (PSK).

c. Vous pouvez également sélectionner des paramètres de trafic précis, tels que les protocoles de couche supérieure (UDP, TCP, ICMP, etc.), les numéros de port locaux et les numéros de port distants pour protéger le trafic. Les paramètres correspondants sont : `protocols` , `local-ports` et `remote-ports` respectivement.

   Ignorez cette étape pour protéger tout le trafic entre l'adresse IP ONTAP et l'adresse IP du client. La protection de tout le trafic est la valeur par défaut.

d. Entrez PSK ou PKI (public-Key Infrastructure) pour le `auth-method` paramètre de la méthode d'authentification souhaitée.

   i. Si vous entrez une clé PSK, incluez les paramètres, puis appuyez sur <enter> pour que l'invite vous demande d'entrer et de vérifier la clé pré-partagée.

      Les `local-identity` paramètres et `remote-identity` sont facultatifs si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

   ii. Si vous entrez une PKI, vous devez également entrer `cert-name`, `local-identity`, `remote-identity` paramètres. Si l'identité du certificat côté distant est inconnue ou si plusieurs identités client sont attendues, entrez l'identité spéciale `ANYTHING`.

e. À partir d' ONTAP 9.17.1, vous pouvez éventuellement saisir une identité de clé pré-partagée postquantique (PPK) avec le `ppk-identity` Paramètre. Les PPK offrent une couche de sécurité supplémentaire contre d'éventuelles attaques futures par ordinateur quantique. Lorsque vous saisissez une identité PPK, vous êtes invité à saisir son secret. Les PPK ne sont pris en charge que pour l'authentification PSK.

En savoir plus sur `security ipsec policy create` dans le "Référence de commande ONTAP" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Le trafic IP ne peut pas circuler entre le client et le serveur tant que ONTAP et le client n'ont pas configuré les stratégies IPSec correspondantes et que les informations d'identification d'authentification (PSK ou certificat) ne sont pas en place des deux côtés.

Utiliser les identités IPsec

Pour la méthode d'authentification par clé pré-partagée, les identités locales et distantes sont facultatives si

l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

Pour la méthode d'authentification PKI/certificat, les identités locales et distantes sont obligatoires. Les identités spécifient quelle identité est certifiée dans le certificat de chaque côté et sont utilisées dans le processus de vérification. Si l'identité distante est inconnue ou si elle peut être de nombreuses identités différentes, utilisez l'identité spéciale `ANYTHING`.

Description de la tâche

Au sein de ONTAP, les identités sont spécifiées en modifiant l'entrée du démon du processeur de service ou pendant sa création. Le démon du processeur de service peut être un nom d'identité avec une adresse IP ou un format de chaîne.

Étapes

1. Utiliser la commande suivante pour modifier un paramètre d'identité SPD existant :

```
security ipsec policy modify
```

Commande exemple

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configuration client multiple IPsec

Lorsqu'un petit nombre de clients doivent utiliser IPsec, l'utilisation d'une seule entrée SPD pour chaque client est suffisante. Toutefois, lorsque des centaines voire des milliers de clients doivent utiliser IPsec, NetApp recommande l'utilisation d'une configuration client multiple IPsec.

Description de la tâche

ONTAP prend en charge la connexion de plusieurs clients sur de nombreux réseaux à une seule adresse IP de SVM avec IPsec activé. Vous pouvez effectuer cette opération en utilisant l'une des méthodes suivantes :

- **Configuration du sous-réseau**

  Pour permettre à tous les clients d'un sous-réseau particulier (192.168.134.0/24 par exemple) de se connecter à une seule adresse IP de SVM à l'aide d'une seule entrée de la politique SPD, vous devez spécifier le `remote-ip-subnets` sous-réseau. De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte.

  > Lors de l'utilisation d'une seule entrée de stratégie dans une configuration de sous-réseau, les clients IPsec de ce sous-réseau partagent l'identité IPsec et la clé pré-partagée (PSK). Cependant, ceci n'est pas vrai avec l'authentification par certificat. Lors de l'utilisation de certificats, chaque client peut utiliser son propre certificat unique ou un certificat partagé pour s'authentifier. ONTAP IPSec vérifie la validité du certificat en fonction des autorités de certification installées dans son magasin de confiance local. ONTAP prend également en charge la vérification de la liste de révocation de certificats (CRL).

