Certificats et authentification

SANtricity 11.6

NetApp
February 12, 2024

Sommaire

Certificats et authentification

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.

Gestion des accès

Concepts

Fonctionnement de Access Management

Utilisez la gestion des accès pour établir l'authentification des utilisateurs dans SANtricity Unified Manager.

Flux de travail de configuration

La configuration de Access Management fonctionne comme suit :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

> Pour la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système. Le mot de passe doit être défini lors de la première connexion.

2. L'administrateur accède à Access Management dans l'interface utilisateur, qui inclut des rôles utilisateur locaux préconfigurés. Ces rôles permettent la mise en œuvre des fonctionnalités RBAC (contrôle d'accès basé sur des rôles).
3. L'administrateur configure une ou plusieurs des méthodes d'authentification suivantes :
   - **Rôles d'utilisateur local** — l'authentification est gérée via les fonctionnalités RBAC. Les rôles des utilisateurs locaux comprennent des utilisateurs prédéfinis et des rôles avec des autorisations d'accès spécifiques. Les administrateurs peuvent utiliser ces rôles d'utilisateur local comme méthode unique d'authentification, ou les utiliser en combinaison avec un service d'annuaire. Aucune configuration n'est nécessaire, autre que la définition de mots de passe pour les utilisateurs.
   - **Services d'annuaire** — l'authentification est gérée via un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, comme Active Directory de Microsoft. Un administrateur se connecte au serveur LDAP, puis mappe les utilisateurs LDAP aux rôles d'utilisateur local.
4. L'administrateur fournit aux utilisateurs des informations d'identification pour Unified Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants. Pendant la connexion, le système effectue les tâches d'arrière-plan suivantes :
   - Authentifie le nom d'utilisateur et le mot de passe par rapport au compte d'utilisateur.
   - Détermine les autorisations de l'utilisateur en fonction des rôles affectés.
   - Permet à l'utilisateur d'accéder aux fonctions de l'interface utilisateur.
   - Affiche le nom d'utilisateur dans la bannière supérieure.

Fonctions disponibles dans Unified Manager

L'accès aux fonctions dépend des rôles attribués à un utilisateur, qui comprennent les éléments suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Une fonction non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur.

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à SANtricity Unified Manager.

Durée	Description
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.
Reliure	Les opérations BIND sont utilisées pour authentifier les clients sur le serveur d'annuaire. La liaison nécessite généralement des informations d'identification de compte et de mot de passe, mais certains serveurs autorisent des opérations de liaison anonymes.
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.
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.
LDAP	Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer. Ce protocole permet à de nombreuses applications et services différents de se connecter au serveur LDAP pour valider les utilisateurs.
RBAC	Le contrôle d'accès basé sur les rôles (RBAC) est une méthode qui permet de réguler l'accès aux ressources informatiques ou réseau en fonction des rôles des utilisateurs individuels. Unified Manager inclut des rôles prédéfinis.
SSO	Single Sign-on (SSO) est un service d'authentification qui permet à un ensemble d'informations d'identification de connexion d'accéder à plusieurs applications.
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 disponible avec le proxy de services Web.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) comprennent des utilisateurs prédéfinis avec un ou plusieurs rôles qui leur sont associés. Chaque rôle inclut des autorisations d'accès aux tâches dans SANtricity Unified Manager.

Les rôles permettent à l'utilisateur d'accéder aux tâches comme suit :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

Si un utilisateur ne dispose pas des autorisations pour une certaine fonction, cette fonction est soit indisponible pour la sélection, soit ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Les administrateurs peuvent utiliser des fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans SANtricity Unified Manager. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles d'utilisateur local sont préconfigurés dans le système. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

1. Un administrateur se connecte à Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. Un administrateur examine les profils utilisateur, qui sont prédéfinis et ne peuvent pas être modifiés.
3. **Facultatif:** l'administrateur attribue de nouveaux mots de passe pour chaque profil utilisateur.
4. Les utilisateurs se connectent au système avec leurs identifiants attribués.

Gestion

Lors de l'utilisation de rôles d'utilisateur local uniquement pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Gestion des accès avec les services d'annuaire

Les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que Active Directory de Microsoft.

Flux de travail de configuration

Si un serveur LDAP et un service d'annuaire sont utilisés sur le réseau, la configuration fonctionne comme suit :

1. Un administrateur se connecte à SANtricity Unified Manager avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité.

   Le `admin` l'utilisateur dispose d'un accès complet à toutes les fonctions du système.

