Gestion des certificats de sécurité

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/oncommand-unified-manager-95/online-help/task-viewing-the-https-security-certificate-ocf.html on October 23, 2024. Always check docs.netapp.com for the latest.

Sommaire

Gestion des certificats de sécurité 1
Affichage du certificat de sécurité HTTPS 1
Génération d’un certificat de sécurité HTTPS 1
Téléchargement d’une demande de signature de certificat HTTPS 3
Installation d’un certificat de sécurité HTTPS 4
Descriptions des pages pour la gestion des certificats 5

Gestion des certificats de sécurité

Vous pouvez configurer HTTPS sur le serveur Unified Manager pour surveiller et gérer les clusters via une connexion sécurisée.

Affichage du certificat de sécurité HTTPS

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion chiffrée de votre navigateur à Unified Manager n'est pas interceptée.

Avant de commencer

Vous devez avoir le rôle opérateur, administrateur OnCommand ou administrateur stockage.

Description de la tâche

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher d'autres noms d'URL à partir desquels vous pouvez accéder à Unified Manager.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **certificat HTTPS** dans le menu **Setup**.

   Le certificat HTTPS s'affiche en haut de la page

Une fois que vous avez terminé

Si vous avez besoin d'afficher des informations plus détaillées sur le certificat de sécurité par rapport à ce qui s'affiche sur la page certificat HTTPS, vous pouvez afficher le certificat de connexion dans votre navigateur.

Génération d'un certificat de sécurité HTTPS

Vous pouvez générer un nouveau certificat de sécurité HTTPS pour plusieurs raisons, notamment si vous souhaitez vous connecter à une autre autorité de certification ou si le certificat de sécurité actuel a expiré. Le nouveau certificat remplace le certificat existant.

Avant de commencer

Vous devez avoir le rôle d'administrateur OnCommand.

Description de la tâche

Si vous n'avez pas accès à l'interface utilisateur Web d'Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **certificat HTTPS** dans le menu **Setup**.
2. Cliquez sur **régénérer le certificat HTTPS**.

   La boîte de dialogue régénérer le certificat HTTPS s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la façon dont vous souhaitez générer le certificat :

Les fonctions que vous recherchez…	Procédez comme ça…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **régénérer en utilisant les attributs de certificat actuels**.
Générez le certificat à l'aide de valeurs différentes	`Click the *Update the Current Certificate Attributes* option. Les champs Nom commun et noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez entrer des valeurs, par exemple, pour la ville, l'état et le pays si vous souhaitez que ces valeurs soient renseignées dans le certificat.` Vous pouvez cocher la case « exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager afin que le nouveau certificat prenne effet.

Une fois que vous avez terminé

Vérifiez les nouvelles informations de certificat en consultant le certificat HTTPS.

Redémarrage de la machine virtuelle Unified Manager

Vous pouvez redémarrer le serveur virtuel à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou en cas de problème avec la machine virtuelle.

Avant de commencer

L'appliance virtuelle est sous tension.

En tant qu'utilisateur de maintenance, vous êtes connecté à la console de maintenance.

Description de la tâche

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option **redémarrer invité**. Pour plus d'informations, consultez la documentation VMware.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration du système** > **redémarrer la machine virtuelle**.

Téléchargement d'une demande de signature de certificat HTTPS

Vous pouvez télécharger une demande de certification pour le certificat de sécurité HTTPS actuel afin de pouvoir fournir le fichier à une autorité de certification à signer. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme du milieu et offre une meilleure protection contre la sécurité qu'un certificat auto-signé.

Avant de commencer

Vous devez avoir le rôle d'administrateur OnCommand.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **certificat HTTPS** dans le menu **Setup**.
2. Cliquez sur **Télécharger demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Une fois que vous avez terminé

Vous pouvez fournir le fichier à une autorité de certification pour signer, puis installer le certificat signé.