- **Autoriser la configuration de tous les clients**

  Pour permettre à n'importe quel client, quelle que soit son adresse IP source, de se connecter à l'adresse IP du SVM IPsec, utilisez l' `0.0.0.0/0` caractère générique lors de la spécification du `remote-ip-subnets` légale.

De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte. Pour l'authentification par certificat, vous pouvez entrer `ANYTHING`.

Aussi, lorsque le `0.0.0.0/0` le caractère générique est utilisé. vous devez configurer un numéro de port local ou distant spécifique à utiliser. Par exemple : `NFS port 2049`.

Étapes

a. Utilisez l'une des commandes suivantes pour configurer IPsec pour plusieurs clients.

i. Si vous utilisez **subnet configuration** pour prendre en charge plusieurs clients IPsec :

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

Commande exemple

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

i. Si vous utilisez **Autoriser la configuration de tous les clients** à prendre en charge plusieurs clients IPsec :

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

Commande exemple

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Afficher les statistiques IPsec

Lors de la négociation, un canal de sécurité appelé Association de sécurité IKE (sa) peut être établi entre l'adresse IP du SVM ONTAP et l'adresse IP du client. IPSec SAS est installé sur les deux noeuds finaux pour effectuer le cryptage et le décryptage des données. Vous pouvez utiliser les commandes de statistiques pour vérifier l'état des ports SAS IPsec et SAS IKE.

Si vous utilisez la fonction de déchargement matériel IPSec, plusieurs nouveaux compteurs sont affichés avec la commande `security ipsec config show-ipsecsa`.

Exemples de commandes

IKE sa exemple de commande :

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Exemple de commande et de sortie IPsec sa :

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Exemple de commande et de sortie IPsec sa :

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Informations associées

- "installation du certificat de sécurité"
- "sécurité ipsec"

Configurer le chiffrement du réseau du cluster backend ONTAP

À partir d' ONTAP 9.18.1, vous pouvez configurer le chiffrement TLS (Transport Layer Security) pour les données en transit sur le réseau du cluster backend. Ce chiffrement protège les données client stockées dans ONTAP lors de leur transmission entre les nœuds ONTAP du réseau du cluster dorsal.

Description de la tâche

- Le chiffrement du réseau du cluster backend est désactivé par défaut.
- Lorsque le chiffrement du réseau du cluster backend est activé, toutes les données client stockées dans ONTAP sont chiffrées lors de leur transmission entre les nœuds ONTAP sur le réseau du cluster backend. Certains flux de trafic réseau du cluster, tels que les données du chemin de contrôle, ne sont pas chiffrés.
- Par défaut, le chiffrement du réseau du cluster backend utilisera des certificats générés automatiquement pour chaque nœud du cluster. Tu peuxGérer les certificats de chiffrement du réseau du cluster sur chaque nœud pour utiliser un certificat installé personnalisé.

Avant de commencer

- Vous devez être administrateur ONTAP au niveau `admin` niveau de privilège permettant d'effectuer les tâches suivantes.
- Tous les nœuds du cluster doivent exécuter ONTAP 9.18.1 ou une version ultérieure pour activer le chiffrement du réseau du cluster backend.

Activer ou désactiver le chiffrement pour la communication réseau du cluster

Étapes

1. Afficher l'état actuel du chiffrement du réseau du cluster :

   ```
   security cluster-network show
   ```

   Cette commande affiche l'état actuel du chiffrement du réseau du cluster :

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Activer ou désactiver le chiffrement du réseau du cluster backend TLS :

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Cette commande active ou désactive la communication chiffrée des données client en transit sur le réseau du cluster backend.

Gérer les certificats de chiffrement du réseau du cluster

1. Consultez les informations actuelles du certificat de chiffrement du réseau du cluster :

   ```
   security cluster-network certificate show
   ```

   Cette commande affiche les informations actuelles du certificat de chiffrement du réseau du cluster :

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

Le nom du certificat et de l'autorité de certification (CA) est affiché pour chaque nœud du cluster.

2. Modifier le certificat de chiffrement du réseau du cluster pour un nœud :

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Cette commande modifie le certificat de chiffrement du réseau du cluster pour un nœud spécifique. Le certificat doit être installé et signé par une autorité de certification installée avant l'exécution de cette commande. Pour plus d'informations sur la gestion des certificats, veuillez consulter"Gestion des certificats ONTAP avec System Manager" . Si `-name` Si aucun certificat n'est spécifié, le certificat par défaut généré automatiquement est utilisé.

