Instructions de renforcement de la sécurité ONTAP

ONTAP 9

NetApp
July 18, 2024

Sommaire

Instructions de renforcement de la sécurité ONTAP

Présentation du renforcement de la sécurité ONTAP

ONTAP propose un ensemble de commandes qui vous permettent d'utiliser en toute sécurité le système d'exploitation du stockage ONTAP, le logiciel de gestion des données n° 1 du secteur. Utilisez les conseils et les paramètres de configuration de ONTAP pour aider votre entreprise à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

L'évolution du paysage actuel des menaces présente à une entreprise des défis uniques pour protéger ses ressources les plus précieuses : les données et les informations. Les menaces et vulnérabilités dynamiques et avancées auxquelles nous sommes confrontés sont de plus en plus sophistiquées. Associés à une augmentation de l'efficacité des techniques d'obfuscation et de reconnaissance de la part des intrus potentiels, les gestionnaires de systèmes doivent aborder de façon proactive la sécurité des données et de l'information.

Depuis juillet 2024, le contenu des rapports techniques publiés au format PDF a été intégré à la documentation produit de ONTAP. La documentation relative à la sécurité de ONTAP inclut désormais du contenu de *TR-4569: Guide de renforcement de la sécurité pour ONTAP*.

Validation des images ONTAP

ONTAP fournit des mécanismes permettant de s'assurer que l'image ONTAP est valide lors de la mise à niveau et au démarrage.

Validation des images de mise à niveau

La signature de code permet de vérifier que les images ONTAP installées via des mises à jour d'images sans interruption ou des mises à jour d'images automatisées sans interruption, des interfaces de ligne de commande ou des API ONTAP sont produites de manière authentique par NetApp et n'ont pas été falsifiées. La validation des images de mise à niveau a été introduite dans ONTAP 9.3.

Cette fonction est une amélioration de la sécurité sans intervention de la mise à niveau ou de la restauration ONTAP. L'utilisateur ne doit rien faire différemment, sauf en cas de vérification facultative de la signature de premier niveau "image.tgz".

Validation de l'image de démarrage

À partir de ONTAP 9.4, le démarrage sécurisé UEFI (Unified extensible Firmware interface) est activé pour les systèmes NetApp AFF A800, AFF A220, FAS2750 et FAS2720, ainsi que pour les systèmes nouvelle génération qui utilisent le BIOS UEFI.

Lors de la mise sous tension, le chargeur d'amorçage valide la base de données de la liste blanche des clés d'amorçage sécurisées avec la signature associée à chaque module chargé. Une fois que chaque module est validé et chargé, le processus de démarrage continue avec l'initialisation ONTAP. Si la validation de la signature échoue pour un module, le système redémarre.

Ces éléments s'appliquent aux images ONTAP et au BIOS de la plate-forme.

Comptes d'administrateur du stockage local

Rôles, applications et authentification

ONTAP offre aux entreprises soucieuses de leur sécurité la possibilité de fournir un accès granulaire à différents administrateurs via différentes applications et méthodes de connexion. Les clients peuvent ainsi créer un modèle zéro confiance centré sur les données.

Il s'agit des rôles disponibles pour les administrateurs admin et Storage Virtual machine. Les méthodes d'application de connexion et les méthodes d'authentification de connexion sont spécifiées.

Rôles

Grâce au contrôle d'accès basé sur des rôles (RBAC), les utilisateurs n'ont accès qu'aux systèmes et aux options requis pour leurs rôles et fonctions. La solution RBAC d'ONTAP limite l'accès administratif des utilisateurs au niveau correspondant à leur rôle, ce qui permet aux administrateurs de gérer les utilisateurs par rôle attribué. ONTAP fournit plusieurs rôles prédéfinis. Les opérateurs et les administrateurs peuvent créer, modifier ou supprimer des rôles de contrôle d'accès personnalisés et peuvent spécifier des restrictions de compte pour des rôles spécifiques.

Rôles prédéfinis pour les administrateurs du cluster

Ce rôle…	Dispose de ce niveau d'accès…	Aux commandes ou répertoires de commandes suivants
`admin`	Tout	Tous les répertoires de commandes (`DEFAULT`)
`admin-no-fsa` (Disponible à partir de ONTAP 9.12.1)	Lecture/écriture	• Tous les répertoires de commandes (`DEFAULT`) • `security login rest-role` • `security login role`

Lecture seule	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Aucune
`volume file show-disk-usage`	`autosupport`	Tout
• `set` • `system node autosupport`	Aucune	Tous les autres répertoires de commandes (`DEFAULT`)
`backup`	Tout	`vserver services ndmp`
Lecture seule	`volume`	Aucune
Tous les autres répertoires de commandes (`DEFAULT`)	`readonly`	Tout
• `security login password` Pour la gestion du mot de passe local et des informations clés du compte utilisateur • `set`	Aucune	`security`

Lecture seule	Tous les autres répertoires de commandes (`DEFAULT`)	`none`

> Le `autosupport` le rôle est affecté au prédéfini `autosupport` Compte, utilisé par AutoSupport OnDemand. ONTAP vous empêche de modifier ou de supprimer le `autosupport` compte. ONTAP vous empêche également d'attribuer le `autosupport` rôle vers d'autres comptes utilisateur.

Rôles prédéfinis pour les administrateurs des machines virtuelles de stockage (SVM)

Nom du rôle	Capacités
`vsadmin`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Effectuer des opérations SnapLock, sauf la suppression privilégiée • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau • Surveiller l'état de santé du SVM
`vsadmin-volume`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, notamment les déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Gérer les LUN • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Interface réseau du moniteur • Surveiller l'état de santé du SVM

`vsadmin-protocol`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Configuration des protocoles : NFS, SMB, iSCSI, FC, FCoE, NVMe/FC et NVMe/TCP • Configuration des services : DNS, LDAP et NIS • Gérer les LUN • Interface réseau du moniteur • Surveiller l'état de santé du SVM
`vsadmin-backup`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gestion des opérations NDMP • Effectuez une lecture/écriture de volume restauré • Gestion des relations SnapMirror et des copies Snapshot • Afficher les volumes et les informations réseau
`vsadmin-snaplock`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Gérez les volumes, à l'exception des déplacements de volumes • Gérez les quotas, les qtrees, les copies Snapshot et les fichiers • Effectuer des opérations SnapLock, y compris la suppression privilégiée • Configuration des protocoles : NFS et SMB • Configuration des services : DNS, LDAP et NIS • Surveiller les tâches • Surveiller les connexions réseau et l'interface réseau
`vsadmin-readonly`	• Gérer le mot de passe et les informations de clé locaux du compte utilisateur • Surveiller l'état de santé du SVM • Interface réseau du moniteur • Vision des volumes et des LUN • Vision des services et protocoles

Méthodes d'application

La méthode d'application spécifie le type d'accès de la méthode de connexion. Les valeurs possibles incluent `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, et `telnet`.

La définition de ce paramètre sur accorde à `service-processor` l'utilisateur l'accès au processeur de service. Lorsque ce paramètre est défini sur `service-processor`, le `-authentication-method` paramètre doit être défini sur `password` car le processeur de service ne prend en charge que l'authentification par mot de passe. Les comptes utilisateurs SVM ne peuvent pas accéder au processeur de service. Par conséquent, les opérateurs et les administrateurs ne peuvent pas utiliser le `-vserver` paramètre lorsque ce paramètre est défini sur `service-processor`.

Pour restreindre davantage l'accès à l' `service-processor` , utilisez la commande `system service-processor ssh add-allowed-addresses`. La commande `system service-processor api-service` peut être utilisée pour mettre à jour les configurations et les certificats.

Pour des raisons de sécurité, Telnet et le shell distant (RSH) sont désactivés par défaut car NetApp recommande le shell sécurisé (SSH) pour un accès distant sécurisé. S'il existe une exigence ou un besoin unique de Telnet ou RSH, ils doivent être activés.

La `security protocol modify` commande modifie la configuration existante de RSH et Telnet au niveau du cluster. Activez RSH et Telnet dans le cluster en définissant le champ activé sur `true`.

Méthodes d'authentification

Le paramètre de méthode d'authentification spécifie la méthode d'authentification utilisée pour les connexions.

METHODE d'authentification	Description
`cert`	Authentification par certificat SSL
`community`	Chaînes de communauté SNMP
`domain`	Authentification Active Directory
`nsswitch`	Authentification LDAP ou NIS
`password`	Mot de passe
`publickey`	Authentification par clé publique
`usm`	Modèle de sécurité utilisateur SNMP

L'utilisation de NIS n'est pas recommandée en raison des faiblesses de sécurité du protocole.

Depuis la version ONTAP 9.3, une authentification à deux facteurs est disponible dans les chaînes pour les comptes SSH locaux `admin` et utilise le `publickey` mot de passe comme deux méthodes d'authentification. En plus du `-authentication-method` champ de la `security login` commande, un nouveau champ nommé `-second-authentication-method` a été ajouté. La clé publique ou le mot de passe peuvent être spécifiés comme ou comme `-authentication-method` `-second-authentication-method`. Toutefois, lors de l'authentification SSH, l'ordre est toujours une clé publique avec authentification partielle, suivie de l'invite de mot de passe pour une authentification complète.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

À partir de ONTAP 9.4, `nsswitch` peut être utilisé comme deuxième méthode d'authentification avec `publickey`.

A partir de ONTAP 9.12.1, FIDO2 peut également être utilisé pour l'authentification SSH à l'aide d'un dispositif d'authentification matérielle YubiKey ou d'autres appareils compatibles FIDO2.

À partir de ONTAP 9.13.1 :

- `domain` les comptes peuvent être utilisés comme deuxième méthode d'authentification avec `publickey`.
- Mot de passe à usage unique basé sur l'heure (`totp`) est un code d'accès temporaire généré par un algorithme qui utilise l'heure actuelle comme l'un de ses facteurs d'authentification pour la deuxième méthode d'authentification.
- La révocation des clés publiques est prise en charge avec les clés publiques SSH ainsi que les certificats qui seront vérifiés pour leur expiration/révocation au cours de SSH.

Pour plus d'informations sur l'authentification multifacteur (MFA) pour ONTAP System Manager, Active IQ Unified Manager et SSH, consultez la section "Tr-4647 : authentification multifacteur dans ONTAP 9".

Comptes d'administration par défaut

Le compte admin doit être restreint car le rôle d'administrateur est autorisé à accéder à l'aide de toutes les applications. Le compte diag permet l'accès à l'interpréteur de commandes du système et ne doit être réservé qu'au support technique pour effectuer les tâches de dépannage.