2. L'administrateur entre les paramètres de configuration du serveur LDAP. Les paramètres incluent le nom de domaine, l'URL et les informations de compte Bind.
3. Si le serveur LDAP utilise un protocole sécurisé (LDAPS), l'administrateur télécharge une chaîne de certificats d'autorité de certification (CA) pour l'authentification entre le serveur LDAP et le système hôte sur lequel le proxy des services Web est installé.
4. Une fois la connexion au serveur établie, l'administrateur mappe les groupes d'utilisateurs sur les rôles d'utilisateur local. Ces rôles sont prédéfinis et ne peuvent pas être modifiés.
5. L'administrateur teste la connexion entre le serveur LDAP et Web Services Proxy.
6. Les utilisateurs se connectent au système avec les informations d'identification des services LDAP/Directory qui leur sont attribuées.

Gestion

Lors de l'utilisation des services d'annuaire pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Ajouter un serveur de répertoire.
- Modifier les paramètres du serveur de répertoire.
- Mappez les utilisateurs LDAP aux rôles d'utilisateur local.
- Supprimer un serveur de répertoires.
- Modifier les mots de passe.
- Définissez une longueur minimale pour les mots de passe.
- Autoriser les utilisateurs à se connecter sans mot de passe.

Comment

Afficher les rôles d'utilisateur local

Dans l'onglet rôles d'utilisateur local, vous pouvez afficher les mappages des utilisateurs sur les rôles par défaut. Ces mappages font partie du RBAC (contrôle d'accès basé sur des rôles) appliqué dans le proxy de services Web pour SANtricity Unified Manager.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Les utilisateurs et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.

Les utilisateurs sont présentés dans le tableau :

- **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles.
- **Stockage** — l'administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle.
- **Sécurité** — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur.
- **Support** — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor.
- **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor.
- **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur.
- **Ro** (lecture seule) — cet utilisateur n'inclut que le rôle moniteur.

Modifier les mots de passe

Vous pouvez modifier les mots de passe utilisateur de chaque utilisateur dans Access Management.

Avant de commencer

- Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.
- Vous devez connaître le mot de passe administrateur local.

Description de la tâche

Suivez les consignes suivantes lorsque vous choisissez un mot de passe :

- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel pour un mot de passe minimum (dans Afficher/Modifier les paramètres).
- Les mots de passe sont sensibles à la casse.
- Les espaces en fin de page ne sont pas supprimés des mots de passe lorsqu'ils sont définis. Veillez à inclure des espaces s'ils étaient inclus dans le mot de passe.
- Pour renforcer la sécurité, utilisez au moins 15 caractères alphanumériques et modifiez fréquemment le mot de passe.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez un utilisateur dans le tableau.

   Le bouton **Modifier le mot de passe** devient disponible.

4. Sélectionnez **Modifier le mot de passe**.

   La boîte de dialogue **Modifier le mot de passe** s'ouvre.

5. Si aucun mot de passe minimum n'est défini pour les mots de passe d'utilisateur local, vous pouvez cocher la case pour demander à l'utilisateur d'entrer un mot de passe pour accéder au système.
6. Saisissez le nouveau mot de passe pour l'utilisateur sélectionné dans les deux champs.
7. Entrez votre mot de passe administrateur local pour confirmer cette opération, puis cliquez sur **Modifier**.

Résultats

Si l'utilisateur est actuellement connecté, le changement de mot de passe entraîne la fin de la session active de l'utilisateur.

Modifier les paramètres de mot de passe de l'utilisateur local

Vous pouvez définir la longueur minimale requise pour tous les mots de passe utilisateur locaux nouveaux ou mis à jour. Vous pouvez également autoriser les utilisateurs locaux à accéder au système sans saisir de mot de passe.

Avant de commencer

- Vous devez être connecté en tant qu'administrateur local, qui inclut les autorisations d'administrateur racine.

Description de la tâche

Tenez compte des consignes suivantes lorsque vous définissez la longueur minimale des mots de passe utilisateur locaux :

- Les modifications apportées aux paramètres n'affectent pas les mots de passe des utilisateurs locaux existants.
- Le paramètre de longueur minimum requis pour les mots de passe utilisateur local doit comporter entre 0 et 30 caractères.
- Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre de longueur minimale actuel.
- Ne définissez pas de longueur minimale pour le mot de passe si vous souhaitez que les utilisateurs locaux accèdent au système sans saisir de mot de passe.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres de mot de passe utilisateur local** s'ouvre.

4. Effectuez l'une des opérations suivantes :
   - Pour permettre aux utilisateurs locaux d'accéder au système *sans* saisir un mot de passe, décochez la case "exiger au moins tous les mots de passe des utilisateurs locaux".
   - Pour définir une longueur minimale de mot de passe pour tous les mots de passe d'utilisateur local, cochez la case « exiger au moins tous les mots de passe d'utilisateur local », puis utilisez la zone de saisie pour définir la longueur minimale requise pour tous les mots de passe d'utilisateur local.

     Tout nouveau mot de passe utilisateur local doit respecter ou dépasser le paramètre actuel.