Installation d'un certificat de sécurité HTTPS

Vous pouvez télécharger et installer un certificat de sécurité une fois qu'une autorité de certification l'a signé et l'a renvoyé. Le fichier que vous téléchargez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme au milieu et offre une meilleure protection contre la sécurité qu'un certificat auto-signé.

Avant de commencer

Vous devez avoir effectué les actions suivantes :

- A téléchargé le fichier de demande de signature de certificat et l'a signé par une autorité de certification
- Enregistré la chaîne de certificats au format PEM
- Inclus tous les certificats de la chaîne, du certificat du serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez avoir le rôle d'administrateur OnCommand.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **certificat HTTPS** dans le menu **Setup**.
2. Cliquez sur **installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **choisir le fichier…** pour localiser le fichier à télécharger.
4. Sélectionnez le fichier, puis cliquez sur **installer** pour l'installer.

Exemple de chaîne de certificat

L'exemple suivant montre comment le fichier de chaîne de certificats peut s'afficher :

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Descriptions des pages pour la gestion des certificats

Vous pouvez utiliser la page certificat HTTPS pour afficher les certificats de sécurité actuels et générer de nouveaux certificats HTTPS.

Page certificat HTTPS

La page certificat HTTPS vous permet d'afficher le certificat de sécurité actuel, de télécharger une demande de signature de certificat, de générer un nouveau certificat HTTPS ou d'installer un nouveau certificat HTTPS.

Si vous n'avez pas généré de nouveau certificat HTTPS, le certificat qui apparaît sur cette page est le certificat qui a été généré lors de l'installation.

Boutons de commande

Les boutons de commande permettent d'effectuer les opérations suivantes :

- **Télécharger demande de signature de certificat HTTPS**

  Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le `<hostname>.csr` Dossier de sorte que vous puissiez fournir le fichier à une autorité de certification à signer.

- **Installer le certificat HTTPS**

  Vous permet de télécharger et d'installer un certificat de sécurité une fois qu'une autorité de certification a signé et renvoyé ce certificat. Le nouveau certificat est en vigueur après le redémarrage du serveur de gestion.

- **Régénérer le certificat HTTPS**

  Vous permet de générer un certificat HTTPS, qui remplace le certificat de sécurité actuel. Le nouveau certificat est en vigueur après le redémarrage d'Unified Manager.

Boîte de dialogue régénérer le certificat HTTPS

La boîte de dialogue régénérer le certificat HTTPS vous permet de personnaliser les informations de sécurité, puis de générer un nouveau certificat HTTPS avec ces informations.

Les informations actuelles sur le certificat apparaissent sur cette page.

Les sélections « régénérer à l'aide des attributs de certificat actuels » et « mettre à jour les attributs de certificat actuels » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

  Obligatoire. Le nom de domaine complet (FQDN) que vous souhaitez sécuriser.

  Dans les configurations haute disponibilité Unified Manager, utilisez l'adresse IP virtuelle.

- **Courriel**

  Facultatif. Une adresse e-mail pour contacter votre organisation, généralement l'adresse e-mail de l'administrateur de certificat ou DU service INFORMATIQUE.

- **Société**

  Facultatif. Généralement le nom incorporé de votre société.

- **Ministère**

  Facultatif. Le nom du service de votre entreprise.

- **Ville**

  Facultatif. La ville de votre entreprise.

- **État**

  Facultatif. L'emplacement de l'État ou de la province, non abrégé, de votre entreprise.

- **Pays**

  Facultatif. Pays de votre entreprise. Il s'agit généralement d'un code ISO à deux lettres du pays.

- **Noms alternatifs**

  Obligatoire. Noms de domaine supplémentaires non primaires pouvant être utilisés pour accéder à ce serveur en plus de l'hôte local existant ou d'autres adresses réseau. Séparez les différents noms par une virgule.

  Cochez la case « exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

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 DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

Informations sur les marques commerciales

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