Il existe deux comptes d'administration par défaut : `admin` et `diag`.

Les comptes orphelins sont un vecteur de sécurité majeur qui entraîne souvent des vulnérabilités, y compris l'escalade des privilèges. Il s'agit de comptes inutiles et inutilisés qui restent dans le référentiel de comptes d'utilisateurs. Il s'agit principalement de comptes par défaut qui n'ont jamais été utilisés ou pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés. Pour résoudre ce problème, ONTAP prend en charge la suppression et le changement de nom des comptes.

ONTAP ne peut ni supprimer ni renommer les comptes intégrés. Cependant, NetApp recommande de verrouiller tous les comptes intégrés inutiles à l'aide de la commande lock.

Bien que les comptes orphelins constituent un problème de sécurité important, NetApp recommande fortement de tester l'effet de la suppression des comptes du référentiel de comptes local.

Répertorie les comptes locaux

Pour lister les comptes locaux, exécutez la `security login show` commande.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication             Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------ -----------
admin            console     password  admin            no     no
admin            http        password  admin            no     no
admin            ontapi      password  admin            no     no
admin            service-processor password admin       no     no
admin            ssh         password  admin            no     no
autosupport      console     password  autosupport      no     no
6 entries were displayed.
```

Supprimez le compte admin par défaut

Le `admin` compte a le rôle d'administrateur et est autorisé à accéder à l'aide de toutes les applications.

Étapes

1. Créez un autre compte de niveau administrateur.

   Pour supprimer complètement le compte par défaut `admin` , vous devez d'abord créer un autre compte de niveau administrateur qui utilise l' `console` application de connexion.

   > Ces modifications peuvent avoir des effets indésirables. Testez toujours d'abord les nouveaux paramètres susceptibles d'affecter l'état de sécurité de la solution sur un cluster hors production.

   Exemple :

   ```
   cluster1::*> security login create -user-or-group-name NewAdmin
   -application console -authentication-method password -vserver cluster1
   ```

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication             Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------
-----------
NewAdmin         console     password  admin            no     no
admin            console     password  admin            no     no
admin            http        password  admin            no     no
admin            ontapi      password  admin            no     no
admin            service-processor password admin       no     no
admin            ssh         password  admin            no     no
autosupport      console     password  autosupport      no     no
7 entries were displayed.
```

2. Une fois que vous avez créé le nouveau compte admin, testez l'accès à ce compte avec la `NewAdmin` connexion du compte. Avec la `NewAdmin` connexion, configurez le compte pour qu'il ait les mêmes applications de connexion que le compte admin par défaut ou précédent (par exemple, `http`, , `ontapi service-processor`ou `ssh`). Cette étape permet de s'assurer que le contrôle d'accès est maintenu.

   Exemple :

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. Une fois toutes les fonctions testées, vous pouvez désactiver le compte admin pour toutes les applications avant de le supprimer de ONTAP. Cette étape sert de test final pour confirmer qu'il n'y a pas de fonctions persistantes qui s'appuient sur le compte admin précédent.

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. Pour supprimer le compte admin par défaut et toutes les entrées qui lui sont destinées, exécutez la commande suivante :

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
NewAdmin         http        password  admin             no     no
NewAdmin         ontapi      password  admin             no     no
NewAdmin         service-processor password admin        no     no
NewAdmin         ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

Définissez le mot de passe du compte de diagnostic (diag)

Un compte de diagnostic nommé `diag` est fourni avec votre système de stockage. Vous pouvez utiliser le `diag` compte pour effectuer des tâches de dépannage dans `systemshell`. Le `diag` compte est le seul compte qui peut être utilisé pour accéder au systemshell via la `diag` commande Privileged `systemshell`.

> Le systemshell et le compte associé `diag` sont destinés à des fins de diagnostic de bas niveau. Leur accès requiert le niveau de privilège diagnostic et est réservé uniquement pour être utilisé avec l'aide du support technique pour effectuer des tâches de dépannage. Ni le compte ni le n' `diag` `systemshell` est destiné à des fins administratives générales.

Avant de commencer

Avant d'accéder au `systemshell`, vous devez définir le `diag` mot de passe du compte à l'aide de la `security login password` commande. Vous devez utiliser des principes de mot de passe forts et modifier le `diag` mot de passe à intervalles réguliers.

Étapes

1. Définissez le `diag` mot de passe de l'utilisateur du compte :

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Vérification multi-administrateurs

À partir de ONTAP 9.11.1, vous pouvez utiliser la vérification multiadministrateur pour permettre l'exécution de certaines opérations, telles que la suppression de volumes ou de copies Snapshot, uniquement après approbation par les administrateurs désignés. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables.

La configuration de MAV comprend les éléments suivants :

- "Création d'un ou plusieurs groupes d'approbation administrateur."
- "Activation de la fonctionnalité de vérification multi-administrateurs."
- "Ajout ou modification de règles."

Après la configuration initiale, seuls les administrateurs d'un groupe d'approbation MAV (administrateurs MAV) peuvent modifier ces éléments.

Lorsque MAV est activé, la réalisation de chaque opération protégée nécessite trois étapes :

1. Lorsqu'un utilisateur lance l'opération, un "la demande a été générée."
2. Avant de pouvoir l'exécuter, le nombre requis de "Les administrateurs MAV doivent approuver."
3. Après approbation, l'utilisateur termine l'opération.

La MAV n'est pas destinée à être utilisée avec des volumes ou des flux de travail qui impliquent une automatisation poussée car chaque tâche automatisée nécessite une approbation avant que l'opération ne puisse être terminée. Si vous souhaitez utiliser l'automatisation et la vérification multiniveau ensemble, NetApp vous recommande d'utiliser des requêtes pour des opérations de vérification multiniveau spécifiques. Par exemple, vous pouvez appliquer `volume delete` des règles MAV uniquement aux volumes pour lesquels l'automatisation n'est pas impliquée, et vous pouvez désigner ces volumes avec un schéma de nommage particulier.

Pour plus d'informations sur MAV, reportez-vous à la "Documentation de vérification multiadministrateur ONTAP".

Verrouillage des copies Snapshot

Le verrouillage des copies Snapshot est une fonctionnalité SnapLock qui permet de rendre les copies Snapshot indélébiles, manuellement ou automatiquement, avec une période de conservation définie dans la règle Snapshot du volume. L'objectif du verrouillage des copies Snapshot est d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer les snapshots sur le système ONTAP principal ou secondaire.

Le verrouillage des copies Snapshot a été introduit dans ONTAP 9.12.1. Le verrouillage des copies Snapshot est également appelé verrouillage inviolable des copies Snapshot. Bien qu'il nécessite une licence SnapLock et l'initialisation de l'horloge de conformité, le verrouillage des copies Snapshot n'est pas lié à SnapLock Compliance ou SnapLock Enterprise. Il n'existe aucun administrateur de confiance dans le stockage, comme pour SnapLock Enterprise, et il ne protège pas l'infrastructure de stockage physique sous-jacente, comme pour SnapLock Compliance. Il s'agit d'une amélioration par rapport aux copies Snapshot SnapVauting sur un système secondaire. La restauration rapide des copies Snapshot verrouillées sur les systèmes primaires peut être effectuée pour restaurer les volumes corrompus par des ransomwares.

Pour plus de détails sur le verrouillage des copies Snapshot, reportez-vous au "Documentation de l'ONTAP".

Configurez l'accès à l'API basée sur un certificat

Au lieu de l'authentification par ID utilisateur et mot de passe pour l'accès à ONTAP par l'API REST ou l'API du SDK de gestion NetApp, l'authentification basée sur certificat doit être utilisée.

> Comme alternative à l'authentification basée sur certificat pour l'API REST, utilisez "Authentification par jeton OAuth 2.0".)

Vous pouvez générer et installer un certificat auto-signé sur ONTAP comme décrit dans ces étapes.

Étapes

1. À l'aide d'OpenSSL, générez un certificat en exécutant la commande suivante :

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
............................+++
writing new private key to 'test.key'
```

   Cette commande génère un certificat public nommé `test.pem` et une clé privée nommée `key.out`. Le nom commun, CN, correspond à l'ID utilisateur ONTAP.

2. Installez le contenu du certificat public au format courrier amélioré confidentiel (pem) dans ONTAP en exécutant la commande suivante et en collant le contenu du certificat lorsque vous y êtes invité :

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. Activez ONTAP pour autoriser l'accès client via SSL et définissez l'ID utilisateur pour l'accès API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

Dans l'exemple suivant, l'ID utilisateur `cert_user` est désormais activé pour utiliser l'accès à l'API authentifié par certificat. Un script Python du SDK de gestion simple utilisant `cert_user` pour afficher la version ONTAP apparaît comme suit :

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

La sortie du script affiche la version ONTAP.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Pour effectuer une authentification basée sur un certificat avec l'API REST ONTAP, procédez comme suit :
   a. Dans ONTAP, définissez l'ID utilisateur pour l'accès http :

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. Sur votre client Linux, exécutez la commande suivante qui produit la version ONTAP en tant que sortie :

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

Plus d'informations

- "Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP".

Authentification basée sur jeton OAuth 2.0 ONTAP pour l'API REST

En alternative à l'authentification basée sur certificat, vous pouvez utiliser l'authentification basée sur jeton OAuth 2.0 pour l'API REST.

Depuis ONTAP 9.14.1, vous avez la possibilité de contrôler l'accès à vos clusters ONTAP à l'aide de l'infrastructure d'autorisation ouverte (OAuth 2.0). Vous pouvez configurer cette fonctionnalité à l'aide de n'importe quelle interface d'administration ONTAP, notamment l'interface de ligne de commandes ONTAP, System Manager et l'API REST. Cependant, les décisions d'autorisation et de contrôle d'accès OAuth 2.0 ne peuvent être appliquées que lorsqu'un client accède à ONTAP à l'aide de l'API REST.

Les jetons OAuth 2.0 remplacent les mots de passe pour l'authentification des comptes utilisateur.

Pour plus d'informations sur l'utilisation d'OAuth 2.0, consultez le "Documentation ONTAP sur l'authentification et l'autorisation via OAuth 2.0".

Paramètres de connexion et de mot de passe

Une stratégie de sécurité efficace est conforme aux politiques, aux directives et à toute gouvernance ou norme établies de l'entreprise. La durée de vie du nom d'utilisateur, les exigences de longueur du mot de passe, les exigences en termes de caractères et le stockage de ces comptes sont des exemples de ces exigences. La solution ONTAP offre des fonctionnalités pour traiter ces constructions de sécurité.

Nouvelles fonctionnalités de compte local

Pour prendre en charge les stratégies, directives ou normes de compte utilisateur d'une entreprise, notamment la gouvernance, les fonctionnalités suivantes sont prises en charge dans ONTAP :

- Configuration des stratégies de mot de passe pour appliquer un nombre minimum de chiffres, de minuscules ou de majuscules
- Délai nécessaire après un échec de la tentative de connexion
- Définition de la limite d'inactivité du compte
- Expiration d'un compte utilisateur
- Affichage d'un message d'avertissement d'expiration de mot de passe
- Notification d'une connexion non valide

Les paramètres configurables sont gérés à l'aide de la commande Security login role config modify.

Prise en charge de SHA-512

Pour améliorer la sécurité des mots de passe, ONTAP 9 prend en charge la fonction de hachage SHA-2 et utilise par défaut la fonction SHA-512 pour hacher les nouveaux mots de passe ou les mots de passe modifiés. Les opérateurs et les administrateurs peuvent également expirer ou verrouiller les comptes selon les besoins.

Les comptes utilisateur ONTAP 9 préexistants avec des mots de passe inchangés continuent d'utiliser la fonction de hachage MD5 après la mise à niveau vers ONTAP 9.0 ou version ultérieure. Cependant, NetApp recommande vivement de migrer ces comptes utilisateur vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leur mot de passe.

La fonctionnalité de hachage de mot de passe vous permet d'effectuer les tâches suivantes :

- Afficher les comptes utilisateur correspondant à la fonction de hachage spécifiée :

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- Comptes expirés utilisant une fonction de hachage spécifiée (MD5, par exemple), qui oblige les utilisateurs à modifier leur mot de passe lors de la connexion suivante :

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Verrouiller les comptes avec des mots de passe utilisant la fonction de hachage spécifiée.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

La fonction de hachage password est inconnue pour l'utilisateur interne `autosupport` du SVM d'administration de votre cluster. Ce problème est cosmétique. La fonction de hachage est inconnue car cet utilisateur interne ne dispose pas d'un mot de passe configuré par défaut.

  - Pour afficher la fonction de hachage du mot de passe de l' `autosupport` utilisateur, exécutez les commandes suivantes :

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

  - Pour définir la fonction de hachage du mot de passe (par défaut : sha512), exécutez la commande suivante :

