Gestion des certificats

SANtricity 11.6

NetApp
February 12, 2024

Sommaire

Gestion des certificats

Concepts

Fonctionnement des certificats

Les certificats sont des fichiers numériques qui identifient des entités en ligne, telles que des sites Web et des serveurs, pour des communications sécurisées sur Internet.

Certificats signés

Les certificats garantissent que les communications Web sont transmises sous forme cryptée, en privé et sans modification, uniquement entre le serveur et le client spécifiés. Unified Manager vous permet de gérer les certificats du navigateur sur un système de gestion hôte et les contrôleurs des baies de stockage découvertes.

Un certificat peut être signé par une autorité de confiance, ou il peut être auto-signé. La « signature » signifie simplement que quelqu'un a validé l'identité du propriétaire et déterminé que ses appareils peuvent être fiables. Les baies de stockage sont fournies avec un certificat auto-signé généré automatiquement sur chaque contrôleur. Vous pouvez continuer à utiliser les certificats auto-signés ou obtenir des certificats signés par l'autorité de certification pour une connexion plus sécurisée entre les contrôleurs et les systèmes hôtes.

> Bien que les certificats signés par l'autorité de certification offrent une meilleure protection contre la sécurité (par exemple, la prévention des attaques de l'homme au milieu), ils exigent également des frais qui peuvent être coûteux si vous avez un réseau étendu. En revanche, les certificats auto-signés sont moins sûrs, mais ils sont libres. Par conséquent, les certificats auto-signés sont le plus souvent utilisés pour les environnements de test internes, pas dans les environnements de production.

Un certificat signé est validé par une autorité de certification (CA), qui est une organisation tierce de confiance. Les certificats signés incluent des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web), la date de délivrance et d'expiration du certificat, des domaines valides pour l'entité et une signature numérique composée de lettres et de chiffres.

Lorsque vous ouvrez un navigateur et saisissez une adresse Web, votre système exécute un processus de vérification de certificat en arrière-plan pour déterminer si vous vous connectez à un site Web qui inclut un certificat valide signé par une autorité de certification. En général, un site sécurisé avec un certificat signé comprend une icône de cadenas et une désignation https dans l'adresse. Si vous tentez de vous connecter à un site Web qui ne contient pas de certificat signé par une autorité de certification, votre navigateur affiche un avertissement indiquant que le site n'est pas sécurisé.

L'autorité de certification prend des mesures pour vérifier votre identité pendant le processus d'application. Ils peuvent envoyer un e-mail à votre entreprise enregistrée, vérifier votre adresse professionnelle et effectuer une vérification HTTP ou DNS. Lorsque le processus d'application est terminé, l'autorité de certification vous envoie des fichiers numériques à charger sur un système de gestion hôte. Généralement, ces fichiers incluent une chaîne de confiance, comme suit :

- **Root** — en haut de la hiérarchie est le certificat racine, qui contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
- **Intermédiaire** — les ramifications à partir de la racine sont les certificats intermédiaires. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat

serveur protégés.

- **Server** — au bas de la chaîne se trouve le certificat de serveur, qui identifie votre entité spécifique, comme un site Web ou un autre périphérique. Chaque contrôleur d'une matrice de stockage nécessite un certificat de serveur distinct.

Certificats auto-signés

Chaque contrôleur de la baie de stockage comprend un certificat préinstallé et auto-signé. Un certificat auto-signé est similaire à un certificat signé par l'AC, sauf qu'il est validé par le propriétaire de l'entité au lieu d'un tiers. Tout comme un certificat signé par une autorité de certification, un certificat auto-signé contient sa propre clé privée et garantit également que les données sont cryptées et envoyées via une connexion HTTPS entre un serveur et un client.

Les certificats auto-signés ne sont pas « approuvés » par les navigateurs. Chaque fois que vous tentez de vous connecter à un site Web qui ne contient qu'un certificat auto-signé, le navigateur affiche un message d'avertissement. Vous devez cliquer sur un lien dans le message d'avertissement qui vous permet de passer au site Web ; ce faisant, vous acceptez essentiellement le certificat auto-signé.

Certificats pour Unified Manager

L'interface Unified Manager est installée avec le proxy de services Web sur un système hôte. Lorsque vous ouvrez un navigateur et que vous essayez de vous connecter à Unified Manager, le navigateur tente de vérifier que l'hôte est une source de confiance en recherchant un certificat numérique. Si le navigateur ne trouve pas de certificat signé par l'autorité de certification pour le serveur, il ouvre un message d'avertissement. De là, vous pouvez continuer sur le site Web pour accepter le certificat auto-signé pour cette session. Vous pouvez également obtenir des certificats numériques signés auprès d'une autorité de certification afin de ne plus afficher le message d'avertissement.

