Certificats

SANtricity 11.5

NetApp
February 12, 2024

Sommaire

Certificats

Concepts

Fonctionnement des certificats CA

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.

Lorsque vous ouvrez un navigateur et que vous essayez de vous connecter à System Manager via le port de gestion du contrôleur, le navigateur tente de vérifier que le contrôleur de la matrice de stockage est une source fiable. Si le navigateur ne parvient pas à localiser un certificat numérique pour le contrôleur, il vous avertit que le certificat n'est pas signé par une autorité reconnue et vous demande si vous souhaitez continuer. Si vous ne souhaitez plus voir cette alerte, vous devez obtenir un certificat numérique signé d'une autorité de certification.

Si vous utilisez un serveur de gestion externe des clés avec la fonction sécurité des lecteurs, vous pouvez également créer des certificats d'authentification entre ce serveur et les contrôleurs ou accepter les certificats auto-signés à partir de la matrice de stockage.

Les étapes suivantes sont requises pour l'utilisation d'un certificat numérique d'une autorité de confiance :

1. Accédez au **Paramètres › certificats**. Votre connexion utilisateur doit inclure des autorisations d'administrateur de sécurité ; sinon, **certificats** ne s'affiche pas sur la page.
2. Créez une requête de signature de certificat (RSC) pour chaque contrôleur ou pour un serveur de gestion de clés.
3. Envoyez le(s) fichier(s) .CSR à une autorité de certification, puis attendez qu'ils vous envoient les certificats.
4. Importez le certificat de confiance (intermédiaire et racine) à partir de l'autorité de certification. Ces certificats établissent un point de confiance pour une hiérarchie de CA.
5. Importez les certificats de gestion signés pour chaque contrôleur ou le serveur de gestion des clés.

Terminologie du certificat

Découvrez comment les termes du certificat s'appliquent à votre baie de stockage.

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.

Durée	Description
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.
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 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.
Certificat de gestion	Un certificat de gestion est approuvé par une autorité de certification (CA) et permet un accès sécurisé à l'application Web. Également appelé « certificat signé ».
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 auto-signé	Un certificat auto-signé est préchargé sur le contrôleur. Si la connexion au site est auto-signée, un message d'avertissement s'affiche avant de pouvoir accéder à l'application Web.
Certificat approuvé	Un certificat approuvé d'une autorité de certification (CA) est un certificat connu en haut de la hiérarchie de certificats. Également appelé « certificat racine ».

Comment

Remplir une demande de signature de certificat CA (CSR) pour les contrôleurs

Pour recevoir un certificat d'autorité de certification (CA) pour les contrôleurs de la matrice de stockage, vous devez d'abord générer un fichier de demande de signature de

certificat (CSR) pour chaque contrôleur 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.

Description de la tâche

Cette tâche décrit comment générer les fichiers .CSR (demandes de signature de certificat) que vous envoyez à une autorité de certification pour recevoir des certificats de gestion signés pour les contrôleurs. Vous devez fournir des informations sur votre organisation, ainsi que l'adresse IP ou le nom DNS du ou des contrôleurs. 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.

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 contrôleurs doubles, deux fichiers .CSR sont téléchargés. L'emplacement du dossier de téléchargement dépend de votre navigateur.

6. Envoyez le(s) fichier(s) .CSR à votre autorité de certification.

Une fois que vous avez terminé

Lorsque vous recevez les certificats numériques, importez les fichiers de certificat que l'AC vous a envoyés.

Importer des certificats approuvés pour les contrôleurs

Après avoir reçu des certificats numériques d'une autorité de certification (CA), vous pouvez importer la chaîne de certificats (intermédiaire et racine) des contrôleurs.

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.

Description de la tâche

Cette tâche explique comment télécharger les certificats de confiance pour les contrôleurs de la matrice de stockage.

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.

Une fois que vous avez terminé

Importez le certificat de gestion.

Importer un certificat de gestion pour les contrôleurs

Après avoir importé la chaîne de certificats approuvée, vous importez un fichier de certificat de gestion (signé) pour chaque contrôleur 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.
- Les certificats approuvés ont été importés.
- L'autorité de certification a renvoyé un fichier de certificat de gestion pour chaque contrôleur.
- Les fichiers de certificat de gestion sont disponibles sur votre système local.

Description de la tâche

Cette tâche décrit comment télécharger les fichiers de certificat de gestion pour l'authentification du contrôleur.

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 **Parcourir** pour sélectionner le fichier du contrôleur A. S'il y a deux contrôleurs, cliquez sur le deuxième bouton **Parcourir** pour sélectionner le fichier du contrôleur B.

   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.

