Utilisez des certificats

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

Utilisez des certificats

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.
- Vous devez connaître l'adresse IP ou les noms DNS de chaque contrôleur.

Description de la tâche

L'utilisation de certificats signés par l'autorité de certification est une procédure en trois étapes.

Étape 1 : compléter les 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.

Description de la tâche

Cette tâche décrit comment générer un fichier CSR à partir de System Manager. La RSC fournit des informations sur votre organisation, ainsi que l'adresse IP ou le nom DNS du contrôleur. Au cours de cette tâche, un fichier CSR est généré si la matrice de stockage dispose d'un contrôleur et de deux fichiers CSR s'il possède deux contrôleurs.

> Vous pouvez également générer un fichier CSR à l'aide d'un outil tel que OpenSSL et passer à Étape 2 : soumettez les fichiers CSR.

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. Le nom DNS ne peut pas commencer par un caractère générique.
   - **Contrôleur Une adresse IP alternative** — si le nom commun est une adresse IP, vous pouvez éventuellement entrer des adresses IP ou alias supplémentaires pour le contrôleur A. pour plusieurs entrées, utilisez un format délimité par des virgules.
   - **Contrôleur A autres noms DNS** — si le nom commun est un nom DNS, entrez des noms DNS supplémentaires pour le contrôleur A. pour les entrées multiples, 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. Le nom DNS ne peut pas commencer par un caractère générique. 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. Allez à Étape 2 : soumettez les fichiers CSR.

Étape 2 : soumettez les fichiers CSR

Après avoir créé les fichiers de demande de signature de certificat (CSR), envoyez les fichiers à une autorité de certification (AC). Les systèmes E-Series nécessitent le format PEM (Base64 ASCII codage) pour les certificats signés, qui inclut les types de fichiers suivants : pem, .crt, .cer ou .key.

Étapes

1. Localisez les fichiers CSR téléchargés.
2. Envoyez les fichiers CSR à une autorité de certification (par exemple VeriSign ou DigiCert) et demandez des certificats signés au format PEM.

Après avoir soumis un fichier CSR à l'autorité de certification, NE régénérez PAS un autre fichier CSR. Chaque fois que 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 du système. Lorsque vous recevez les certificats signés et que vous les importez, le système garantit que les clés privées et publiques sont la paire d'origine. Si les clés ne correspondent pas, les certificats signés ne fonctionneront pas et vous devez demander de nouveaux certificats à l'autorité de certification.

3. Lorsque l'autorité de certification renvoie les certificats signés, passez à Étape 3 : importation de certificats signés pour les contrôleursl' .

Étape 3 : importation de certificats signés pour les contrôleurs

Une fois que vous avez reçu des certificats signés de l'autorité de certification (CA), importez les fichiers des contrôleurs.

Avant de commencer

- L'autorité de certification a renvoyé des fichiers de certificat signés. Ces fichiers incluent le certificat racine, un ou plusieurs certificats intermédiaires et les certificats de serveur.
- Si l'autorité de certification a fourni un fichier de 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 l'utilitaire Windows `certmgr` pour décompresser les fichiers (cliquez avec le bouton droit de la souris et sélectionnez **toutes les tâches › Exporter**). Le codage base-64 est recommandé. Une fois les exportations terminées, un fichier CER est affiché pour chaque fichier de certificat de la chaîne.
- Vous avez copié les fichiers de certificat sur le système hôte sur lequel vous accédez à System Manager.

Étapes

1. Menu sélection:Paramètres[certificats]
2. Dans l'onglet gestion des baies, 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 de certificat 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. Si vous avez généré la RSC à partir d'un outil externe, vous devez également importer le fichier de clé privée créé avec la RSC.

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

4. Cliquez sur **Importer**.

   Les fichiers sont chargés et validés.

Résultat

La session est automatiquement interrompue. Vous devez vous reconnecter pour que les certificats prennent effet. Lorsque vous vous connectez de nouveau, les nouveaux certificats signés par l'autorité de certification sont utilisés 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 gestion des baies, sélectionnez **Réinitialiser**.

   La boîte de dialogue confirmer la réinitialisation des certificats de gestion s'ouvre.

3. Saisissez `reset` 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 chargés 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. • **Certificats pré-installés** — 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 approuvé, sélectionnez **Importer**.

   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 Menu:tâches rares[Supprimer].

   La boîte de dialogue confirmer la suppression du certificat de confiance s'ouvre.
5. Saisissez `delete` 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. 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).

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 avez un certificat client, rendez-vous sur 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. 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.

Avant de commencer

- Vous disposez d'un fichier de certificat client signé (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 sur lequel 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 un fichier de certificat à partir du serveur de gestion des clés, puis le copier 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. Vous pouvez utiliser un certificat racine, intermédiaire ou serveur pour le serveur de gestion des clés.

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

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Dans l'onglet gestion des clés, sélectionnez **Importer**.

   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. Vous pouvez choisir un certificat racine, intermédiaire ou serveur pour le serveur de gestion des 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**.

Informations sur le copyright

Informations sur les marques commerciales