Certificats pour contrôleurs

Au cours d'une session Unified Manager, des messages de sécurité supplémentaires peuvent s'afficher lorsque vous tentez d'accéder à un contrôleur qui ne possède pas de certificat signé par une autorité de certification. Dans ce cas, vous pouvez faire confiance de façon permanente au certificat auto-signé ou importer les certificats signés par l'autorité de certification pour les contrôleurs afin que le serveur proxy des services Web puisse authentifier les demandes client entrantes de ces contrôleurs.

Terminologie du certificat

Les termes suivants s'appliquent à la gestion des certificats.

Durée	Description
ENV	Une autorité de certification (AC) est une entité de confiance qui délivre des documents électroniques, appelés certificats numériques, pour la sécurité Internet. Ces certificats identifient les propriétaires de sites Web, ce qui permet des connexions sécurisées entre les clients et les serveurs.
CSR	Une demande de signature de certificat (CSR) est un message envoyé par un déposant à une autorité de certification (AC). La RSC valide les informations dont l'AC a besoin pour émettre un certificat.

Durée	Description
Certificat	Un certificat identifie le propriétaire d'un site à des fins de sécurité, ce qui empêche les pirates d'emprunter l'identité du site. Le certificat contient des informations sur le propriétaire du site et l'identité de l'entité de confiance qui certifie (signe) ces informations.
Chaîne de certificat	Hiérarchie de fichiers qui ajoute une couche de sécurité aux certificats. Généralement, la chaîne inclut un certificat racine en haut de la hiérarchie, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les entités.
Certificat intermédiaire	Un ou plusieurs certificats intermédiaires sont débranche de la racine dans la chaîne de certificats. L'AC délivre un ou plusieurs certificats intermédiaires pour agir comme intermédiaires entre un certificat racine et un certificat serveur protégés.
Magasin de clés	Un magasin de clés est un référentiel sur votre système de gestion hôte qui contient des clés privées, ainsi que leurs clés publiques et certificats correspondants. Ces clés et certificats identifient vos propres entités, telles que les contrôleurs.
Certificat racine	Le certificat racine se trouve en haut de la hiérarchie dans la chaîne de certificats et contient une clé privée utilisée pour signer d'autres certificats. La racine identifie une organisation CA particulière. Si vous utilisez la même autorité de certification pour tous vos périphériques réseau, vous n'avez besoin que d'un seul certificat racine.
Certificat signé	Certificat validé par une autorité de certification (CA). Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. En outre, un certificat signé comprend des détails sur le propriétaire de l'entité (généralement un serveur ou un site Web) et une signature numérique composée de lettres et de chiffres. Un certificat signé utilise une chaîne de confiance et est donc le plus souvent utilisé dans les environnements de production. Également appelé « certificat signé par l'autorité de certification » ou « certificat de gestion ».
Certificat auto-signé	Un certificat auto-signé est validé par le propriétaire de l'entité. Ce fichier de données contient une clé privée et garantit que les données sont envoyées sous forme chiffrée entre un serveur et un client via une connexion HTTPS. Il comprend également une signature numérique composée de lettres et de chiffres. Un certificat auto-signé n'utilise pas la même chaîne de confiance qu'un certificat signé par l'autorité de certification et est donc le plus souvent utilisé dans les environnements de test. Également appelé certificat « préinstallé ».
Certificat de serveur	Le certificat du serveur se trouve au bas de la chaîne de certificats. Il identifie votre entité spécifique, telle qu'un site Web ou un autre appareil. Chaque contrôleur d'un système de stockage nécessite un certificat de serveur distinct.

Durée	Description
Magasin de confiance	Un magasin de confiance est un référentiel qui contient des certificats de tiers de confiance, tels que les autorités de certification.
Proxy de services Web	Le proxy de services Web, qui fournit un accès via des mécanismes HTTPS standard, permet aux administrateurs de configurer des services de gestion pour les matrices de stockage. Le proxy peut être installé sur des hôtes Windows ou Linux. L'interface Unified Manager est fournie avec le proxy de services Web.

Comment

Utiliser des certificats signés CA

Vous pouvez obtenir et importer des certificats signés par une autorité de certification pour un accès sécurisé au système de gestion hébergeant Unified Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

L'utilisation de certificats signés CA est une procédure en deux étapes.

Étape 1 : remplir et soumettre une RSC

Vous devez d'abord générer un fichier de demande de signature de certificat (CSR) et l'envoyer à l'autorité de certification.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche décrit comment générer le fichier CSR que vous envoyez à une autorité de certification pour recevoir des certificats de gestion signés pour le système hébergeant Unified Manager et le proxy des services Web. Vous devez fournir des informations sur votre organisation, ainsi que l'adresse IP ou le nom DNS du système hôte.

