Certificats

SANtricity 11.6

NetApp
February 12, 2024

Sommaire

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.

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. System Manager vous permet de gérer les certificats entre le navigateur d'un système de gestion hôte (en tant que client) et les contrôleurs d'un système de stockage (en tant que serveurs).

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.

Certificats signés

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 :

- Racine — en haut de la hiérarchie se trouve 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 — en bas de la chaîne se trouve le certificat de serveur, qui identifie votre entité spécifique, telle qu'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. Toutefois, un certificat auto-signé n'utilise pas la même chaîne de fiducie qu'un certificat signé par l'AC.

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 utilisés pour le serveur de gestion des clés

Si vous utilisez un serveur de gestion des clés externe avec la fonction sécurité des lecteurs, vous pouvez également gérer les certificats d'authentification entre ce serveur et les 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 requête 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.
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.

Durée	Description
Certificat client	Pour la gestion des clés de sécurité, un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut ainsi faire confiance à leurs adresses IP.
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.
Certificat de serveur de gestion des clés	Pour la gestion des clés de sécurité, un certificat de serveur de gestion des clés valide le serveur, afin que la baie de stockage puisse faire confiance à son adresse IP.
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.
Serveur OCSP	Le serveur OCSP (Online Certificate Status Protocol) détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis empêche l'utilisateur d'accéder à un serveur si le certificat est révoqué.
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.

Comment

Utiliser des certificats signés CA pour les contrôleurs

Vous pouvez obtenir des certificats signés par une autorité de certification pour sécuriser les communications entre les contrôleurs et le navigateur utilisé pour accéder à System 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 par l'autorité de certification est une procédure en trois étapes.

Étape 1 : compléter et soumettre une RSC pour les contrôleurs

Vous devez d'abord générer un fichier de requête de signature de certificat (CSR) pour chaque contrôleur de la matrice de stockage, puis soumettre le(s) fichier(s) à une autorité de certification (CA).

Avant de commencer

- Vous devez connaître l'adresse IP ou le nom DNS de chaque contrôleur.

Description de la tâche

La RSC fournit des informations sur votre organisation, l'adresse IP ou le nom DNS du contrôleur et une paire de clés qui identifie le serveur Web dans le contrôleur. Au cours de cette tâche, un fichier CSR est généré s'il n'y a qu'un seul contrôleur dans la matrice de stockage et deux fichiers CSR s'il y a deux contrôleurs.

> 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 **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Complete CSR**.

   > Si une boîte de dialogue vous invite à accepter un certificat auto-signé pour le second contrôleur, cliquez sur **accepter le certificat auto-signé** pour continuer.

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 se trouve votre baie de stockage ou votre entreprise.
- **État/région (facultatif)** — l'état ou la région où se trouve votre baie de stockage 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.

> Certains champs peuvent être pré-remplis avec les informations appropriées, telles que l'adresse IP du contrôleur. Ne modifiez pas les valeurs préremplies sauf si vous êtes certain qu'elles sont incorrectes. Par exemple, si vous n'avez pas encore effectué de RSC, l'adresse IP du contrôleur est définie sur « localhost ». Dans ce cas, vous devez remplacer ""localhost" par le nom DNS ou l'adresse IP du contrôleur.

4. Vérifiez ou entrez les informations suivantes sur le contrôleur A de votre matrice de stockage :
   - **Contrôleur Un nom commun** — l'adresse IP ou le nom DNS du contrôleur A est affiché par défaut. Vérifiez que cette adresse est correcte. Elle doit correspondre exactement à ce que vous entrez pour accéder à System Manager dans le navigateur.
   - **Contrôleur Une autre adresse IP** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou des alias supplémentaires pour le contrôleur A. Pour plusieurs entrées, utilisez un format délimité par des virgules.
   - **Contrôleur Autre nom DNS** — si le nom commun est un nom DNS, entrez tout nom DNS supplémentaire pour le contrôleur A. 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. Si la matrice de stockage ne comporte qu'un seul contrôleur, le bouton **Finish** est disponible. Si la matrice de stockage comporte deux contrôleurs, le bouton **Suivant** est disponible.

