Gestion des certificats de sécurité

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Sommaire

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.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher les noms des objets (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.

   Le certificat HTTPS s'affiche en haut de la page

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.

Téléchargement d'une demande de signature de certificat HTTPS

Vous pouvez télécharger une demande de signature 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **Télécharger demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

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

L’installation d’une autorité de certification a signé et renvoyé un certificat 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.

Ce dont vous aurez besoin

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 Administrateur d’applications.

Si la validité du certificat pour lequel une RSC a été créée est supérieure à 397 jours, la validité sera réduite à 397 jours par l’AC avant de signer et de retourner le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
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.

   Pour plus d’informations, reportez-vous à la section "Installation d’un certificat HTTPS généré à l’aide d’outils externes".

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-----
```

Installation d'un certificat HTTPS généré à l'aide d'outils externes

Vous pouvez installer des certificats qui sont auto-signés ou qui sont générés à l'aide d'un outil externe tel que OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats car ces certificats sont des paires de clés publiques-privées générées par l'extérieur. Les algorithmes de paire de clés autorisés sont « RSA » et « EC ». L'option **installer le certificat HTTPS** est disponible dans la page certificats HTTPS de la section général. Le fichier que vous téléchargez doit avoir le format d'entrée suivant.

1. Clé privée du serveur appartenant à l'hôte Active IQ Unified Manager
2. Certificat du serveur correspondant à la clé privée
3. Certificat des autorités de certification en sens inverse jusqu'à la racine, qui sont utilisés pour signer le certificat ci-dessus

Format de chargement d'un certificat avec une paire de clés EC

Les courbes autorisées sont « prime256v1 » et « sept-4r1 ». Exemple de certificat avec une paire EC générée en externe :

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----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-----
```

Format de chargement d'un certificat avec une paire de clés RSA

Les tailles de clé autorisées pour la paire de clés RSA appartenant au certificat hôte sont 2048, 3072 et 4096. Certificat avec une paire de clés **RSA générée en externe** :

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----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-----
```

Une fois le certificat téléchargé, vous devez redémarrer l'instance Active IQ Unified Manager pour que les modifications prennent effet.

Vérifie lors du téléchargement de certificats générés en externe

Le système effectue des vérifications pendant le chargement d'un certificat généré à l'aide d'outils externes. Si l'une des vérifications échoue, le certificat est rejeté. Il existe également une validation pour les certificats générés à partir de la RSC dans le produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée de l'entrée est validée par rapport au certificat hôte dans l'entrée.
- Le nom commun (CN) du certificat hôte est vérifié par rapport au FQDN de l'hôte.

- Le nom commun (CN) du certificat hôte ne doit pas être vide ou vide et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être ultérieure et la date d'expiration de validité du certificat ne doit pas être antérieure.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être ultérieure et la date d'expiration de la validité ne doit pas être antérieure.

La clé privée de l'entrée ne doit pas être chiffrée. Si des clés privées sont cryptées, elles sont rejetées par le système.

Exemple 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemple 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemple 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

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 auto-signé ou d'installer un nouveau certificat HTTPS.

Si vous n'avez pas généré de nouveau certificat HTTPS auto-signé, 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 fichier <HOSTNAME>.csr pour 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 nouveau certificat HTTPS auto-signé, 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.

- **TAILLE DE CLÉ (ALGORITHME CLÉ : RSA)**

  L'algorithme clé est défini sur RSA. Vous pouvez choisir parmi l'une des tailles de touches : 2048, 3072 ou 4096 bits. La taille de clé par défaut est de 2048 bits.

- * PÉRIODE DE VALIDITÉ*

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau à partir d'une version précédente, la validité du certificat peut changer.

Pour plus d'informations, voir "Génération de certificats HTTPS".

Informations sur le copyright

Informations sur les marques commerciales