> Ne générez pas de nouvelle RSC après la soumission à l'AC. Lorsque vous générez une RSC, le système crée une paire de clés privée et publique. La clé publique fait partie de la RSC, tandis que la clé privée est conservée dans le magasin de clés. Lorsque vous recevez les certificats signés et que vous les importez dans le magasin de clés, le système s'assure que les clés privées et publiques sont la paire d'origine. Par conséquent, vous ne devez pas générer de nouvelle RSC après en avoir soumis une à l'autorité de certification. Dans ce cas, les contrôleurs génèrent de nouvelles clés et les certificats que vous recevez de l'autorité de certification ne fonctionneront pas.

Étapes

1. Sélectionnez **gestion des certificats**.

2. Dans l'onglet **Management**, sélectionnez **Complete CSR**.
3. Entrez les informations suivantes, puis cliquez sur **Suivant** :
   - **Organisation** — le nom légal complet de votre entreprise ou organisation. Inclure les suffixes, tels que Inc. Ou Corp
   - **Unité organisationnelle (facultative)** — la division de votre organisation qui gère le certificat.
   - **Ville/localité** — la ville où votre système hôte ou entreprise est situé.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre système hôte ou votre entreprise.
   - **Code ISO de pays** — le code ISO à deux chiffres de votre pays (Organisation internationale de normalisation), tel que les États-Unis.
4. Entrez les informations suivantes sur le système hôte :
   - **Nom commun** — l'adresse IP ou le nom DNS du système hôte sur lequel le proxy de services Web est installé. Assurez-vous que cette adresse est correcte ; elle doit correspondre exactement à ce que vous entrez pour accéder à Unified Manager dans le navigateur. Ne pas inclure http:// ou https://.
   - **Adresses IP alternatives** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules.
   - **Noms DNS alternatifs** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le système hôte. Pour plusieurs entrées, utilisez un format délimité par des virgules. S'il n'y a pas de noms DNS alternatifs, mais que vous avez saisi un nom DNS dans le premier champ, copiez ce nom ici.
5. Cliquez sur **Terminer**.

   Un fichier CSR est téléchargé sur votre système local. L'emplacement du dossier de téléchargement dépend de votre navigateur.

6. Soumettez le fichier CSR à une autorité de certification et demandez des certificats signés au format PEM ou DER.

Une fois que vous avez terminé

Attendez que l'autorité de certification retourne les fichiers de certificat, puis allez à "Étape 2 : certificats de gestion des importations".

Étape 2 : certificats de gestion des importations

Une fois les certificats signés reçus, importez la chaîne de certificats du système hôte sur lequel l'interface Unified Manager est installée.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Vous avez généré une demande de signature de certificat (.CSR file) et l'avez envoyée à l'autorité de certification.
- L'autorité de certification a renvoyé des fichiers de certificat approuvés.
- Les fichiers de certificat sont installés sur votre système local.
- Si l'autorité de certification a fourni un certificat enchaîné (par exemple, un fichier .p7b), vous devez déballer le fichier chaîné dans des fichiers individuels : le certificat racine, un ou plusieurs certificats intermédiaires et le certificat de serveur. Vous pouvez utiliser Windows `certmgr` Utilitaire pour

décompresser les fichiers (cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches › Exporter**). Une fois les exportations terminées, un fichier CER est affiché pour chaque fichier de certificat de la chaîne.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet **Management**, sélectionnez **Import**.

   Une boîte de dialogue s'ouvre pour importer les fichiers de certificat.

3. Cliquez sur **Parcourir** pour sélectionner d'abord les fichiers racine et intermédiaire, puis sélectionnez le certificat du serveur.

   Les noms de fichier s'affichent dans la boîte de dialogue.

4. Cliquez sur **Importer**.

Résultats

Les fichiers sont chargés et validés. Les informations de certificat s'affichent sur la page gestion des certificats.

Réinitialisez les certificats de gestion

Vous pouvez rétablir le certificat de gestion à l'état d'origine auto-signé en usine.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Description de la tâche

Cette tâche supprime le certificat de gestion actuel du système hôte sur lequel le proxy de services Web et SANtricity Unified Manager sont installés. Une fois le certificat réinitialisé, le système hôte reprend à l'aide du certificat auto-signé.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Dans l'onglet **Management**, sélectionnez **Reset**.

   Une boîte de dialogue **confirmer la réinitialisation du certificat de gestion** s'ouvre.

3. Type `reset` Dans le champ, puis cliquez sur **Réinitialiser**.

   Une fois que votre navigateur a été actualisé, le navigateur risque de bloquer l'accès au site de destination et de signaler que le site utilise HTTP strict transport Security. Cette condition survient lorsque vous revenez à des certificats auto-signés. Pour effacer la condition qui bloque l'accès à la destination, vous devez effacer les données de navigation du navigateur.