> Ne cliquez pas sur le lien **Ignorer cette étape** lorsque vous créez une demande CSR. Ce lien est fourni dans les situations de récupération d'erreurs. Dans de rares cas, une requête CSR peut échouer sur un contrôleur, mais pas sur l'autre. Ce lien vous permet d'ignorer l'étape de création d'une requête CSR sur le contrôleur A s'il est déjà défini et de passer à l'étape suivante pour recréer une requête CSR sur le contrôleur B.

5. S'il n'y a qu'un seul contrôleur, cliquez sur **Finish**. S'il y a deux contrôleurs, cliquez sur **Suivant** pour entrer les informations relatives au contrôleur B (comme ci-dessus), puis cliquez sur **Terminer**.

   Pour un seul contrôleur, un fichier CSR est téléchargé sur votre système local. Pour les doubles contrôleurs, deux fichiers CSR sont téléchargés. L'emplacement du dossier de téléchargement dépend de votre navigateur.

6. Localisez le(s) fichier(s) CSR téléchargé(s). L'emplacement du dossier dépend de votre navigateur.
7. Soumettez le(s) fichier(s) CSR à une autorité de certification et demandez des certificats signés au format PEM.
8. Attendez que l'AC retourne les certificats, puis allez à Étape 2 : importation de certificats signés pour les contrôleurs.

Étape 2 : importation de certificats signés pour les contrôleurs

Une fois que vous avez reçu des certificats signés, vous importez les fichiers des contrôleurs.

Avant de commencer

- L'autorité de certification a renvoyé des fichiers de certificat signés.

- Les fichiers sont disponibles sur votre système local.
- Si l'autorité de certification a fourni un certificat chaîné (par exemple, un fichier .p7b), vous devez déballer le fichier chaîné dans des fichiers individuels : le certificat racine, un ou plusieurs certificats intermédiaires et les certificats de serveur qui identifient les contrôleurs. 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.

Description de la tâche

Cette tâche décrit comment télécharger les fichiers de certificat.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Importer**.

   Une boîte de dialogue s'ouvre pour importer le(s) fichier(s) de certificat.

3. Cliquez sur les boutons **Browse** pour sélectionner d'abord les fichiers racine et intermédiaire, puis sélectionnez chaque certificat de serveur pour les contrôleurs. Les fichiers racine et intermédiaire sont les mêmes pour les deux contrôleurs. Seuls les certificats de serveur sont uniques pour chaque contrôleur.

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

4. Cliquez sur **Importer**.

   Le(s) fichier(s) est chargé(s) et validé(s).

Résultats

La session est automatiquement interrompue. Vous devez vous reconnecter pour que le ou les certificats prennent effet. Lorsque vous vous connectez de nouveau, le nouveau certificat signé par l'autorité de certification est utilisé pour votre session.

Réinitialisez les certificats de gestion

Vous pouvez rétablir les certificats sur les contrôleurs de l'utilisation de certificats signés par l'autorité de certification aux certificats configurés en usine et 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.
- Les certificats signés CA doivent être importés au préalable.

Description de la tâche

La fonction Réinitialiser supprime les fichiers de certificat actuellement signés par l'autorité de certification de chaque contrôleur. Les contrôleurs retournent à l'utilisation de certificats auto-signés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Array Management**, sélectionnez **Réinitialiser**.

Une boîte de dialogue confirmer **Réinitialiser les certificats 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

Les contrôleurs retournent à l'utilisation de certificats auto-signés. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Afficher les informations de certificat importé

À partir de la page certificats, vous pouvez afficher le type de certificat, l'autorité d'émission et la plage de dates valide des certificats de la matrice de stockage.

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 **Paramètres › certificats**.
2. Sélectionnez l'un des onglets pour afficher des informations sur les certificats.

