



Vérifiez l'identité des serveurs distants à l'aide de certificats

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Vérifiez l'identité des serveurs distants à l'aide de certificats 1
 - Vérifiez l'identité des serveurs distants à l'aide de la présentation des certificats 1
 - Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP 1
 - Afficher les certificats par défaut pour les applications basées sur TLS 3

Vérifiez l'identité des serveurs distants à l'aide de certificats

Vérifiez l'identité des serveurs distants à l'aide de la présentation des certificats

ONTAP prend en charge les fonctions de certificat de sécurité pour vérifier l'identité des serveurs distants.

Le logiciel ONTAP permet des connexions sécurisées à l'aide des fonctionnalités et protocoles de certificat numérique suivants :

- Le protocole OCSP (Online Certificate Status Protocol) valide le statut des demandes de certificat numérique des services ONTAP à l'aide de connexions SSL et TLS (transport Layer Security). Cette fonction est désactivée par défaut.
- Un ensemble par défaut de certificats racine de confiance est inclus avec le logiciel ONTAP.
- Les certificats KMIP (Key Management Interoperability Protocol) permettent d'effectuer une authentification mutuelle d'un cluster et d'un serveur KMIP.

Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP

Depuis ONTAP 9.2, le protocole OCSP (Online Certificate Status Protocol) permet aux applications ONTAP qui utilisent les communications TLS (transport Layer Security) de recevoir le statut du certificat numérique lorsque le protocole OCSP est activé. Vous pouvez à tout moment activer ou désactiver les vérifications d'état des certificats OCSP pour des applications spécifiques. Par défaut, la vérification du statut du certificat OCSP est désactivée.

Ce dont vous avez besoin

Vous avez besoin d'un accès de niveau de privilège avancé pour effectuer cette tâche.

Description de la tâche

OCSP prend en charge les applications suivantes :

- AutoSupport
- Système de gestion des événements (EMS)
- LDAP sur TLS
- Protocole KMIP (Key Management Interoperability Protocol)
- Consignation d'audits
- FabricPool
- SSH (à partir de ONTAP 9.13.1)

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`.
2. Pour activer ou désactiver les vérifications du statut des certificats OCSP pour des applications ONTAP spécifiques, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour certaines applications...	Utilisez la commande...
Activé	<code>security config ocsp enable -app app name</code>
Désactivé	<code>security config ocsp disable -app app name</code>

La commande suivante active la prise en charge OCSP pour AutoSupport et EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Lorsque OCSP est activé, l'application reçoit l'une des réponses suivantes :

- Bon - le certificat est valide et la communication continue.
 - Révoqué - le certificat est considéré comme non digne de confiance par son autorité de certification émettrice et la communication ne peut pas se poursuivre.
 - Inconnu - le serveur n'a pas d'informations d'état sur le certificat et la communication ne peut pas se poursuivre.
 - Il manque des informations de serveur OCSP dans le certificat. Le serveur agit comme si OCSP est désactivé et continue avec la communication TLS, mais aucune vérification d'état n'a lieu.
 - Aucune réponse du serveur OCSP - l'application ne peut pas continuer.
3. Pour activer ou désactiver les vérifications d'état des certificats OCSP pour toutes les applications utilisant les communications TLS, utilisez la commande appropriée.

Si vous souhaitez que l'état du certificat OCSP soit vérifié pour toutes les applications...	Utilisez la commande...
Activé	<code>security config ocsp enable</code> <code>-app all</code>
Désactivé	<code>security config ocsp disable</code> <code>-app all</code>

Lorsque cette option est activée, toutes les applications reçoivent une réponse signée indiquant le statut du certificat spécifié : bon, révoqué ou inconnu. Dans le cas d'un certificat révoqué, l'application ne pourra pas continuer. Si l'application ne parvient pas à recevoir de réponse du serveur OCSP ou si le serveur est inaccessible, l'application ne pourra pas continuer.

4. Utilisez le `security config oosp show` Commande pour afficher toutes les applications qui prennent en charge OCSP et leur état de support.

```
cluster::*> security config oosp show
Application                                OCSP Enabled?
-----
autosupport                               false
audit_log                                 false
fabricpool                                false
ems                                        false
kmip                                       false
ldap_ad                                   true
ldap_nis_namemap                          true
ssh                                       true

8 entries were displayed.
```

Afficher les certificats par défaut pour les applications basées sur TLS

Depuis ONTAP 9.2, ONTAP fournit un ensemble par défaut de certificats racine de confiance pour les applications ONTAP utilisant TLS (transport Layer Security).

Ce dont vous avez besoin

Les certificats par défaut ne sont installés que sur le SVM d'admin pendant sa création ou lors d'une mise à niveau vers ONTAP 9.2.

Description de la tâche

Les applications actuelles qui agissent en tant que client et qui nécessitent une validation de certificat sont AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Et KMIP.

Lorsque les certificats expirent, un message EMS est appelé pour demander à l'utilisateur de supprimer les certificats. Les certificats par défaut ne peuvent être supprimés qu'au niveau de privilège avancé.



La suppression des certificats par défaut peut entraîner l'absence de fonctionnement de certaines applications ONTAP (par exemple, AutoSupport et Audit Logging).

Étape

1. Vous pouvez afficher les certificats par défaut qui sont installés sur le SVM d'admin en utilisant la commande `Security Certificate show` :

```
security certificate show -vserver -type server-ca
```

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01                AACertificateServices
server-ca
  Certificate Authority: AAA Certificate Services
    Expiration Date: Sun Dec 31 18:59:59 2028
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.