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 que vous avez précédemment importés.

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 explique comment afficher les informations relatives aux certificats installés par l'utilisateur ou

préinstallés.

Étapes

1. Sélectionnez **Paramètres › certificats**.
2. Sélectionnez l'un des onglets pour afficher des informations sur les certificats de gestion des contrôleurs, les certificats de confiance et les certificats d'un serveur de gestion des clés.

Onglet	Description
Gestion de la baie	Afficher des informations sur tous les certificats de serveur importés pour les contrôleurs.
Fiabilité	Afficher des informations sur tous les certificats (racine) de confiance 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 (y compris les certificats de confiance, les certificats LDAPS et les certificats de fédération d'identité). • **Préinstallé**. Certificats inclus avec la matrice de stockage.
Gestion des clés	Afficher des informations sur tous les certificats de gestion (signés) importés pour un serveur de gestion de clés externe.

Supprimer les certificats de confiance

Vous pouvez supprimer tous les certificats importés par l'utilisateur.

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 au système si vous supprimez un certificat utilisé pour authentifier les certificats de gestion de la matrice de stockage ou le serveur LDAP avant d'importer un certificat de remplacement.

Description de la tâche

Cette tâche décrit comment supprimer des certificats importés par l'utilisateur. Les certificats prédéfinis 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. Type `delete` Dans le champ, puis cliquez sur **Supprimer**.

Réinitialisez les certificats de gestion

Vous pouvez rétablir les certificats de gestion de la matrice de stockage à l'état 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.
- Les certificats doivent être importés au préalable.

Description de la tâche

La réinitialisation des certificats de gestion sur la matrice de stockage supprime les certificats de gestion actuels de chacun des contrôleurs. Une fois les certificats réinitialisés, 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 la réinitialisation des certificats de gestion** s'ouvre.

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

Résultats

Une fois votre navigateur actualisé, les contrôleurs reviennent à utiliser des certificats auto-signés. Par conséquent, le système invite les utilisateurs à accepter manuellement le certificat auto-signé pour leurs sessions.

Remplir la demande de signature de certificat de l'autorité de certification (CSR) pour un serveur de clés

Pour recevoir un certificat d'autorité de certification (CA) pour un serveur de gestion des clés, vous devez d'abord générer un fichier de requête de signature de certificat (CSR).

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 les fichiers .CSR (demandes de signature de certificat) que vous envoyez à une autorité de certification pour recevoir des certificats signés pour un serveur de gestion de clés. 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. Envoyez le(s) fichier(s) .CSR à votre autorité de certification.

Une fois que vous avez terminé

Lorsque vous obtenez les certificats client et serveur du serveur de gestion des clés, importez-les pour authentification avec les contrôleurs de la matrice de stockage.

Importer les certificats du serveur de gestion des clés

Pour la gestion externe des clés, vous importez des certificats d'authentification entre la matrice de stockage et le serveur de gestion des clés de sorte que les deux entités puissent se faire confiance. Il existe deux types de certificats : le certificat client valide les contrôleurs, 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.
- Un certificat client est disponible pour la matrice de stockage.

> Un certificat client valide les contrôleurs de la baie de stockage. Le serveur de gestion des clés peut donc faire confiance à leurs adresses IP. Pour obtenir un certificat client, vous devez remplir une RSC pour la matrice de stockage, puis la télécharger sur le serveur de gestion des clés. À partir du serveur, générez un certificat client.

- Le certificat du serveur de gestion des clés est disponible.

> Un certificat de serveur de gestion des clés valide le serveur, afin que la baie de stockage puisse approuver son adresse IP. Pour obtenir un certificat de serveur de gestion des clés, vous devez le générer à partir du 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.

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. Cliquez sur les boutons **Parcourir** pour sélectionner les fichiers.

   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).

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**.

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. Le contrôle automatique de révocation est utile dans les cas où l'autorité de certification (AC) a émis un certificat de façon incorrecte ou si une clé privée est compromise.

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

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 gestion des clés.

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**.

Résultat

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.

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 avec System Manager, acceptez le certificat auto-signé, puis revenez au

premier contrôleur et continuez.

Comment puis-je savoir quels certificats doivent être téléchargés dans System Manager ?

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 adresses IP. Pour obtenir un certificat client, vous devez remplir une RSC pour la matrice de stockage, puis la télécharger sur le serveur de gestion des clés. Depuis le serveur, générez un certificat client, puis utilisez System Manager pour l'importer.

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 obtenir un certificat de serveur de gestion des clés, vous devez le générer à partir du serveur de gestion des clés.

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.

Informations sur le copyright

Informations sur les marques commerciales