```
::> security login password -username autosupport
```

    La définition du mot de passe n'a pas d'importance.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

Paramètres de mot de passe

La solution ONTAP prend en charge les paramètres de mot de passe qui répondent aux exigences et directives de l'entreprise et qui les prennent en charge.

Attribut	Description	Valeur par défaut	Gamme
`username-minlength`	Longueur minimale du nom d'utilisateur requise	3	3-16
`username-alphanum`	Nom d'utilisateur alphanumérique	désactivé	Activé/Désactivé
`passwd-minlength`	Longueur minimale du mot de passe requise	8	3-64
`passwd-alphanum`	Mot de passe alphanumérique	activé	Activé/Désactivé
`passwd-min-special-chars`	Nombre minimum de caractères spéciaux requis dans le mot de passe	0	0-64
`passwd-expiry-time`	Heure d'expiration du mot de passe (en jours)	Illimité, ce qui signifie que les mots de passe n'expirent jamais	0-illimité 0 == expire maintenant
`require-initial-passwd-update`	Exiger la mise à jour initiale du mot de passe lors de la première connexion	Désactivé	Activé/Désactivé Modifications autorisées via la console ou SSH
`max-failed-login-attempts`	Nombre maximal de tentatives infructueuses	0, ne pas verrouiller le compte	-

Attribut	Description	Valeur par défaut	Gamme
`lockout-duration`	Durée maximale de verrouillage (en jours)	La valeur par défaut est 0, ce qui signifie que le compte est verrouillé pendant une journée	-
`disallowed-reuse`	Interdire les N derniers mots de passe	6	Le minimum est de 6
`change-delay`	Délai entre les modifications du mot de passe (en jours)	0	-
`delay-after-failed-login`	Délai après chaque tentative de connexion échouée (en secondes)	4	-
`passwd-min-lowercase-chars`	Nombre minimum de caractères alphabétiques minuscules requis dans le mot de passe	0, qui ne nécessite pas de caractères minuscules	0-64
`passwd-min-uppercase-chars`	Nombre minimum de caractères alphabétiques majuscules requis	0, qui ne nécessite pas de majuscules	0-64
`passwd-min-digits`	Nombre minimum de chiffres requis dans le mot de passe	0, qui ne nécessite pas de chiffres	0-64
`passwd-expiry-warn-time`	Afficher le message d'avertissement avant l'expiration du mot de passe (en jours)	Illimité, ce qui signifie ne jamais avertir de l'expiration du mot de passe	0, ce qui signifie avertir l'utilisateur de l'expiration du mot de passe à chaque connexion réussie
`account-expiry-time`	Le compte expire dans N jours	Illimité, ce qui signifie que les comptes n'expirent jamais	Le délai d'expiration du compte doit être supérieur à la limite d'inactivité du compte
`account-inactive-limit`	Durée maximale d'inactivité avant l'expiration du compte (en jours)	Illimité, ce qui signifie que les comptes inactifs n'expirent jamais	La limite d'inactivité du compte doit être inférieure à l'heure d'expiration du compte

Exemple

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

À partir de 9.14.1, les mots de passe sont de plus en plus complexes et les règles de verrouillage. Ceci s'applique uniquement aux nouvelles installations de ONTAP.

Méthodes d'administration du système

Ce sont des paramètres importants pour renforcer l'administration du système ONTAP.

Accès en ligne de commande

L'établissement d'un accès sécurisé aux systèmes est un élément essentiel du maintien de la sécurité de la solution. Les options d'accès en ligne de commande les plus courantes sont SSH, Telnet et RSH. Parmi ces technologies, SSH est la meilleure pratique standard du secteur et la plus sécurisée pour l'accès à distance en ligne de commande. NetApp recommande vivement d'utiliser SSH pour l'accès en ligne de commande à la solution ONTAP.

Configurations SSH

La `security ssh show` commande affiche les configurations des algorithmes d'échange de clés SSH, du chiffrement et des algorithmes MAC pour le cluster et les SVM. La méthode d'échange de clés utilise ces algorithmes et ces chiffrements pour spécifier comment les clés de session à usage unique sont générées

pour le cryptage et l'authentification et comment l'authentification du serveur a lieu.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

Bannières de connexion

Les bannières de connexion permettent aux entreprises de présenter aux opérateurs, administrateurs, voire même aux utilisateurs malveillants, les conditions d'utilisation. Elles indiquent qui est autorisé à accéder au système. Cette approche est utile pour établir les attentes en matière d'accès et d'utilisation du système. La `security login banner modify` commande modifie la bannière de connexion. La bannière de connexion s'affiche juste avant l'étape d'authentification lors du processus de connexion SSH et du périphérique de la console. Le texte de la bannière doit être entre guillemets (« »), comme dans l'exemple suivant.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

Paramètres de bannière de connexion

Paramètre	Description
`vserver`	Utiliser ce paramètre pour spécifier le SVM avec la bannière modifiée. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster. La message au niveau du cluster est utilisée par défaut pour les SVM de données qui ne disposent pas de message défini.

Paramètre	Description
`message`	Ce paramètre facultatif peut être utilisé pour spécifier un message de bannière de connexion. Si le cluster a un ensemble de messages de bannière de connexion, la bannière de connexion au cluster est également utilisée par tous les SVM de données. La définition de la bannière de connexion d'un SVM de données remplace l'affichage de la bannière de connexion du cluster. Pour réinitialiser une bannière de connexion SVM de données afin d'utiliser la bannière de connexion au cluster, utilisez ce paramètre avec la valeur « - ». Si vous utilisez ce paramètre, la bannière de connexion ne peut pas contenir de nouvelles lignes (également appelées extrémités de lignes [EOL] ou sauts de ligne). Pour saisir un message de bannière de connexion avec des lignes de rappel, ne spécifiez aucun paramètre. Vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes. Les caractères non ASCII doivent utiliser Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Utilisez ce paramètre pour spécifier l'URI à partir de laquelle la bannière de connexion est téléchargée. La longueur du message ne doit pas dépasser 2048 octets. Les caractères non ASCII doivent être fournis au format Unicode UTF-8.

Message du jour

La `security login motd modify` commande met à jour le message du jour (MOTD).

Il existe deux catégories de MOTD : le MOTD au niveau du cluster et le MOTD au niveau du SVM de données. Un utilisateur se connectant au cluster d'un SVM de données peut voir deux messages : le MOTD au niveau du cluster suivi du MOTD au niveau du SVM pour ce SVM.

L'administrateur du cluster peut activer ou désactiver le MOTD au niveau du cluster sur chaque SVM individuellement si nécessaire. Si l'administrateur du cluster désactive le MOTD au niveau du cluster pour un SVM, un utilisateur se connectant au SVM ne voit pas le message au niveau du cluster. Seul un administrateur de cluster peut activer ou désactiver le message au niveau du cluster.

Paramètre MOTD	Description
Un vServer	Utiliser ce paramètre pour spécifier le SVM pour lequel le MOTD est modifié. Utiliser le nom du SVM admin du cluster pour modifier le message au niveau du cluster.

Paramètre MOTD	Description
messagerie	Ce paramètre facultatif peut être utilisé pour spécifier un message. Si vous utilisez ce paramètre, le MOTD ne peut pas contenir de nouvelles lignes. Si vous ne spécifiez aucun paramètre autre que le `-vserver` paramètre, vous êtes invité à saisir le message de manière interactive. Les messages entrés de manière interactive peuvent contenir des nouvelles lignes. Les caractères non ASCII doivent être fournis au format Unicode UTF-8. Le message peut contenir du contenu généré de façon dynamique à l'aide des séquences d'échappement suivantes : • `\\` - Un seul caractère de jeu • `\b` - Pas de sortie (pris en charge pour la compatibilité avec Linux uniquement) • `\C` - Nom du cluster • `\d` - La date actuelle telle qu'elle est définie sur le nœud de connexion • `\t` - Heure actuelle définie sur le nœud de connexion • `\I` - Adresse IP de LIF entrante (imprime la console pour une `console` connexion) • `\l` - Nom du périphérique de connexion (imprime la console pour une `console` connexion) • `\L` - Dernière connexion de l'utilisateur sur n'importe quel nœud du cluster • `\m` - Architecture de la machine • `\n` - Nom du nœud ou du SVM de données • `\N` - Nom de l'utilisateur se connectant • `\o` - Identique à \O. Fourni pour la compatibilité Linux. • `\O` - Nom de domaine DNS du nœud. Notez que la sortie dépend de la configuration du réseau et peut être vide. • `\r` - Numéro de version du logiciel • `\s` - Nom du système d'exploitation • `\u` - Nombre de sessions clustershell actives sur le nœud local. Pour l'administrateur du cluster : tous les utilisateurs du cluster shell. Pour le SVM de données admin : sessions actives uniquement pour ce SVM de données. • `\U` - Identique à `\u`, mais a ou a `user users` ajouté • `\v` - Chaîne de version de cluster effective • `\W` - Sessions actives sur le cluster pour l'utilisateur se connectant (`who`)

Pour plus d'informations sur la configuration du message du jour dans ONTAP, reportez-vous au "Documentation ONTAP sur message du jour".

Expiration de la session CLI

Le délai d'expiration par défaut de la session CLI est de 30 minutes. Le délai d'expiration est important pour éviter les sessions obsolètes et le piggydorsal de session.

Utilisez `system timeout show` la commande pour afficher le délai d'expiration actuel de la session de l'interface de ligne de commande. Pour définir la valeur du délai d'expiration, utilisez la `system timeout modify -timeout <minutes>` commande.

Accès Internet avec NetApp ONTAP System Manager

Si un administrateur ONTAP préfère utiliser une interface graphique au lieu de l'interface de ligne de commandes pour accéder au cluster et le gérer, utilisez NetApp ONTAP System Manager. Il est inclus avec ONTAP en tant que service Web, activé par défaut et accessible à l'aide d'un navigateur. Pointez le navigateur sur le nom d'hôte si vous utilisez DNS ou l'adresse IPv4 ou IPv6 via `https://cluster-management-LIF`.

Si le cluster utilise un certificat numérique auto-signé, il est possible que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez soit reconnaître le risque de continuer l'accès, soit installer un certificat numérique signé par l'autorité de certification (CA) sur le cluster pour l'authentification du serveur.

Depuis ONTAP 9.3, l'authentification SAML (Security assertion Markup Language) est une option disponible dans ONTAP System Manager.

Authentification SAML pour ONTAP System Manager

SAML 2.0 est une norme du secteur largement adoptée qui permet à tout fournisseur d'identités tiers conforme à la norme SAML d'effectuer un MFA à l'aide de mécanismes propres à l'IDP choisi par l'entreprise et en tant que source d'authentification unique (SSO).

Trois rôles sont définis dans la spécification SAML : le principal, l'IDP et le fournisseur de services. Dans l'implémentation de ONTAP, un principal est l'administrateur du cluster qui accède à ONTAP via ONTAP System Manager ou NetApp Active IQ Unified Manager. Le PDI est un logiciel tiers IDP. Depuis ONTAP 9.3, Microsoft Active Directory Federated Services (ADFS) et l'IDP open source Shibboleth sont des PDI pris en charge. À partir de ONTAP 9.12.1, Cisco DUO est un IDP pris en charge. Le fournisseur de services est la fonctionnalité SAML intégrée à ONTAP qui est utilisée par ONTAP System Manager ou l'application Web Active IQ Unified Manager.

Contrairement au processus de configuration à deux facteurs SSH, une fois l'authentification SAML activée, l'accès à ONTAP System Manager ou au processeur de service ONTAP requiert l'authentification de tous les administrateurs existants via ce protocole. Aucune modification n'est requise pour les comptes utilisateur du cluster. Lorsque l'authentification SAML est activée, une nouvelle méthode d'authentification de `saml` est ajoutée aux utilisateurs existants disposant des rôles d'administrateur pour `http` et `ontapi` les applications.

Une fois l'authentification SAML activée, les nouveaux comptes supplémentaires nécessitant l'accès SAML IDP doivent être définis dans ONTAP avec le rôle d'administrateur et la méthode d'authentification saml pour et les `http` `ontapi` applications. Si l'authentification SAML est désactivée à un moment ou à un autre, ces nouveaux comptes requièrent que la `password` méthode d'authentification soit définie avec le rôle d'administrateur pour `http` et les applications et `ontapi` qu'elle ajoute l'application de console pour l'authentification ONTAP locale à ONTAP System Manager.

Une fois l'IDP SAML activé, il effectue l'authentification pour l'accès au Gestionnaire système ONTAP à l'aide des méthodes disponibles pour ce dernier, telles que le protocole LDAP (Lightweight Directory Access Protocol), Active Directory (AD), Kerberos, le mot de passe, etc. Les méthodes disponibles sont uniques au PDI. Il est important que les comptes configurés dans ONTAP aient des ID utilisateur qui correspondent aux méthodes d'authentification IDP.

Les PDI validés par NetApp sont Microsoft ADFS, Cisco DUO et Shibboleth IDP open source.

À partir de ONTAP 9.14.1, Cisco DUO peut être utilisé comme second facteur d'authentification pour SSH.

Pour plus d'informations sur MFA pour ONTAP System Manager, Active IQ Unified Manager et SSH, voir "Tr-4647 : authentification multifacteur dans ONTAP 9".

Informations ONTAP System Manager

À partir de ONTAP 9.11.1, ONTAP System Manager fournit des informations exploitables pour aider les administrateurs du cluster à rationaliser leurs tâches quotidiennes. Les informations de sécurité sont basées sur les recommandations de ce rapport technique.

Analyse de la sécurité	Détermination
Telnet est activé	NetApp recommande un accès sécurisé à distance (SSH).
Le shell distant (RSH) est activé	NetApp recommande SSH pour un accès distant sécurisé.
AutoSupport utilise un protocole non sécurisé	AutoSupport n'est pas configuré pour être envoyé via lien:HTTPS.
La bannière de connexion n'est pas configurée au niveau du cluster	Avertissement si la bannière de connexion n'est pas configurée pour le cluster.
SSH utilise des chiffrements non sécurisés	Avertissement si SSH utilise des chiffrements non sécurisés.
Trop peu de serveurs NTP sont configurés	Avertissement si le nombre de serveurs NTP configurés est inférieur à trois.
Utilisateur admin par défaut non verrouillé	Lorsque vous n'utilisez aucun compte d'administration par défaut (admin ou diag) pour vous connecter à System Manager et que ces comptes ne sont pas verrouillés, il est recommandé de les verrouiller.
Défense contre les ransomwares : les volumes n'ont pas de règles Snapshot	Aucune règle Snapshot adéquate n'est associée à un ou plusieurs volumes.
Défense contre les ransomware : désactivez la suppression automatique de Snapshot	La suppression automatique des snapshots est définie pour un ou plusieurs volumes.
Les attaques par ransomware ne font pas l'objet d'une surveillance des volumes	La protection anti-ransomware autonome est prise en charge sur plusieurs volumes, mais pas encore configurée.
Les SVM ne sont pas configurés pour la protection autonome contre les ransomware	La protection anti-ransomware autonome est prise en charge sur plusieurs SVM, mais pas encore configurée.
FPolicy natif n'est pas configuré	FPolicy n'est pas défini pour les SVM NAS.
Activez le mode actif de protection anti-ransomware autonome	Plusieurs volumes ont terminé leur mode d'apprentissage et vous pouvez activer le mode actif
La conformité à la norme FIPS 140-2 globale est désactivée	La conformité à la norme FIPS 140-2 globale n'est pas activée.
Le cluster n'est pas configuré pour les notifications	Les e-mails, les webhooks ou les traphosts SNMP ne sont pas configurés pour recevoir des notifications.

Pour plus d'informations sur ONTAP System Manager Insights, consultez le "Informations exploitables avec ONTAP System Manager".

La protection anti-ransomware autonome de ONTAP

Pour compléter l'analytique du comportement des utilisateurs pour Storage Workload Security, la protection anti-ransomware autonome de ONTAP analyse les workloads de volume et l'entropie pour détecter les ransomware, puis prend une Snapshot et notifie l'administrateur lorsqu'une attaque est suspectée.

Outre la détection et la prévention des ransomwares grâce à l'analytique comportementale des utilisateurs (UBA) FPolicy externes avec NetApp Cloud Insights/Cloud Secure et l'écosystème de partenaires NetApp FPolicy, ONTAP 9.10.1 propose une protection anti-ransomware autonome. La protection anti-ransomware autonome de ONTAP utilise une fonctionnalité intégrée de machine learning (ML) qui analyse l'activité des workloads de volume et l'entropie des données pour détecter automatiquement les ransomware. Il surveille les activités différentes de l'UBA afin de détecter les attaques qui ne l'ont pas été.

Pour plus d'informations sur cette fonctionnalité, reportez-vous à la section "Tr-4572 : la solution NetApp pour ransomware" ou à la "Documentation sur la protection anti-ransomware autonome de ONTAP".

Audit du système d'administration du stockage

Assurez l'intégrité de l'audit des événements en transférant les événements ONTAP vers un serveur syslog distant. Ce serveur peut être un système de gestion des événements liés aux informations de sécurité tel que Splunk.

Envoyer syslog

Les informations d'audit et de journalisation sont extrêmement précieuses pour le support et la disponibilité. En outre, les informations figurant dans les journaux (syslog) ainsi que dans les rapports et résultats d'audit sont généralement sensibles. Pour préserver les contrôles et le niveau de sécurité, les entreprises doivent impérativement gérer les données de journalisation et d'audit de manière sécurisée.

Le délestage des données des syslog est nécessaire pour limiter l'impact d'une faille à un seul système ou une seule solution. Par conséquent, NetApp recommande de décharger des informations syslog en toute sécurité vers un emplacement de stockage ou de conservation sécurisé.

Créez une destination de transfert de journaux

Utilisez `cluster log-forwarding create` la commande pour créer des destinations de transfert de journaux pour la journalisation à distance.

Paramètres

Utiliser les paramètres suivants pour configurer la `cluster log-forwarding create` commande :

- **Hôte de destination.** Ce nom est le nom d'hôte ou l'adresse IPv4 ou IPv6 du serveur vers lequel transférer les journaux.

