Gestion des accès

SANtricity software

NetApp
March 27, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/e-series-santricity-117/um-certificates/overview-access-management-um.html on March 27, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion des accès . . . 1
- Présentation de Access Management . . . 1
  - Quelles sont les méthodes d'authentification disponibles ? . . . 1
  - Comment configurer Access Management ? . . . 1
- Concepts . . . 1
  - Fonctionnement de Access Management . . . 1
  - Terminologie de la gestion des accès . . . 2
  - Autorisations pour les rôles mappés . . . 3
  - Gestion des accès avec rôles d'utilisateur local . . . 4
  - Gestion des accès avec les services d'annuaire . . . 4
- Utiliser les rôles d'utilisateur local . . . 5
  - Afficher les rôles d'utilisateur local . . . 5
  - Modifiez les mots de passe des profils utilisateur locaux . . . 6
  - Modifier les paramètres de mot de passe de l'utilisateur local . . . 7
- Utiliser les services d'annuaire . . . 8
  - Ajouter un serveur de répertoire . . . 8
  - Modifier les paramètres du serveur d'annuaire et les mappages de rôles . . . 13
  - Supprimer le serveur de répertoire . . . 17
- FAQ . . . 17
  - Pourquoi ne puis-je pas me connecter ? . . . 17
  - Que dois-je savoir avant d'ajouter un serveur d'annuaire ? . . . 17
  - De quoi ai-je besoin savoir concernant le mappage aux rôles de la baie de stockage ? . . . 18
  - Qu'est-ce que les utilisateurs locaux ? . . . 18

Gestion des accès

Présentation de Access Management

Access Management est une méthode de configuration de l'authentification utilisateur dans SANtricity Unified Manager.

Quelles sont les méthodes d'authentification disponibles ?

Les méthodes d'authentification suivantes sont disponibles :

- **Rôles d'utilisateur local** — l'authentification est gérée via les fonctions RBAC (contrôle d'accès basé sur les rôles). Les rôles des utilisateurs locaux comprennent des profils utilisateur prédéfinis et des rôles avec des autorisations d'accès spécifiques.
- **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.

En savoir plus :

- "Fonctionnement de Access Management"
- "Terminologie de la gestion des accès"
- "Autorisations pour les rôles mappés"

Comment configurer Access Management ?

Le logiciel SANtricity est préconfiguré pour utiliser les rôles des utilisateurs locaux. Si vous souhaitez utiliser LDAP, vous pouvez le configurer sous la page gestion des accès.

En savoir plus :

- "Gestion des accès avec rôles d'utilisateur local"
- "Gestion des accès avec les services d'annuaire"

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. L'administrateur affecte éventuellement 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 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.

Utiliser les rôles d'utilisateur local

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.

Modifiez les mots de passe des profils utilisateur locaux

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 modification du 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 du mot de passe de l'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**.

Utiliser les services d’annuaire

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=cpoc, 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. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Cliquez dans le champ et sélectionnez l'un des rôles d'utilisateur local à mapper avec le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles mappés incluent les autorisations suivantes : • **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.

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.

Détails du champ

Réglage	Description
Paramètres de configuration	Domaine(s)
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

Réglage	Description
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**
Rechercher un NA de base	Contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de `CN=Users, DC=cpoc, 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.

Détails du champ

Réglage	Description
Mappages	DN du groupe
Nom de domaine du groupe d'utilisateurs LDAP à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappé avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : \.[]{}()<>*+-=!?^$	
Rôles	Rôles à mapper sur le DN du groupe. Vous devez sélectionner individuellement chaque rôle que vous souhaitez inclure pour ce groupe. Le rôle de contrôle est requis en association avec les autres rôles pour se connecter à SANtricity Unified Manager. Les rôles incluent 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.

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 Supprimer le serveur d'annuaire 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 la tentative de connexion, consultez ces causes possibles.

Des erreurs de connexion 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.
- Vous avez tenté de vous connecter plusieurs fois sans succès, ce qui a déclenché le mode de verrouillage. Attendez 10 minutes pour vous reconnecter.

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.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.