5. Cliquez sur **Enregistrer**.

Ajouter un serveur de répertoire

Pour configurer l'authentification pour Access Management, vous établissez des communications entre un serveur LDAP et l'hôte exécutant le proxy de services Web pour SANtricity Unified Manager. Vous associez ensuite les groupes d'utilisateurs LDAP aux rôles d'utilisateur local.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

Description de la tâche

L'ajout d'un serveur de répertoires est un processus en deux étapes. Vous devez d'abord entrer le nom de domaine et l'URL. Si votre serveur utilise un protocole sécurisé, vous devez également télécharger un certificat d'autorité de certification pour l'authentification s'il est signé par une autorité de signature non standard. Si vous disposez d'informations d'identification pour un compte BIND, vous pouvez également saisir votre nom de compte d'utilisateur et votre mot de passe. Ensuite, vous associez les groupes d'utilisateurs du serveur LDAP aux rôles d'utilisateur locaux.

Étapes

1. Sélectionnez **Access Management**.
2. Dans l'onglet **Directory Services**, sélectionnez **Add Directory Server**.

   La boîte de dialogue **Ajouter un serveur de répertoire** s'ouvre.

3. Dans l'onglet **Paramètres du serveur**, entrez les informations d'identification du serveur LDAP.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
Entrez le nom de domaine du serveur LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Saisissez l'URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Télécharger le certificat (facultatif)

Réglage	Description
Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus. Cliquez sur **Parcourir** et sélectionnez un certificat d'autorité de certification à télécharger. Il s'agit du certificat ou de la chaîne de certificats sécurisés utilisés pour l'authentification du serveur LDAP.	Lier un compte (facultatif)
Entrez un compte utilisateur en lecture seule pour les requêtes de recherche sur le serveur LDAP et pour la recherche dans les groupes. Entrez le nom du compte au format LDAP. Par exemple, si l'utilisateur bind est appelé "bindacct", vous pouvez entrer une valeur telle que `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Liaison du mot de passe (facultatif)

Réglage	Description
Ce champ s'affiche lorsque vous entrez un compte de liaison. Saisissez le mot de passe du compte de liaison.	Testez la connexion au serveur avant d'ajouter
Cochez cette case pour vous assurer que le système peut communiquer avec la configuration du serveur LDAP que vous avez saisie. Le test se produit après avoir cliqué sur **Ajouter** en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas ajoutée. Vous devez résoudre l'erreur ou désélectionner la case à cocher pour ignorer le test et ajouter la configuration.	**Paramètres des privilèges**
Rechercher un NA de base	Entrez le contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=copc, DC=local`.
Attribut de nom d'utilisateur	Saisissez l'attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Entrez une liste d'attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

4. Cliquez sur l'onglet **Role Mapping**.
5. Attribuez des groupes LDAP aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Spécifiez le nom unique (DN) du groupe pour lequel le groupe d'utilisateurs LDAP doit être mappé.	Rôles

Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

6. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
7. Lorsque vous avez terminé les mappages, cliquez sur **Ajouter**.

   Le système effectue une validation, en vous assurant que la matrice de stockage et le serveur LDAP peuvent communiquer. Si un message d'erreur s'affiche, vérifiez les informations d'identification saisies dans la boîte de dialogue et entrez-les à nouveau si nécessaire.

Modifier les paramètres du serveur d'annuaire et les mappages de rôles

Si vous avez déjà configuré un serveur d'annuaire dans Access Management, vous pouvez modifier ses paramètres à tout moment. Les paramètres incluent les informations de connexion du serveur et les mappages de groupe à rôle.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un serveur d'annuaire doit être défini.

Étapes

1. Sélectionnez **Access Management**.
2. Sélectionnez l'onglet **Services Annuaire**.
3. Si plusieurs serveurs sont définis, sélectionnez le serveur que vous souhaitez modifier dans la table.
4. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres du serveur d'annuaire** s'ouvre.

5. Dans l'onglet **Paramètres du serveur**, modifiez les paramètres souhaités.

Réglage	Description
Paramètres de configuration	Domaine(s)

Réglage	Description
Nom(s) de domaine du ou des serveurs LDAP. Pour plusieurs domaines, entrez les domaines dans une liste séparée par des virgules. Le nom de domaine est utilisé dans le login (*username@domain*) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
URL d'accès au serveur LDAP sous la forme de `ldap[s]://host:port`.	Lier un compte (facultatif)
Le compte utilisateur en lecture seule pour rechercher des requêtes sur le serveur LDAP et pour effectuer des recherches dans les groupes.	Liaison du mot de passe (facultatif)
Mot de passe du compte BIND. (Ce champ s'affiche lorsqu'un compte de liaison est saisi.)	Testez la connexion au serveur avant d'enregistrer
Vérifie que le système peut communiquer avec la configuration du serveur LDAP. Le test se produit après avoir cliqué sur **Enregistrer**. Si cette case est cochée et que le test échoue, la configuration n'est pas modifiée. Vous devez résoudre l'erreur ou décocher la case pour ignorer le test et modifier de nouveau la configuration.	**Paramètres des privilèges**

Réglage	Description
Rechercher un NA de base	Contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=copc, DC=local`.
Attribut de nom d'utilisateur	Attribut lié à l'ID utilisateur pour l'authentification. Par exemple : `sAMAccountName`.
Attribut(s) de groupe	Liste des attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : `memberOf, managedObjects`.