  ```
  -destination <Remote InetAddress>
  ```

- **Port de destination.** Il s'agit du port sur lequel le serveur de destination écoute.

```
[-port <integer>]
```

- **Protocole de transfert de journaux.** Ce protocole est utilisé pour envoyer des messages à la destination.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

Le protocole de transfert de journaux peut utiliser l'une des valeurs suivantes :

  - `udp-unencrypted`. Protocole de datagramme utilisateur sans sécurité.
  - `tcp-unencrypted`. TCP sans sécurité.
  - `tcp-encrypted`. TCP avec TLS (transport Layer Security).

- **Vérifiez l'identité du serveur de destination.** Lorsque ce paramètre est défini sur true, l'identité de la destination de transfert de journaux est vérifiée en validant son certificat. La valeur peut être définie sur vrai uniquement lorsque la `tcpencrypted` valeur est sélectionnée dans le champ de protocole.

```
[-verify-server \{true|false}]
```

- **Fonction Syslog.** Cette valeur est la fonction syslog à utiliser pour les journaux transmis.

```
[-facility <Syslog Facility>]
```

- **Ignorez le test de connectivité.** Normalement, la `cluster log-forwarding create` commande vérifie que la destination est accessible en envoyant une requête ping ICMP (Internet Control message Protocol) et échoue si elle n'est pas accessible. La définition de cette valeur `true` permet de contourner la vérification ping afin que vous puissiez configurer la destination lorsqu'elle est inaccessible.