Onglet	Description
Gestion de la baie	Afficher des informations sur les certificats signés par l'autorité de certification importés pour chaque contrôleur, y compris le fichier racine, le(s) fichier(s) intermédiaire(s) et le(s) fichier(s) du serveur.
Fiabilité	Afficher des informations sur tous les autres types de certificats importés pour les contrôleurs. Utilisez le champ filtre sous **Afficher les certificats qui sont…** pour afficher les certificats installés par l'utilisateur ou pré-installés. • **Installé par l'utilisateur**. Certificats qu'un utilisateur a téléchargés sur la matrice de stockage, qui peuvent inclure des certificats de confiance lorsque le contrôleur agit comme un client (au lieu d'un serveur), des certificats LDAPS et des certificats de fédération d'identité. • **Préinstallé**. Certificats auto-signés inclus avec la matrice de stockage.
Gestion des clés	Afficher des informations sur les certificats signés par l'autorité de certification importés pour un serveur de gestion de clés externe.

Importer des certificats pour les contrôleurs lorsqu'ils agissent en tant que clients

Si le contrôleur rejette une connexion parce qu'il ne peut pas valider la chaîne de confiance d'un serveur réseau, vous pouvez importer un certificat depuis l'onglet

approuvé qui permet au contrôleur (agissant en tant que client) d'accepter les communications de ce serveur.

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.
- Les fichiers de certificat sont installés sur votre système local.

Description de la tâche

L'importation de certificats à partir de l'onglet approuvé peut être nécessaire si vous souhaitez autoriser un autre serveur à contacter les contrôleurs (par exemple, un serveur LDAP ou un serveur syslog utilisant TLS).

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Trusted**, sélectionnez **Import**.

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

3. Cliquez sur **Parcourir** pour sélectionner les fichiers de certificat des contrôleurs.

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

4. Cliquez sur **Importer**.

Résultats

Les fichiers sont chargés et validés.

Activez la vérification de révocation de certificats

Vous pouvez activer les vérifications automatiques des certificats révoqués, de sorte qu'un serveur OCSP (Online Certificate Status Protocol) bloque les utilisateurs à établir des connexions non sécurisées.

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.
- Un serveur DNS est configuré sur les deux contrôleurs, ce qui permet d'utiliser un nom de domaine complet pour le serveur OCSP. Cette tâche est disponible à partir de la page matériel.
- Si vous souhaitez spécifier votre propre serveur OCSP, vous devez connaître l'URL de ce serveur.

Description de la tâche

La vérification automatique de révocation est utile dans les cas où l'AC a émis un certificat de façon incorrecte ou si une clé privée est compromise.

Au cours de cette tâche, vous pouvez configurer un serveur OCSP ou utiliser le serveur spécifié dans le fichier de certificat. Le serveur OCSP détermine si l'autorité de certification a révoqué des certificats avant leur date d'expiration prévue, puis bloque l'accès de l'utilisateur à un site si le certificat est révoqué.

Étapes

1. Sélectionnez **Paramètres › certificats**.

2. Sélectionnez l'onglet **approuvé**.

> Vous pouvez également activer la vérification de révocation à partir de l'onglet **Key Management**.

3. Cliquez sur **tâches rares**, puis sélectionnez **Activer la vérification** dans le menu déroulant.
4. Sélectionnez **Je veux activer la vérification de révocation**, de sorte qu'une coche s'affiche dans la case et d'autres champs apparaissent dans la boîte de dialogue.
5. Dans le champ **OCSP responder address** (adresse de réponse * OCSP), vous pouvez éventuellement entrer une URL pour un serveur de réponse OCSP. Si vous n'entrez pas d'adresse, le système utilise l'URL du serveur OCSP à partir du fichier de certificat.
6. Cliquez sur **Tester adresse** pour vous assurer que le système peut ouvrir une connexion à l'URL spécifiée.
7. Cliquez sur **Enregistrer**.

Résultats

Si la matrice de stockage tente de se connecter à un serveur dont le certificat est révoqué, la connexion est refusée et un événement est consigné.

Supprimer les certificats de confiance

Vous pouvez supprimer les certificats installés par l'utilisateur précédemment importés de l'onglet approuvé.

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 mettez à jour un certificat approuvé avec une nouvelle version, le certificat mis à jour doit être importé avant de supprimer l'ancien certificat.

> Vous risquez de perdre l'accès à un système si vous supprimez un certificat utilisé pour authentifier les contrôleurs et un autre serveur, tel qu'un serveur LDAP, avant d'importer un certificat de remplacement.

Description de la tâche

Cette tâche décrit comment supprimer des certificats installés par l'utilisateur. Les certificats pré-installés et auto-signés ne peuvent pas être supprimés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **approuvé**.