Configuration des politiques de pare-feu pour les LIF du réseau ONTAP

La configuration d'un pare-feu améliore la sécurité du cluster et permet d'empêcher tout accès non autorisé au système de stockage. Par défaut, le pare-feu intégré est configuré pour autoriser l'accès à distance à un ensemble spécifique de services IP pour les données, la gestion et les LIF intercluster.

À partir d'ONTAP 9.10.1 :

- Les politiques de pare-feu sont obsolètes et sont remplacées par les politiques de service LIF. Auparavant, le pare-feu intégré était géré à l'aide de politiques de pare-feu. Cette fonctionnalité s'effectue désormais à l'aide d'une politique de service LIF.
- Toutes les politiques de pare-feu sont vides et n'ouvrent aucun port dans le pare-feu sous-jacent. En revanche, tous les ports doivent être ouverts via une règle de service LIF.
- Aucune action n'est requise après une mise à niveau vers la version 9.10.1 ou ultérieure afin de passer des politiques de pare-feu aux politiques de service LIF. Le système construit automatiquement des politiques de service LIF conformes aux politiques de pare-feu utilisées dans la version précédente de ONTAP. Si vous utilisez des scripts ou d'autres outils qui créent et gèrent des politiques de pare-feu personnalisées, vous devrez peut-être mettre à niveau ces scripts pour créer des stratégies de service personnalisées.

Pour en savoir plus, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Les politiques de pare-feu peuvent être utilisées pour contrôler l'accès aux protocoles de service de gestion tels que SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS OU SNMP. Les politiques de pare-feu ne peuvent pas être définies pour des protocoles de données tels que NFS ou SMB.

Vous pouvez gérer le service et les politiques de pare-feu des manières suivantes :

- Activation ou désactivation du service de pare-feu
- Affichage de la configuration actuelle du service de pare-feu
- Création d'une nouvelle politique de pare-feu avec le nom de la politique et les services réseau spécifiés
- Application d'une politique de pare-feu à une interface logique
- Création d'une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante

  Vous pouvez l'utiliser pour créer une politique avec des caractéristiques similaires au sein d'une même SVM ou pour copier la politique dans une autre SVM.

- Affichage d'informations sur les politiques de pare-feu
- Modification des adresses IP et des masques de réseau utilisés par une politique de pare-feu
- Suppression d'une politique de pare-feu qui n'est pas utilisée par une LIF

Politiques de pare-feu et LIF

Les politiques de pare-feu de LIF sont utilisées pour restreindre l'accès au cluster sur chaque LIF. Vous devez comprendre comment la politique de pare-feu par défaut affecte l'accès au système sur chaque type de LIF, et comment personnaliser une politique de pare-feu pour augmenter ou diminuer la sécurité par rapport à une LIF.

Lors de la configuration d'une LIF à l'aide de la `network interface create` commande ou `network interface modify`, la valeur spécifiée pour le `-firewall-policy` paramètre détermine les protocoles de service et les adresses IP qui sont autorisés à accéder à la LIF. Pour en savoir plus, `network interface` consultez le "Référence de commande ONTAP".

Dans de nombreux cas, vous pouvez accepter la valeur de la stratégie de pare-feu par défaut. Dans d'autres cas, vous devrez peut-être restreindre l'accès à certaines adresses IP et à certains protocoles de service de gestion. Les protocoles de service de gestion disponibles sont : SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS ET SNMP.

La politique de pare-feu de toutes les LIFs de cluster est par défaut définie sur `""` et ne peut pas être modifié.

Le tableau ci-dessous décrit les politiques de pare-feu par défaut qui sont attribuées à chaque LIF, en fonction de leur rôle (ONTAP 9.5 et versions antérieures) ou de la politique de service (ONTAP 9.6 et versions ultérieures) lors de la création de cette LIF :

Politique de pare-feu	Protocoles de service par défaut	Accès par défaut	LIFs appliquées à
gstn	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Toute adresse (0.0.0.0/0)	Gestion du cluster, gestion SVM et LIF de node-management

gestion-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Toute adresse (0.0.0.0/0)	LIF de données qui prennent également en charge l'accès à la gestion des SVMs
intercluster	https, ndmp, ndmps	Toute adresse (0.0.0.0/0)	Toutes les LIFs intercluster
les données	dns, ndmp, ndmps, portmap	Toute adresse (0.0.0.0/0)	Toutes les LIF de données

Configuration du service portmap

Le service portmap mappe les services RPC aux ports sur lesquels ils écoutent.