```
[-force [true]]
```

NetApp recommande d'utiliser la `cluster log-forwarding` commande pour forcer la connexion à un `-tcp-encrypted` type.

Notification d'événement

La sécurisation des informations et des données quittant un système est essentielle au maintien et à la gestion du niveau de sécurité du système. Les événements générés par la solution ONTAP sont une mine d'informations sur le problème rencontré par la solution, les informations traitées, etc. La vitalité de ces données souligne la nécessité de les gérer et de les migrer de manière sécurisée.

La `event notification create` commande envoie une nouvelle notification d'un ensemble d'événements défini par un filtre d'événements à une ou plusieurs destinations de notification. Les exemples suivants illustrent la configuration de la notification d'événements et la `event notification show` commande, qui affiche les destinations et les filtres de notification d'événements configurés.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Chiffrement du stockage

Pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque, utilisez le chiffrement de stockage NetApp matériel ou le chiffrement logiciel de volume NetApp/chiffrement d'agrégat NetApp. Ces deux mécanismes sont validés conformément à la norme FIPS-140-2 et lors de l'utilisation de mécanismes matériels avec des mécanismes logiciels, la solution est admissible au programme CSfC (commercial Solutions for Classified Program). Il offre une protection renforcée des données secrètes et les plus secrètes au repos, à la fois au niveau du matériel et des logiciels.

Le chiffrement des données au repos est important pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque.

ONTAP 9 propose trois solutions de chiffrement des données au repos conformes à la norme FIPS 140-2 :

- NetApp Storage Encryption (NSE) est une solution matérielle qui utilise des disques à chiffrement automatique.
- NetApp Volume Encryption (NVE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.
- NetApp Aggregate Encryption (NAE) est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

NSE, NVE et NAE peuvent utiliser soit la gestion des clés externe, soit le gestionnaire de clés intégré (OKM). L'utilisation de NSE, NVE et NAE n'affecte pas les fonctionnalités d'efficacité du stockage ONTAP. Toutefois, les volumes NVE sont exclus de la déduplication dans les agrégats. Les volumes NAE participent à la déduplication dans les agrégats et en tirent profit.

Le gestionnaire de clés intégré OKM fournit une solution de chiffrement autonome pour les données au repos avec NSE, NVE ou NAE.

NVE, NAE et OKM utilisent le module de chiffrement ONTAP. CryptoMod figure dans la liste des modules validés CCVP FIPS 140-2. Voir "FIPS 140-2 Cert. No 4144".

Pour commencer la configuration de OKM, utilisez la `security key-manager onboard enable` commande. Pour configurer les gestionnaires de clés KMIP (Key Management Interoperability Protocol) externes, utilisez la `security key-manager external enable` commande. À partir de ONTAP 9.6, la colocation est prise en charge pour les gestionnaires de clés externes. Utiliser le `-vserver <vserver name>` paramètre pour activer la gestion externe des clés pour un SVM spécifique. Avant la version 9.6, la `security key-manager setup` commande servait à configurer OKM et des gestionnaires de clés

externes. Pour la gestion intégrée des clés, cette configuration guide l'opérateur ou l'administrateur tout au long de la configuration de la phrase de passe et des paramètres supplémentaires pour la configuration de OKM.

Une partie de la configuration est fournie dans l'exemple suivant :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

À partir de ONTAP 9.4, vous pouvez utiliser l' `-enable-cc-mode` option vrai avec `security key-manager setup` pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage. Pour ONTAP 9.6 et versions ultérieures, la syntaxe de la commande est `security key-manager onboard enable -cc-mode-enabled yes`.

À partir de ONTAP 9.4, vous pouvez utiliser la `secure-purge` fonctionnalité avec privilèges avancés pour « nettoyer » les données sur des volumes NVE sans interruption. Le nettoyage des données sur un volume chiffré garantit qu'elles ne peuvent pas être restaurées à partir du support physique. La commande suivante purge de manière sécurisée les fichiers supprimés sur vol1 sur SVM vs1 :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

À partir de ONTAP 9.7, NAE et NVE sont activés par défaut si la licence VE est en place, OKM ou des gestionnaires de clés externes sont configurés et NSE n'est pas utilisé. Les volumes NAE sont créés par défaut sur les agrégats NAE et les volumes NVE sont créés par défaut sur des agrégats non NAE. Vous

pouvez le remplacer en saisissant la commande suivante :

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

À partir de la version ONTAP 9.6, vous pouvez utiliser une étendue SVM pour configurer la gestion externe des clés pour un SVM de données dans le cluster. Cette configuration est idéale pour les environnements mutualisés dans lesquels chaque locataire utilise un SVM différent (ou un ensemble de SVM) pour le service des données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire. Pour plus d'informations, reportez-vous à la section "Activez la gestion externe des clés dans ONTAP 9.6 et versions ultérieures" de la documentation ONTAP.

À partir de la version ONTAP 9.11.1, vous pouvez configurer la connectivité aux serveurs de gestion externe des clés en cluster en désignant des serveurs clés principaux et secondaires sur une SVM. Pour plus d'informations, reportez-vous à la section "configurez les serveurs de clés externes en cluster" de la documentation ONTAP.

À partir de ONTAP 9.13.1, vous pouvez configurer des serveurs de gestionnaire de clés externes dans le gestionnaire de système. Pour plus d'informations, reportez-vous à la section "Gestion de gestionnaires de clés externes" de la documentation ONTAP.

Chiffrement de réplication des données

Pour compléter le chiffrement des données au repos, vous pouvez chiffrer le trafic de réplication des données ONTAP entre les clusters à l'aide de TLS 1.2 avec une clé prépartagée pour SnapMirror, SnapVault ou FlexCache.

Lors de la réplication de données pour la reprise sur incident, la mise en cache ou la sauvegarde, vous devez protéger ces données lors du transport sur le réseau entre un cluster ONTAP et un autre. Cela permet d'éviter les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de ONTAP 9.6, le chiffrement de peering de cluster prend en charge le chiffrement TLS 1.2 AES-256 GCM pour les fonctionnalités de réplication des données ONTAP telles que SnapMirror, SnapVault et FlexCache. Le chiffrement est configuré au moyen d'une clé pré-partagée (PSK) entre deux pairs de cluster.

Les clients qui utilisent des technologies comme NSE, NVE et NAE pour protéger les données au repos peuvent également utiliser le chiffrement des données de bout en bout en passant à ONTAP 9.6 ou version ultérieure pour utiliser le chiffrement de cluster.

Le cluster peering chiffre toutes les données entre les pairs de cluster. Par exemple, lorsque vous utilisez SnapMirror, toutes les informations de peering ainsi que toutes les relations SnapMirror entre l'homologue du cluster source et l'homologue du cluster destination sont chiffrées. Vous ne pouvez pas envoyer de données en texte clair entre les pairs de cluster lorsque le chiffrement de peering de cluster est activé.

Depuis ONTAP 9.6, le chiffrement est activé par défaut pour les nouvelles relations entre clusters. Pour activer le chiffrement sur les relations entre clusters créées avant ONTAP 9.6, vous devez mettre à niveau le cluster source et le cluster de destination vers la version 9.6. En outre, vous devez utiliser `cluster peer modify` la commande pour modifier les pairs de cluster source et cible afin d'utiliser le chiffrement de peering de cluster.

Vous pouvez convertir une relation de pairs existante pour utiliser le chiffrement de peering de clusters dans ONTAP 9.6, comme illustré dans l'exemple suivant :

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

Chiffrement IPsec des données en transit

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPSec : IPSec offre une alternative au chiffrement NFS ou SMB/CIFS et est la seule option de chiffrement à la volée pour le trafic iSCSI.

Dans certains cas, il peut être nécessaire de protéger toutes les données client transportées sur le réseau (ou en transit) vers le SVM ONTAP. Vous empêchez ainsi les attaques par réexécution et les attaques de l'homme du milieu malveillantes contre les données sensibles lorsqu'elles sont en transit.

À partir de la version ONTAP 9.8, IPsec offre la prise en charge du chiffrement de bout en bout pour l'ensemble du trafic IP entre un client et un SVM ONTAP. Le cryptage de données IPSec pour tout le trafic IP inclut les protocoles NFS, iSCSI et SMB/CIFS. IPSec fournit la seule option de cryptage en vol pour le trafic iSCSI.

Le chiffrement NFS sur le réseau est l'un des principaux cas d'utilisation d'IPsec. Avant ONTAP 9.8, le chiffrement NFS over-the-wire exigeait l'installation et la configuration de Kerberos pour utiliser krb5p afin de chiffrer les données NFS à la volée. Ce n'est pas toujours simple ou facile à accomplir dans chaque environnement client.

Les clients qui utilisent des technologies de chiffrement des données au repos, telles que NetApp Storage Encryption (NSE) ou NetApp Volume Encryption (NVE) et Cluster Peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre le client et le stockage dans l'ensemble de leur structure de données multicloud hybride en passant à ONTAP 9.8 ou version ultérieure et en utilisant IPSec :

IPSec est une norme IETF. ONTAP utilise IPsec en mode transport. Il utilise également le protocole Internet Key Exchange (IKE) version 2, qui utilise une clé communiquée à l'avance (PSK) pour négocier les éléments clés entre le client et ONTAP avec IPv4 ou IPv6. Par défaut, IPsec utilise le chiffrement Suite-B AES-GCM 256 bits. Les normes Suite-B AES-GMAC256 et AES-CBC256 avec cryptage 256 bits sont également prises en charge.

Bien que la fonctionnalité IPsec doive être activée sur le cluster, elle s'applique aux adresses IP de SVM individuelles via l'utilisation d'une entrée de base de données de stratégie de sécurité (SPD). L'entrée de règle (SPD) contient l'adresse IP du client (sous-réseau IP distant), l'adresse IP du SVM (sous-réseau IP local), la suite de chiffrement à utiliser et le secret prépartagé (PSK) requis pour l'authentification via IKEv2 et l'établissement de la connexion IPsec. En plus de l'entrée de stratégie IPSec, le client doit être configuré avec les mêmes informations (IP locale et distante, PSK et suite de chiffrement) avant que le trafic puisse circuler sur la connexion IPsec. À partir de ONTAP 9.10.1, la prise en charge de l'authentification par certificat IPsec est ajoutée. Ceci supprime les limites de stratégie IPsec et active la prise en charge du système d'exploitation Windows pour IPsec.