   Le tableau indique les certificats de confiance de la matrice de stockage.

3. Dans le tableau, sélectionnez le certificat à supprimer.
4. Cliquez sur **tâches rares › Supprimer**

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

5. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

Utilisez des certificats signés par l'autorité de certification pour l'authentification avec un serveur de gestion des clés

Pour sécuriser les communications entre un serveur de gestion des clés et les contrôleurs de la matrice de stockage, vous devez configurer les ensembles appropriés de certificats.

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'authentification entre les contrôleurs et un serveur de gestion des clés est une procédure en deux étapes.

Étape 1 : compléter et soumettre une RSC pour authentification avec un serveur de gestion des clés

Vous devez d'abord générer un fichier de requête de signature de certificat (RSC), puis utiliser la RSC pour demander un certificat client signé à une autorité de certification (CA) approuvée par le serveur de gestion de clés. Vous pouvez également créer et télécharger un certificat client à partir du serveur de gestion des clés à l'aide du fichier CSR téléchargé.

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

Dans cette tâche, vous apprendrez à générer le fichier CSR que vous utiliserez ensuite pour demander un certificat client signé à partir d'une autorité de certification approuvée par le serveur de gestion des clés. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol). Au cours de cette tâche, vous devez fournir les informations relatives à votre entreprise.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Key Management**, sélectionnez **Complete CSR**.
3. Saisissez les informations suivantes :
   - **Nom commun** — Un nom qui identifie cette RSC, comme le nom de la matrice de stockage, qui sera affiché dans les fichiers de certificat.
   - **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 ou la localité où se trouve votre organisation.
   - **État/région (facultatif)** — l'état ou la région où se trouve votre organisation.
   - **Code ISO du pays** — le code ISO à deux chiffres (Organisation internationale de normalisation), tel que les États-Unis, où se trouve votre organisation.
4. Cliquez sur **Télécharger**.

Un fichier CSR est enregistré sur votre système local.

5. Demandez un certificat client signé à une autorité de certification approuvée par le serveur de gestion des clés.
6. Lorsque vous disposez d'un certificat client, accédez à Étape 2 : importation de certificats pour le serveur de gestion des clés.

Étape 2 : importation de certificats pour le serveur de gestion des clés

Lors de l'étape suivante, vous importez les certificats d'authentification entre la matrice de stockage et le serveur de gestion des clés. Il existe deux types de certificats : le certificat client valide les contrôleurs de la matrice de stockage, tandis que le certificat du serveur de gestion des clés valide le serveur.

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 signé un fichier de certificat client (voir Étape 1 : compléter et soumettre une RSC pour authentification avec un serveur de gestion des clés), et vous avez copié ce fichier sur l'hôte où vous accédez à System Manager. Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol).
- Vous devez récupérer le fichier de certificat du serveur à partir du serveur de gestion des clés, puis copier ce fichier vers l'hôte où vous accédez à System Manager. Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP.

> Pour plus d'informations sur le certificat du serveur, consultez la documentation de votre serveur de gestion des clés.

Description de la tâche

Cette tâche décrit comment télécharger des fichiers de certificat pour l'authentification entre les contrôleurs de la matrice de stockage et le serveur de gestion des clés. Vous devez charger à la fois le fichier de certificat client pour les contrôleurs et le fichier de certificat de serveur pour le serveur de gestion des clés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet **Key Management**, sélectionnez **Import**.

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

3. En regard de **Sélectionner le certificat client**, cliquez sur le bouton **Parcourir** pour sélectionner le fichier de certificat client pour les contrôleurs de la matrice de stockage.

   Le nom du fichier s'affiche dans la boîte de dialogue.

4. En regard de **Sélectionner le certificat de serveur de gestion de clés**, cliquez sur le bouton **Parcourir** pour sélectionner le fichier de certificat de serveur pour votre serveur de gestion de clés.

   Le nom du fichier s'affiche dans la boîte de dialogue.

5. Cliquez sur **Importer**.

Les fichiers sont chargés et validés.

Exporter les certificats du serveur de gestion des clés

Vous pouvez enregistrer un certificat pour un serveur de gestion des clés sur votre ordinateur local.