Le service portmap était toujours accessible à ONTAP 9.3 et versions antérieures, est devenu configurable dans ONTAP 9.4 à ONTAP 9.6 et est géré automatiquement à partir de ONTAP 9.7.

- Dans ONTAP 9.3 et versions antérieures, le service portmap (rpcbind) était toujours accessible sur le port 111 dans les configurations réseau qui s'appuyaient sur le pare-feu ONTAP intégré plutôt qu'un pare-feu tiers.
- De ONTAP 9.4 à ONTAP 9.6, vous pouvez modifier les politiques de pare-feu pour contrôler si le service portmap est accessible sur des LIF spécifiques.
- Depuis ONTAP 9.7, le service de pare-feu de portmap est supprimé. En revanche, le port portmap est ouvert automatiquement pour toutes les LIF qui prennent en charge le service NFS.

Le service portmap est configurable dans le pare-feu de ONTAP 9.4 à ONTAP 9.6.

Le reste de cette rubrique explique comment configurer le service de pare-feu portmap pour ONTAP 9.4 à ONTAP 9.6.

En fonction de votre configuration, vous pouvez disautoriser l'accès au service sur des types spécifiques de LIF, généralement les LIF intercluster et de gestion. Dans certains cas, vous pourriez même refuser l'accès aux LIF de données.

Quel comportement pouvez-vous attendre

Les ONTAP 9.4 à ONTAP 9.6 Behavior ont été conçus pour offrir une transition transparente lors de la mise à niveau. Si le service portmap est déjà accessible sur des types spécifiques de LIF, il sera toujours accessible sur ces types de LIF. Comme dans ONTAP 9.3 et versions antérieures, vous pouvez spécifier les services accessibles à l'intérieur du pare-feu dans la politique de pare-feu pour le type de LIF.

Pour que le comportement soit effectif, tous les nœuds du cluster doivent exécuter ONTAP 9.4 à ONTAP 9.6. Seul le trafic entrant est affecté.

Les nouvelles règles sont les suivantes :

- Lors de la mise à niveau vers les versions 9.4 à 9.6, ONTAP ajoute le service portmap à toutes les politiques de pare-feu existantes, par défaut ou personnalisées.
- Lorsque vous créez un cluster ou un nouvel IPspace, ONTAP ajoute le service portmap uniquement à la politique de données par défaut, et non aux politiques de gestion par défaut ou intercluster.

- Vous pouvez ajouter le service portmap aux règles par défaut ou personnalisées selon vos besoins, puis supprimer le service selon vos besoins.

Comment ajouter ou supprimer le service portmap

Pour ajouter le service de mappage de port à une SVM ou à une politique de pare-feu de cluster (le rendre accessible via le pare-feu), entrez :

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Pour supprimer le service portmap d'une SVM ou d'une politique de pare-feu de cluster (celle-ci doit être inaccessible au sein du pare-feu), entrez :

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Vous pouvez utiliser la commande network interface modify pour appliquer la politique de pare-feu à une LIF existante. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Créer une politique de pare-feu et l'affecter à une LIF

Des politiques de pare-feu par défaut sont attribuées à chaque LIF lorsque vous créez la LIF. Dans de nombreux cas, les paramètres par défaut du pare-feu fonctionnent bien et vous n'avez pas besoin de les modifier. Si vous souhaitez modifier les services réseau ou les adresses IP pouvant accéder à une LIF, vous pouvez créer une politique de pare-feu personnalisée et l'affecter à la LIF.

Description de la tâche

- Vous ne pouvez pas créer de politique de pare-feu avec `policy` nom `data`, `intercluster`, `cluster`, ou `mgmt`.

  Ces valeurs sont réservées aux politiques de pare-feu définies par le système.

- Vous ne pouvez ni définir ni modifier une politique de pare-feu pour les LIFs de cluster.

  La politique de pare-feu des LIFs de cluster est définie sur 0.0.0.0/0 pour tous les types de services.

- Si vous avez besoin de supprimer un service d'une politique, vous devez supprimer la politique de pare-feu existante et en créer une nouvelle.
- Si IPv6 est activé sur le cluster, vous pouvez créer des politiques de pare-feu avec des adresses IPv6.