Résultats

Le système revient à utiliser le certificat auto-signé à partir du serveur. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Importer des certificats pour les tableaux

Si nécessaire, vous pouvez importer des certificats pour les baies de stockage afin qu'ils puissent s'authentifier auprès du système qui héberge SANtricity Unified Manager. Les certificats peuvent être signés par une autorité de certification ou être auto-signés.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.
- Si vous importez des certificats approuvés, les certificats doivent être importés pour les contrôleurs de la matrice de stockage à l'aide de SANtricity System Manager.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Importer › certificats** pour importer un certificat CA ou **Importer › certificats de matrice de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

4. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.

Afficher les certificats

Vous pouvez afficher les informations récapitulatives d'un certificat, y compris l'organisation utilisant le certificat, l'autorité qui a émis le certificat, la période de validité et les empreintes digitales (identifiants uniques).

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Sinon, les fonctions de certificat n'apparaissent pas.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Pour plus d'informations sur un certificat, sélectionnez sa ligne, les points de suspension à la fin de la ligne, puis cliquez sur **View** ou **Export**.

Exporter les certificats

Vous pouvez exporter un certificat pour en afficher les détails complets.

Avant de commencer

Pour ouvrir le fichier exporté, vous devez disposer d'une application de visionneuse de certificats.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'un des onglets suivants :
   - **Management** — affiche le certificat pour le système hébergeant le proxy de services Web. Un certificat de gestion peut être auto-signé ou approuvé par une autorité de certification (AC). Cette fonctionnalité permet un accès sécurisé à Unified Manager.
   - **Trusted** — affiche les certificats auxquels Unified Manager peut accéder pour les matrices de stockage et les autres serveurs distants, tels qu'un serveur LDAP. Les certificats peuvent être émis par une autorité de certification (CA) ou être auto-signés.
3. Sélectionnez un certificat dans la page, puis cliquez sur les points de suspension à la fin de la ligne.
4. Cliquez sur **Exporter**, puis enregistrez le fichier de certificat.
5. Ouvrez le fichier dans l'application de visualisation de certificats.

Supprimer les certificats de confiance

Vous pouvez supprimer un ou plusieurs certificats qui ne sont plus nécessaires, tels qu'un certificat expiré.

Avant de commencer

Importez le nouveau certificat avant de supprimer l'ancien.

> Sachez que la suppression d'un certificat racine ou intermédiaire peut avoir un impact sur plusieurs matrices de stockage, car ces matrices peuvent partager les mêmes fichiers de certificat.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.
3. Sélectionnez un ou plusieurs certificats dans le tableau, puis cliquez sur **Supprimer**.

   > La fonction **Delete** n'est pas disponible pour les certificats préinstallés.

   La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.

4. Confirmez la suppression, puis cliquez sur **Supprimer**.

   Le certificat est supprimé de la table.

Résoudre les certificats non fiables

Des certificats non fiables se produisent lorsqu'une baie de stockage tente d'établir une connexion sécurisée à SANtricity Unified Manager, mais la connexion ne parvient pas à confirmer la sécurité. À partir de la page certificat, vous pouvez résoudre les certificats non approuvés en important un certificat auto-signé de la matrice de stockage ou en important un certificat d'autorité de certification (CA) émis par un tiers de confiance.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.
- Si vous prévoyez d'importer un certificat signé par une autorité de certification :
  - Vous avez généré une demande de signature de certificat (.CSR file) pour chaque contrôleur de la matrice de stockage et l'avez envoyée à l'autorité de certification.
  - L'autorité de certification a renvoyé des fichiers de certificat approuvés.
  - Les fichiers de certificat sont disponibles sur votre système local.

Description de la tâche

Vous devrez peut-être installer d'autres certificats de confiance si l'un des éléments suivants est vrai :

- Vous avez ajouté récemment une baie de stockage.
- Un ou les deux certificats ont expiré.
- Un ou les deux certificats sont révoqués.
- Un ou les deux certificats ne sont pas titulaires d'un certificat racine ou intermédiaire.

Étapes

1. Sélectionnez **gestion des certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Cette page affiche tous les certificats signalés pour les matrices de stockage.

3. Sélectionnez **Importer › certificats**. Pour importer un certificat d'autorité de certification ou **Import › certificats de matrice de stockage auto-signés** pour importer un certificat auto-signé.

   Pour limiter la vue, vous pouvez utiliser le champ de filtrage **Afficher les certificats qui sont…** ou vous pouvez trier les lignes de certificat en cliquant sur l'un des en-têtes de colonne.

4. Dans la boîte de dialogue, sélectionnez le certificat, puis cliquez sur **Importer**.

   Le certificat est téléchargé et validé.