S'il y a un pare-feu entre le client et l'adresse IP du SVM, il doit permettre aux protocoles ESP et UDP (port 500 et 4500), tant entrants (entrée) que sortants (sortie), de réussir la négociation IKEv2 et ainsi d'autoriser le trafic IPsec.

Pour NetApp SnapMirror et le chiffrement du trafic de peering de cluster, le chiffrement de peering de cluster (CPE) est toujours recommandé sur IPsec pour assurer la sécurité en transit sur le réseau. CPE fonctionne mieux pour ces charges de travail que IPSec. Vous n'avez pas besoin d'une licence pour IPsec et il n'y a pas de restrictions d'importation ou d'exportation.

Vous pouvez activer IPsec sur le cluster et créer une entrée SPD pour un seul client et une adresse IP de SVM unique, comme dans l'exemple suivant :

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

Gestion TLS et SSL

Vous pouvez activer le mode de conformité FIPS 140-2/3 pour les interfaces du plan de contrôle en configurant le `is-fips-enabled` paramètre sur true avec la commande ONTAP `security config modify`.

À partir de ONTAP 9, vous pouvez activer le mode de conformité FIPS 140-2 pour les interfaces du plan de contrôle au niveau du cluster. Par défaut, le mode FIPS 140-2 uniquement est désactivé. Vous pouvez activer le mode de conformité FIPS 140-2 en définissant le `is-fips-enabled` paramètre sur `true` pour la `security config modify` commande. Vous pouvez ensuite utiliser `security config show command` pour confirmer l'état de la connexion.

Lorsque la conformité FIPS 140-2 est activée, TLSv1 et SSLv3 sont désactivés et seuls les modèles TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer TLSv1 et SSLv3 lorsque la conformité FIPS 140-2 est activée. Si vous activez FIPS 140-2 puis désactivez-le par la suite, TLSv1 et SSLv3 restent désactivés, mais TLSv1.2 ou TLSv1.1 et TLSv1.2 restent activés, selon la configuration précédente.

La `security config modify` commande modifie la configuration de sécurité existante au niveau du cluster. Si vous activez le mode conforme FIPS, le cluster ne sélectionne automatiquement que les protocoles

TLS. Utilisez le `-supported-protocols` paramètre pour inclure ou exclure des protocoles TLS indépendamment du mode FIPS. Par défaut, le mode FIPS est désactivé et ONTAP prend en charge les protocoles TLSv1.2, TLSv1.1 et TLSv1.

Pour une compatibilité descendante, ONTAP prend en charge l'ajout de SSLv3 à la `supported-protocols` liste lorsque le mode FIPS est désactivé. Utilisez le `-supported-cipher-suites` paramètre pour configurer uniquement AES (Advanced Encryption Standard) ou AES et 3DES. Vous pouvez également désactiver les chiffrements faibles tels que RC4 en spécifiant !RC4. Par défaut, le paramètre de chiffrement pris en charge est `ALL:!LOW:!aNULL:!EXP:!eNULL`. Ce paramètre signifie que toutes les suites de chiffrement prises en charge pour les protocoles sont activées, à l'exception de celles qui n'ont pas d'authentification, pas de cryptage, pas d'exportations et des suites de chiffrement à faible cryptage. Ces suites utilisent des algorithmes de cryptage 64 bits ou 56 bits.

Sélectionnez une suite de chiffrement disponible avec le protocole sélectionné correspondant. Une configuration non valide peut entraîner l'échec de certaines fonctionnalités.

Pour connaître la syntaxe correcte de la chaîne de chiffrement, reportez-vous à la "chiffrement" page sur OpenSSL (publiée par la fondation du logiciel OpenSSL). Depuis ONTAP 9.9.1 et les versions ultérieures, il n'est plus nécessaire de redémarrer manuellement tous les nœuds après avoir modifié la configuration de sécurité.

L'activation de la conformité FIPS 140-2 a des effets sur d'autres systèmes et communications internes et externes à ONTAP 9. NetApp recommande vivement de tester ces paramètres sur un système hors production disposant d'un accès à la console.

> Si SSH est utilisé pour administrer ONTAP 9, vous devez utiliser un client OpenSSH 5.7 ou une version ultérieure. Les clients SSH doivent négocier avec l'algorithme de clé publique ECDSA (Elliptic Curve Digital Signature Algorithm) pour que la connexion réussisse.

La sécurité TLS peut être renforcée en activant uniquement TLS 1.2 et en utilisant des suites de chiffrement compatibles PFS (Perfect Forward Secret). PFS est une méthode d'échange de clés qui, lorsqu'elle est utilisée en combinaison avec des protocoles de chiffrement tels que TLS 1.2, empêche un attaquant de déchiffrer toutes les sessions réseau entre un client et un serveur. Pour activer uniquement les suites de chiffrement TLS 1.2 et PFS, utilisez la commande du niveau de privilège avancé, `security config modify` comme indiqué dans l'exemple suivant.

> Avant de modifier la configuration de l'interface SSL, il est important de se rappeler que le client doit prendre en charge le chiffrement mentionné (DHE, ECDHE) lors de la connexion à ONTAP. Sinon, la connexion n'est pas autorisée.

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirmez `y` pour chaque invite. Pour plus d'informations sur PFS, voir "Ce blog NetApp".

À partir de la prise en charge de ONTAP 9.11.1 et TLS 1.3, vous pouvez valider FIPS 140-3.

> La configuration FIPS s'applique à ONTAP et au contrôleur BMC de la plate-forme.

Créez un certificat numérique signé par une autorité de certification

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web ONTAP n'est pas conforme à leurs politiques InfoSec. Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou du SVM en tant que serveur SSL pour NetApp.

Vous pouvez utiliser `security certificate generate-csr` la commande pour générer une requête de signature de certificat (CSR) et la `security certificate install` commande pour installer le certificat que vous recevez de l'autorité de certification.

Étapes

1. Pour créer un certificat numérique signé par l'autorité de certification de l'organisation, procédez comme suit :
   a. Générer une RSC.
   b. Suivez la procédure de votre organisation pour demander un certificat numérique à l'aide de la RSC auprès de l'autorité de certification de votre organisation. Par exemple, à l'aide de l'interface Web Microsoft Active Directory Certificate Services, accédez à `<CA_server_name>/certsrv` et demandez un certificat.
   c. Installez le certificat numérique dans ONTAP.

Protocole d'état du certificat en ligne

Le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent des communications TLS ou LDAP de recevoir le statut du certificat numérique lorsque OCSP est activé. L'application reçoit une réponse signée indiquant que le certificat demandé est valide, révoqué ou inconnu.

OCSP permet de déterminer le statut actuel d'un certificat numérique sans nécessiter de listes de révocation de certificats.

Par défaut, la vérification du statut du certificat OCSP est désactivée. Il peut être activé à l'aide de la commande `security config ocsp enable -app name`, où le nom de l'application peut être `autosupport`, `audit_log` `fabricpool` `ems`, , , , , `kmip` `ldap_ad` `ldap_nis_namemap`, ou tous. La commande nécessite un niveau de privilège avancé.

Gestion SSHv2

`security ssh modify`La commande remplace les configurations existantes des algorithmes d'échange de clés SSH, des chiffrements ou des algorithmes MAC pour le cluster ou un SVM par les paramètres de configuration que vous spécifiez.

Recommandation NetApp :

- Utilisez des mots de passe pour les sessions utilisateur.
- Utiliser une clé publique pour accéder à la machine.

Chiffrements et échanges de clés pris en charge

Chiffrement	Échange de clés
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-Group-Exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-groupe14-sha1 (SHA-1)
aes256-cbc	diffie-hellman-groupe1-sha1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Cryptage symétrique AES et 3DES pris en charge

ONTAP prend également en charge les types de chiffrement symétrique AES et 3DES suivants (également appelés chiffrement) :

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm

- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

La configuration de gestion SSH s'applique à ONTAP et au contrôleur BMC de la plate-forme.

NetApp AutoSupport

La fonction AutoSupport de ONTAP vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque le système de stockage est configuré pour la première fois. De plus, AutoSupport commence à envoyer des messages au support technique NetApp 24 heures après son activation. Cette période de 24 heures est configurable. Pour tirer parti de la communication avec l'équipe de support interne d'une entreprise, la configuration de l'hôte de messagerie doit être effectuée.

Seul l'administrateur du cluster peut effectuer la gestion AutoSupport (configuration). L'administrateur du SVM n'a pas accès à AutoSupport. La fonction AutoSupport peut être désactivée. Toutefois, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes en cas de problème sur le système de stockage. Par défaut, le système collecte les informations AutoSupport et les stocke localement même si vous désactivez AutoSupport.

Pour plus d'informations sur les messages AutoSupport, notamment sur ce qui se trouve dans les différents messages et sur l'emplacement d'envoi des différents types de messages, reportez-vous à la "Conseiller digital NetApp Active IQ" documentation.

Les messages AutoSupport contiennent des données sensibles, notamment, mais sans s'y limiter, les éléments suivants :

- Fichiers journaux
- Données contextuelles concernant des sous-systèmes spécifiques
- Données de configuration et d'état
- Les données de performance

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.

De plus, vous devez utiliser `system node autosupport modify` la commande pour spécifier les cibles des données AutoSupport (par exemple, le support technique NetApp, les opérations internes d'une entreprise ou les partenaires). Cette commande vous permet également d'indiquer quelles informations AutoSupport spécifiques envoyer (par exemple, données de performances, fichiers journaux, etc.).

Pour désactiver entièrement AutoSupport, utilisez `system node autosupport modify -state disable` la commande.

Protocole de temps réseau

Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec au moins trois serveurs NTP externes.

Les problèmes peuvent survenir lorsque l'heure du cluster est incorrecte. Bien que ONTAP vous permette de définir manuellement le fuseau horaire, la date et l'heure sur le cluster, vous devez configurer les serveurs NTP (Network Time Protocol) afin de synchroniser l'heure du cluster avec les serveurs NTP externes.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Vous pouvez associer un maximum de 10 serveurs NTP externes à l'aide de la `cluster time-service ntp server create` commande. Pour la redondance et la qualité du service de temps, vous devez associer au moins trois serveurs NTP externes au cluster.

Pour plus de détails sur la configuration de NTP dans ONTAP, reportez-vous à la section "Gestion de l'heure du cluster (administrateurs du cluster uniquement)".