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.
- Les certificats doivent être importés au préalable.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'onglet **gestion des clés**.
3. Dans le tableau, sélectionnez le certificat à exporter, puis cliquez sur **Exporter**.

   Une boîte de dialogue Enregistrer s'ouvre.

4. Entrez un nom de fichier et cliquez sur **Enregistrer**.

FAQ

Pourquoi la boîte de dialogue Impossible d'accéder à un autre contrôleur s'affiche-t-elle ?

Lorsque vous effectuez certaines opérations liées aux certificats d'autorité de certification (par exemple, importation d'un certificat), une boîte de dialogue vous invitant à accepter un certificat auto-signé pour le second contrôleur s'affiche.

Dans les matrices de stockage avec deux contrôleurs (configurations duplex), cette boîte de dialogue apparaît parfois si SANtricity System Manager ne peut pas communiquer avec le second contrôleur ou si votre navigateur n'accepte pas le certificat pendant une opération donnée.

Si cette boîte de dialogue s'ouvre, cliquez sur **accepter le certificat auto-signé** pour continuer. Si une autre boîte de dialogue vous invite à saisir un mot de passe, entrez votre mot de passe administrateur utilisé pour accéder à System Manager.

Si cette boîte de dialogue s'affiche de nouveau et que vous ne pouvez pas terminer une tâche de certificat, essayez l'une des procédures suivantes :

- Utilisez un autre type de navigateur pour accéder à ce contrôleur, accepter le certificat et continuer.
- Accédez au second contrôleur avecSystem Manager, acceptez le certificat auto-signé, puis revenez au premier contrôleur et continuez.

Comment puis-je savoir quels certificats doivent être téléchargés sur System Manager pour la gestion externe des clés ?

Pour la gestion externe des clés, vous importez deux types de certificats pour

l'authentification entre la matrice de stockage et le serveur de gestion des clés afin que les deux entités puissent se faire confiance.

Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs demandes KMIP (Key Management Interoperability Protocol). Pour obtenir un certificat client, utilisez System Manager pour effectuer une RSC pour la matrice de stockage. Vous pouvez ensuite télécharger la RSC sur un serveur de gestion des clés et générer un certificat client à partir de ce serveur. Une fois que vous avez un certificat client, copiez ce fichier vers l'hôte sur lequel vous accédez à System Manager.

Un certificat de serveur de gestion des clés valide le serveur de gestion des clés. La baie de stockage peut donc avoir confiance en son adresse IP. Récupérez le fichier de certificat du serveur à partir du serveur de gestion des clés, puis copiez-le vers l'hôte sur lequel vous accédez à System Manager.

Que dois-je savoir au sujet de la vérification de révocation de certificats ?

System Manager vous permet de rechercher des certificats révoqués à l'aide d'un serveur OCSP (Online Certificate Status Protocol) au lieu de télécharger des listes de révocation de certificats.

Les certificats révoqués ne doivent plus être approuvés. Un certificat peut être révoqué pour plusieurs raisons : par exemple, si l'autorité de certification (AC) a émis incorrectement le certificat, si une clé privée a été compromise ou si l'entité identifiée n'a pas respecté les exigences de la politique.

Après avoir établi une connexion à un serveur OCSP dans System Manager, la matrice de stockage effectue une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog. La baie de stockage tente de valider les certificats de ces serveurs pour s'assurer qu'ils n'ont pas été révoqués. Le serveur renvoie alors la valeur "bon", "révoqué" ou "inconnu" pour ce certificat. Si le certificat est révoqué ou si la matrice ne peut pas contacter le serveur OCSP, la connexion est refusée.

> La spécification d'une adresse de réponse OCSP dans System Manager ou dans l'interface de ligne de commande (CLI) remplace l'adresse OCSP trouvée dans le fichier de certificat.

Pour quels types de serveurs la vérification de révocation sera-t-elle activée ?

La baie de stockage effectue une vérification de révocation chaque fois qu'elle se connecte à un serveur AutoSupport, à un serveur EKMS (External Key Management Server), à un serveur LDAPS (Lightweight Directory Access Protocol over SSL) ou à un serveur Syslog.