  Une fois IPv6 activé, `data`, `intercluster`, et `mgmt` Les politiques de pare-feu incluent ::/0, le caractère générique IPv6, dans leur liste d'adresses acceptées.

- Lorsque vous utilisez System Manager pour configurer la fonctionnalité de protection des données sur les clusters, vous devez vous assurer que les adresses IP LIF intercluster sont incluses dans la liste des autorisés et que le service HTTPS est autorisé sur les LIF intercluster et sur les pare-feu de votre entreprise.

  Par défaut, le `intercluster` La politique de pare-feu permet l'accès à partir de toutes les adresses IP (0.0.0.0/0, ou ::/0 pour IPv6) et active les services HTTPS, NDMP et NDMPS. Si vous modifiez cette politique par défaut ou si vous créez votre propre politique de pare-feu pour les LIF intercluster, vous devez ajouter chaque adresse IP LIF intercluster à la liste des autorisés et activer le service HTTPS.

- Depuis ONTAP 9.6, les services de pare-feu HTTPS et SSH ne sont pas pris en charge.

  Dans ONTAP 9.6, le `management-https` et `management-ssh` Les services LIF sont disponibles pour l'accès à la gestion HTTPS et SSH.

Étapes

1. Créer une politique de pare-feu qui sera disponible pour les LIF sur un SVM spécifique :

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Vous pouvez utiliser cette commande plusieurs fois pour ajouter plusieurs services réseau et une liste d'adresses IP autorisées pour chaque service de la politique de pare-feu.

2. Vérifiez que la stratégie a été correctement ajoutée en utilisant le `system services firewall policy show` commande.
3. Appliquer la politique de pare-feu à une LIF :

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Vérifier que la policy a été correctement ajoutée à la LIF à l'aide de l' `network interface show -fields firewall-policy` commande.

   Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

Exemple de création d'une politique de pare-feu et de son assignation à une LIF

La commande suivante crée une politique de pare-feu nommée Data_http qui active l'accès au protocole HTTP et HTTPS à partir des adresses IP sur le sous-réseau 10.10, applique cette politique à la LIF nommée data1 sur le SVM vs1, puis affiche toutes les politiques de pare-feu sur le cluster :

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Commandes ONTAP pour gérer le service et les politiques de pare-feu

Vous pouvez utiliser le `system services firewall` commandes permettant de gérer le service de pare-feu, le `system services firewall policy` commandes pour gérer les politiques de pare-feu et `network interface modify` Commande permettant de gérer les paramètres de pare-feu des LIF.

À partir d'ONTAP 9.10.1 :

- Les politiques de pare-feu sont obsolètes et sont remplacées par les politiques de service LIF. Auparavant, le pare-feu intégré était géré à l'aide de politiques de pare-feu. Cette fonctionnalité s'effectue désormais à l'aide d'une politique de service LIF.
- Toutes les politiques de pare-feu sont vides et n'ouvrent aucun port dans le pare-feu sous-jacent. En revanche, tous les ports doivent être ouverts via une règle de service LIF.
- Aucune action n'est requise après une mise à niveau vers la version 9.10.1 ou ultérieure afin de passer des politiques de pare-feu aux politiques de service LIF. Le système construit automatiquement des politiques de service LIF conformes aux politiques de pare-feu utilisées dans la version précédente de ONTAP. Si vous utilisez des scripts ou d'autres outils qui créent et gèrent des politiques de pare-feu personnalisées, vous devrez peut-être mettre à niveau ces scripts pour créer des stratégies de service personnalisées.

Pour en savoir plus, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez ou désactivez le service de pare-feu	`system services firewall modify`
Affiche la configuration actuelle du service de pare-feu	`system services firewall show`
Créez une politique de pare-feu ou ajoutez un service à une politique de pare-feu existante	`system services firewall policy create`
Appliquer une politique de pare-feu à une LIF	`network interface modify -lif lifname -firewall-policy`
Modifiez les adresses IP et les masques de réseau associés à une politique de pare-feu	`system services firewall policy modify`
Affiche des informations sur les politiques de pare-feu	`system services firewall policy show`
Créez une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante	`system services firewall policy clone`
Supprimez une politique de pare-feu qui n'est pas utilisée par une LIF	`system services firewall policy delete`

Informations associées

- "pare-feu des services système"
- "modification de l’interface réseau"

Informations sur le copyright

Copyright © 2026 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 DÉLICTUELLE (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.