Comptes locaux du système de fichiers NAS (groupe de travail CIFS)

L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Utilisez `vserver cifs session show` la commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et le type d'authentification.

À partir de ONTAP 9, vous pouvez configurer un serveur CIFS dans un groupe de travail avec des clients CIFS qui s'authentifient auprès du serveur à l'aide d'utilisateurs et de groupes définis localement. L'authentification des clients de groupe de travail offre une couche de sécurité supplémentaire à la solution ONTAP, qui est conforme à une posture d'authentification de domaine traditionnelle. Pour configurer le serveur CIFS, utilisez `vserver cifs create` la commande. Une fois le serveur CIFS créé, vous pouvez le joindre à un domaine CIFS ou le joindre à un groupe de travail. Pour rejoindre un groupe de travail, utilisez le `-workgroup` paramètre. Voici un exemple de configuration :

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Un serveur CIFS en mode groupe de travail prend uniquement en charge l'authentification Windows NT LAN Manager (NTLM) et ne prend pas en charge l'authentification Kerberos.

NetApp recommande d'utiliser la fonction d'authentification NTLM avec des groupes de travail CIFS pour maintenir la sécurité de votre entreprise. Pour valider la posture de sécurité CIFS, NetApp recommande d'utiliser la `vserver cifs session show` commande pour afficher de nombreuses informations relatives au positionnement, notamment les informations IP, le mécanisme d'authentification, la version du protocole et le type d'authentification.

Audit du système de fichiers NAS

Les systèmes de fichiers NAS occupent une place de plus en plus importante dans le paysage actuel des menaces. Les fonctions d'audit sont essentielles pour assurer la visibilité des menaces.

La sécurité nécessite une validation. ONTAP 9 propose davantage d'événements d'audit et de détails dans l'ensemble de la solution. Dans la mesure où les menaces pèsent aujourd'hui sur les systèmes de fichiers NAS, les fonctions d'audit jouent un rôle essentiel pour assurer la visibilité. Grâce aux fonctionnalités d'audit améliorées de ONTAP 9, les informations d'audit CIFS sont plus que jamais abondantes. Les détails clés, y compris les suivants, sont consignés avec les événements créés :

- Accès aux fichiers, aux dossiers et au partage
- Fichiers créés, modifiés ou supprimés
- Accès en lecture du fichier réussi
- Échec des tentatives de lecture ou d'écriture des fichiers
- Modification des autorisations sur les dossiers

Créer une configuration d'audit

Vous devez activer l'audit CIFS pour générer des événements d'audit. Utiliser `vserver audit create` la commande pour créer une configuration d'audit. Par défaut, le journal d'audit utilise une méthode de rotation basée sur la taille. Vous pouvez utiliser une option de rotation basée sur le temps si elle est spécifiée dans le champ Paramètres de rotation. Les détails supplémentaires de la configuration de rotation de l'audit de journal incluent le planning de rotation, les limites de rotation, les jours de rotation de la semaine et la taille de rotation. Le texte suivant fournit un exemple de configuration d'audit utilisant une rotation mensuelle planifiée pour tous les jours de la semaine à 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Événements d'audit CIFS

Les événements d'audit CIFS sont les suivants :

- **Partage de fichiers** : génère un événement d'audit lorsqu'un partage réseau CIFS est ajouté, modifié ou supprimé à l'aide des commandes associées `vserver cifs share` .
- **Changement de stratégie d'audit** : génère un événement d'audit lorsque la stratégie d'audit est désactivée, activée ou modifiée à l'aide des commandes associées `vserver audit` .
- **Compte utilisateur** : génère un événement d'audit lorsqu'un utilisateur CIFS ou UNIX local est créé ou supprimé ; un compte utilisateur local est activé, désactivé ou modifié ; ou un mot de passe est réinitialisé ou modifié. Cet événement utilise la `vserver cifs users-and-groups local-group` commande ou la commande associée `vserver services name-service unix-user` .
- **Groupe de sécurité** : génère un événement d'audit lorsqu'un groupe de sécurité local CIFS ou UNIX est créé ou supprimé à l'aide de la `vserver cifs users-and-groups local-group` commande ou de la commande associée `vserver services name-service unix-group` .

- **Changement de stratégie d'autorisation** : génère un événement d'audit lorsque des droits sont accordés ou révoqués pour un utilisateur CIFS ou un groupe CIFS à l'aide de la `vserver cifs users-and-groups privilege` commande.

Cette fonctionnalité est basée sur la fonction d'audit du système, qui permet à un administrateur de vérifier ce que le système autorise et exécute du point de vue d'un utilisateur de données.

Effet des API REST sur l'audit NAS

ONTAP permet aux comptes d'administrateur d'accéder aux fichiers SMB/CIFS ou NFS et de les manipuler à l'aide d'API REST. Bien que les API REST puissent uniquement être exécutées par les administrateurs ONTAP, les commandes de l'API REST contournent le journal d'audit NAS du système. En outre, les administrateurs ONTAP peuvent également ignorer les autorisations liées aux fichiers lors de l'utilisation des API REST. Cependant, les actions de l'administrateur avec les API REST sur les fichiers sont capturées dans le journal de l'historique des commandes du système.

Créez un rôle d'API REST sans accès

Vous pouvez empêcher les administrateurs ONTAP d'utiliser des API REST pour l'accès aux fichiers en créant un rôle d'API REST qui n'a pas accès aux volumes ONTAP via REST. Pour configurer ce rôle, procédez comme suit.

Étapes

1. Créez un nouveau rôle REST qui n'a pas accès aux volumes de stockage mais qui dispose de tout autre accès API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Attribuez le compte administrateur au nouveau rôle d'API REST que vous avez créé à l'étape précédente.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

Pour empêcher le compte d'administrateur de cluster ONTAP intégré d'utiliser les API REST pour accéder aux fichiers, vous devez d'abord "créez un nouveau compte administrateur et désactivez ou supprimez le compte intégré".

Configuration et activation de la signature et du chiffrement SMB CIFS

Vous pouvez configurer et activer la signature SMB qui protège la sécurité de la Data Fabric en veillant à ce que le trafic entre les systèmes de stockage et les clients ne soit pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu.

La signature SMB assure la protection en vérifiant que les messages SMB ont une signature valide.

Description de la tâche

Le protocole SMB constitue un vecteur de menaces courant pour les systèmes de fichiers et les architectures. Pour résoudre ce problème, la solution ONTAP 9 utilise la signature et le chiffrement SMB standard. La signature SMB protège la sécurité du maillage Data Fabric en s'assurant que le trafic entre les systèmes de stockage et les clients n'est pas compromis par des attaques par réexécution ou des attaques de l'homme du milieu. Il vérifie que les messages SMB ont une signature valide.

Bien que la signature SMB soit désactivée par défaut dans l'intérêt des performances, NetApp vous recommande fortement de l'activer. En outre, la solution ONTAP prend en charge le chiffrement SMB. Cette approche permet le transport sécurisé des données partage par partage. Le chiffrement SMB est désactivé par défaut. Cependant, NetApp vous recommande d'activer le chiffrement SMB.

La signature et le chiffrement LDAP sont désormais pris en charge dans SMB 2.0 et versions ultérieures. La signature (protection contre toute falsification) et le chiffrement (chiffrement) assurent une communication sécurisée entre les SVM et les serveurs Active Directory. Le chiffrement accéléré des nouvelles instructions AES (Intel AES ni) est désormais pris en charge par SMB 3.0 et les versions ultérieures. Intel AES ni améliore l'algorithme AES et accélère le chiffrement des données pour toute la gamme de processeurs compatibles.

Étapes

1. Pour configurer et activer la signature SMB, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-signing-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Pour configurer et activer le chiffrement SMB et le chiffrement, utilisez `vserver cifs security modify` la commande et vérifiez que le `-is-smb-encryption-required` paramètre est défini sur `true`. Voir l'exemple de configuration suivant :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Sécurisation NFS

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client d'un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment gérer les

demandes d'accès client. Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy.

Le contrôle d'accès est essentiel au maintien d'une posture de sécurité. Par conséquent, ONTAP utilise la fonctionnalité export policy pour limiter l'accès au volume NFS aux clients correspondant à des paramètres spécifiques. Les export-policy contiennent une ou plusieurs règles d'exportation qui traitent chaque requête d'accès client. Une export policy est associée à chaque volume afin de configurer l'accès client au volume. Le résultat de ce processus détermine si le client est autorisé ou refusé (avec un message d'autorisation refusée) à accéder au volume. Ce processus détermine également le niveau d'accès fourni au volume.

Pour que les clients puissent accéder aux données, une export policy doit exister sur un SVM. Un SVM peut contenir plusieurs export policies.

L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Les règles d'exportation déterminent les autorisations d'accès client en appliquant les critères suivants :

- Protocole d'accès aux fichiers utilisé par le client qui envoie la requête (par exemple, NFSv4 ou SMB)
- Un identifiant client (par exemple, le nom d'hôte ou l'adresse IP)
- Type de sécurité utilisé par le client pour l'authentification (par exemple, Kerberos v5, NTLM ou AUTH_SYS)

Si une règle spécifie plusieurs critères et que le client ne correspond pas à un ou plusieurs d'entre eux, la règle ne s'applique pas.

Un exemple de export-policy contient une règle d'export avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Le type de sécurité détermine le niveau d'accès qu'un client reçoit. Les trois niveaux d'accès sont lecture seule, lecture-écriture et superutilisateur (pour les clients avec l'ID utilisateur `0`). Comme le niveau d'accès déterminé par le type de sécurité est évalué dans cet ordre, vous devez respecter les règles répertoriées :

Règles pour les paramètres de niveau d'accès dans les règles d'exportation

Pour qu'un client obtienne les niveaux d'accès suivants	Ces paramètres d'accès doivent correspondre au type de sécurité du client
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`)
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`