6. Dans l'onglet **Role Mapping**, modifiez le mappage souhaité.

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper.	Rôles

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

7. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
8. Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Supprimer le serveur de répertoire

Pour interrompre la connexion entre un serveur d'annuaire et Web Services Proxy, vous pouvez supprimer les informations sur le serveur de la page gestion des accès. Vous pouvez effectuer cette tâche si vous avez configuré un nouveau serveur, puis que vous souhaitez supprimer l'ancien serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Étapes

1. Sélectionnez **Access Management**.

2. Sélectionnez l'onglet **Services Annuaire**.
3. Dans la liste, sélectionnez le serveur de répertoire à supprimer.
4. Cliquez sur **Supprimer**.

   La boîte de dialogue **Remove Directory Server** s'ouvre.

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

   Les paramètres de configuration du serveur d'annuaire, les paramètres de privilèges et les mappages de rôles sont supprimés. Les utilisateurs ne peuvent plus se connecter avec les informations d'identification de ce serveur.

FAQ

Pourquoi ne puis-je pas me connecter ?

Si vous recevez une erreur lors de votre tentative de connexion à SANtricity Unified Manager, consultez les causes possibles.

Des erreurs de connexion à Unified Manager peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un nom d'utilisateur ou un mot de passe incorrect.
- Vous disposez de privilèges insuffisants.
- Le serveur d'annuaire (si configuré) est peut-être indisponible. Si c'est le cas, essayez de vous connecter avec un rôle d'utilisateur local.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.

Les erreurs de connexion à une baie de stockage distante pour les tâches de mise en miroir peuvent se produire pour l'une des raisons suivantes :

- Vous avez saisi un mot de passe incorrect.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.
- Le nombre maximal de connexions client utilisées sur le contrôleur a été atteint. Recherchez plusieurs utilisateurs ou clients.

Que dois-je savoir avant d'ajouter un serveur d'annuaire ?

Avant d'ajouter un serveur d'annuaire dans Access Management, vous devez répondre à certaines exigences.

- Les groupes d'utilisateurs doivent être définis dans votre service d'annuaire.
- Les informations d'identification du serveur LDAP doivent être disponibles, y compris le nom de domaine, l'URL du serveur, et éventuellement le nom d'utilisateur et le mot de passe du compte BIND.
- Pour les serveurs LDAPS utilisant un protocole sécurisé, la chaîne de certificats du serveur LDAP doit être installée sur votre ordinateur local.

De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ?

Avant de mapper des groupes à des rôles, consultez les directives.

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage sur les baies, mais pas à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management et Certificate Management.
- **Support admin** — accès à toutes les ressources matérielles sur les matrices de stockage, aux données de panne et aux événements MEL. Aucun accès aux objets de stockage ou à la configuration de sécurité.
- **Monitor** — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.

> Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur.

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol) et des services d'annuaire, assurez-vous que :

- Un administrateur a défini des groupes d'utilisateurs dans le service d'annuaire.
- Vous connaissez les noms de domaine de groupe des groupes d'utilisateurs LDAP.

Qu'est-ce que les utilisateurs locaux ?

Les utilisateurs locaux sont prédéfinis dans le système et incluent des autorisations spécifiques.

Les utilisateurs locaux incluent :

- **Admin** — Super administrateur qui a accès à toutes les fonctions du système. Cet utilisateur inclut tous les rôles. Le mot de passe doit être défini lors de la première connexion.
- **Stockage** — l'administrateur responsable de tout le provisionnement du stockage. Cet utilisateur comprend les rôles suivants : administrateur du stockage, administrateur du support et contrôle. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Sécurité** — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès et la gestion des certificats. Cet utilisateur inclut les rôles suivants : administrateur de sécurité et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Support** — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur inclut les rôles suivants : support Admin et Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Moniteur** — Un utilisateur avec accès en lecture seule au système. Cet utilisateur inclut uniquement le rôle Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **rw** (lecture/écriture) — cet utilisateur comprend les rôles suivants : administrateur de stockage, administrateur de support et moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
- **Ro** (lecture seule) — cet utilisateur n'inclut que le rôle moniteur. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.