Pour qu'un client obtienne les niveaux d'accès suivants	Ces paramètres d'accès doivent correspondre au type de sécurité du client
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- Toutes
- Aucune
- Jamais

Ces types de sécurité ne peuvent pas être utilisés avec le `-superuser` paramètre :

- krb5
- ntlm
- system

Règles pour les résultats des paramètres d'accès

Si le type de sécurité du client …	Puis …
Correspond à un type de sécurité spécifié dans le paramètre d'accès.	Le client reçoit l'accès pour ce niveau avec son propre ID utilisateur.
Ne correspond pas à un type de sécurité spécifié, mais le paramètre d'accès inclut l'option `none`.	Le client reçoit l'accès pour ce niveau et reçoit l'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.
Ne correspond pas à un type de sécurité spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Le client ne reçoit aucun accès pour ce niveau. Cette restriction ne s'applique pas au `-superuser` paramètre car ce paramètre n'inclut toujours aucune, même si elle n'est pas spécifiée.

Kerberos 5 et Krb5p

À partir de ONTAP 9, l'authentification Kerberos 5 avec service Privacy (krb5p) est prise en charge. Le mode d'authentification krbp5 est sécurisé et offre une protection contre la falsification et l'espionnage des données. Il utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. La solution ONTAP prend en charge le chiffrement AES 128 bits et 256 bits pour Kerberos. Le service de confidentialité comprend la vérification de l'intégrité des données reçues, l'authentification des utilisateurs et le cryptage des données avant leur transmission.

L'option krb5p est la plus présente dans la fonctionnalité export policy, où elle est définie comme option de cryptage. La méthode d'authentification krb5p peut être utilisée comme paramètre d'authentification, comme illustré dans l'exemple suivant :

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Activez la signature et le chiffrement du protocole d'accès aux répertoires légers

La signature et le chiffrement sont pris en charge pour permettre la sécurité des sessions lors de requêtes vers un serveur LDAP. Cette approche offre une alternative à la sécurité des sessions LDAP-over-TLS.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Les paramètres de sécurité de session sur un SVM correspondent à ceux disponibles sur le serveur LDAP. Par défaut, la signature et le chiffrement LDAP sont désactivés.

Étapes

1. Pour activer cette fonction, exécutez la `vserver cifs security modify` commande avec le `session-security-for-ad-ldap` paramètre.

   Options des fonctions de sécurité LDAP :

   - **Aucun** : par défaut, pas de signature ou de chiffrement
   - **Sign** : signer le trafic LDAP
   - **Sceau** : signer et crypter le trafic LDAP

   > Les paramètres de signe et de sceau sont cumulatifs, ce qui signifie que si l'option de signe est utilisée, le résultat est LDAP avec signature. Cependant, si l'option de joint est utilisée, le résultat est à la fois signe et joint. En outre, si aucun paramètre n'est spécifié pour cette commande, la valeur par défaut est aucun.

   Voici un exemple de configuration :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Créez et utilisez un NetApp FPolicy

Vous pouvez créer et utiliser un composant d'infrastructure FPolicy de la solution ONTAP, qui permet à des applications partenaires de surveiller et définir les autorisations d'accès aux fichiers. L'une des applications les plus puissantes est Storage Workload Security, une application SaaS NetApp qui offre une visibilité et un contrôle centralisés sur tous les accès aux données de l'entreprise dans les environnements de cloud hybride afin d'assurer la conformité et la sécurité.

Le contrôle d'accès est un concept de sécurité clé. La visibilité des accès aux fichiers et des opérations sur fichiers ainsi que la possibilité d'y réagir sont critiques pour maintenir le niveau de sécurité requis. Pour fournir cette visibilité et ce contrôle d'accès aux fichiers, la solution ONTAP utilise la fonction NetApp FPolicy.

Les règles peuvent être définies en fonction des types de fichiers. FPolicy détermine la façon dont le système de stockage gère les requêtes de chaque système client pour des opérations telles que les créations, ouvertures, renommages et suppressions. Depuis ONTAP 9, le système de notification d'accès aux fichiers FPolicy possède des commandes de filtrage et supporte de brèves coupures de réseau.

Étapes

1. Pour exploiter la fonction FPolicy, vous devez d'abord créer la règle FPolicy avec la `vserver fpolicy policy create` commande.

   > En outre, utilisez le `-events` paramètre si vous utilisez FPolicy pour la visibilité et la collecte des événements. La granularité supplémentaire fournie par ONTAP permet de filtrer les données et d'accéder au niveau de contrôle par nom d'utilisateur. Pour contrôler les privilèges et l'accès avec des noms d'utilisateur, spécifiez le `-privilege-user-name` paramètre.

   Le texte suivant fournit un exemple de création FPolicy :

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. Une fois que vous avez créé la règle FPolicy, vous devez l'activer avec `vserver fpolicy enable` la commande. Cette commande définit également la priorité ou la séquence de l'entrée FPolicy.

   > La séquence FPolicy est importante car, si plusieurs règles ont souscrit au même événement d'accès aux fichiers, la séquence détermine l'ordre dans lequel l'accès est accordé ou refusé.

   Le texte suivant fournit un exemple de configuration pour l'activation de la règle FPolicy et la validation de la configuration avec la `vserver fpolicy show` commande :

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                  Sequence  Status
Engine
----------------------- ---------------------------- --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

Améliorations de FPolicy

ONTAP 9 inclut les améliorations de FPolicy décrites dans les sections suivantes.

Filtrage des contrôles

De nouveaux filtres sont disponibles pour `SetAttr` et pour la suppression de notifications sur les activités d'annuaire.

Résilience asynchrone

Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

Sécurité de LIF

Une LIF est une adresse IP ou un nom de port mondial (WWPN) avec des caractéristiques associées, telles qu'un rôle, un port d'attache, un nœud d'attache, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau. Il est essentiel de comprendre les caractéristiques de sécurité de chaque rôle de LIF.

Rôles LIF

Les rôles LIF peuvent être les suivants :

- **Data LIF** : une LIF associée à un SVM et utilisée pour communiquer avec les clients.
- **Cluster LIF** : une LIF utilisée pour transporter le trafic intracluster entre les nœuds d'un cluster.
- **Node management LIF** : une LIF qui fournit une adresse IP dédiée pour la gestion d'un nœud particulier dans un cluster.
- **Cluster management LIF** : une LIF qui fournit une interface de gestion unique pour l'ensemble du cluster.

- **Intercluster LIF** : une LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters.

Caractéristiques de sécurité de chaque rôle de LIF

	LIF de données	LIF Cluster	FRV de gestion des nœuds	LIF de gestion de cluster	FRV InterCluster
Nécessite un sous-réseau IP privé ?	Non	Oui.	Non	Non	Non
Nécessite un réseau sécurisé ?	Non	Oui.	Non	Non	Oui.
Politique de pare-feu par défaut	Très restrictif	Entièrement ouvert	Moyen	Moyen	Très restrictif
Le pare-feu est-il personnalisable ?	Oui.	Non	Oui.	Oui.	Oui.

- La LIF de cluster étant complètement ouverte sans règle de pare-feu configurable, elle doit se trouver sur un sous-réseau IP privé sur un réseau isolé et sécurisé.
- Les rôles LIF ne doivent en aucun cas être exposés à Internet.

Pour en savoir plus sur la sécurisation des LIF, consultez le "Configuration des politiques de pare-feu pour les LIF".

Protocole et sécurité des ports

Outre les opérations et fonctions de sécurité intégrées, le renforcement d'une solution doit également inclure des mécanismes de sécurité externe. L'utilisation de dispositifs d'infrastructure supplémentaires, tels que des pare-feu, des systèmes de prévention des intrusions et d'autres dispositifs de sécurité, pour filtrer et limiter l'accès à ONTAP constitue un moyen efficace d'établir et de maintenir une stratégie de sécurité rigoureuse. Ces informations sont un élément clé pour filtrer et limiter l'accès à l'environnement et à ses ressources.

Protocoles et ports couramment utilisés

Service	Port/Protocole	Description
`SSH`	22/TCP	Connexion SSH
`telnet`	23/TCP	Connexion à distance
`Domain`	53/TCP	Serveur de noms de domaine
`HTTP`	80/TCP 80/UDP	HTTP
`rpcbind`	111/TCP 111/UDP	Appel de procédure à distance

Service	Port/Protocole	Description
NTP	123/UDP	Protocole de temps réseau
msrpc	135/UDP	Appel de procédure à distance Microsoft
Netbios-name	137/TCP 137/UDP	Service de noms NetBIOS
netbios-ssn	139/TCP	Session de service NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Lien sécurisé :http
microsoft-ds	445/TCP	Services d'annuaire Microsoft
IPsec	500/UDP	Sécurité du protocole Internet
mount	635/UDP	Montage NFS
named	953/UDP	Nom démon
NFS	2049/UDP 2049/TCP	Démon du serveur NFS
nrv	2050/TCP	Protocole de volume distant NetApp
iscsi	3260/TCP	Port cible iSCSI
Lockd	4045/TCP 4045/UDP	Démon de verrouillage NFS
NFS	4046/TCP	Protocole de montage NFS
acp-proto	4046/UDP	Protocole de comptabilité
rquotad	4049/UDP	Protocole NFS rquotad
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Sécurité du protocole Internet
acp	5125/UDP 5133/UDP 5144/TCP	Autre port de contrôle pour le disque
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Port HTTPS : protocole binaire d'écoute
TELNET	8023/TCP	Nœud-portée Telnet
HTTPS	8443/TCP	Outil 7MTT avec interface graphique via lien:HTTPS
RSH	8514/TCP	Portée du nœud RSH
KMIP	9877/TCP	Port client KMIP (hôte local interne uniquement)
ndmp	10000/TCP	NDMP
cifs port de témoin	40001/TCP	Port témoin CIFS
TLS	50000/TCP	Sécurité de la couche de transport

Service	Port/Protocole	Description
`Iscsi`	65200/TCP	Port iSCSI
`SSH`	65502/TCP	Coque sécurisée
`vsun`	65503/TCP	vsun

Ports internes NetApp

Port/Protocole	Description
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp
931	RPC de cluster NetApp
932	RPC de cluster NetApp
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp

Port/Protocole	Description
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp
7824	RPC de cluster NetApp

Ressources de sécurité

Pour en savoir plus sur les informations décrites dans cette documentation de sécurité ONTAP, consultez les informations supplémentaires et concepts de sécurité suivants.

Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le "Portail de sécurité NetApp".

- "Notes de mise à jour de ONTAP 9"
- "Références des commandes ONTAP 9"
- "Administration de système"

- "Authentification administrateur et RBAC"
- "Chiffrement NetApp"
- "Tr-4647 : authentification multifacteur dans ONTAP 9.3"
- "Chiffrements OPENSSL"
- "CryptoMod FIPS-140-2 de niveau 1"
- "Authentification basée sur certificat avec le SDK de gestion NetApp pour ONTAP"
- "Gestion du réseau"