Gestion des accès

SANtricity 11.5

NetApp
February 12, 2024

Sommaire

Gestion des accès

Concepts

Fonctionnement de Access Management

Access Management est une méthode pour établir l'authentification des utilisateurs dans SANtricity System Manager. L'authentification exige que les utilisateurs se connectent à ces systèmes avec leurs informations d'identification attribuées.

La configuration de Access Management et l'authentification utilisateur fonctionnent comme suit :

1. Un administrateur se connecte à System 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.

2. L'administrateur accède à Access Management dans l'interface utilisateur. La baie de stockage est préconfigurée pour utiliser des rôles utilisateur locaux, une 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 appliquées dans la matrice de stockage. Les rôles des utilisateurs locaux comprennent des profils utilisateur 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 utilisateur locaux intégrés à la baie de stockage.
   - **SAML** — l'authentification est gérée par un fournisseur d'identité (IDP) à l'aide du langage SAML (Security assertion Markup Language) 2.0. Un administrateur établit la communication entre le système du fournisseur d'identités et la baie de stockage, puis il mappe les utilisateurs de ce fournisseur aux rôles des utilisateurs locaux intégrés dans la baie de stockage.
4. L'administrateur fournit aux utilisateurs des informations de connexion pour System Manager.
5. Les utilisateurs se connectent au système en saisissant leurs identifiants.

   > Si l'authentification est gérée au moyen de SAML et d'une authentification unique (Single Sign-on), le système peut contourner la boîte de dialogue de connexion de System Manager.

   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 tâches dans l'interface utilisateur.
- Affiche le nom d'utilisateur dans le coin supérieur droit de l'interface.

Tâches disponibles dans System Manager

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

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. 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 tâche non disponible est grisée ou ne s'affiche pas dans l'interface utilisateur. Par exemple, un utilisateur ayant le rôle Monitor peut afficher toutes les informations relatives aux volumes, mais ne peut pas accéder aux fonctions permettant de modifier ce volume. Les onglets des fonctions telles que **Copy Services** et **Add to Workload** sont grisés ; seuls les paramètres View/Edit sont disponibles.

Accès des utilisateurs à SANtricity Storage Manager

Lorsque les rôles d'utilisateur local et les services d'annuaire sont configurés, les utilisateurs doivent saisir des informations d'identification avant d'exécuter l'une des fonctions suivantes dans la fenêtre de gestion d'entreprise (EMW) :

- Modification du nom de la matrice de stockage
- Mise à niveau du micrologiciel du contrôleur
- Chargement d'une configuration de matrice de stockage
- Exécution d'un script
- Tentative d'exécution d'une opération active lorsqu'une session inutilisée a expiré

Si le langage SAML est configuré pour une baie de stockage, les utilisateurs ne peuvent pas utiliser l'EMW pour détecter ou gérer le stockage de cette baie.

Terminologie de la gestion des accès

Découvrez comment les termes de gestion des accès s'appliquent à votre matrice de stockage.

Durée	Description
Active Directory	Active Directory (AD) est un service d'annuaire Microsoft qui utilise LDAP pour les réseaux de domaine Windows.

Durée	Description
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.
IDP	Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI.
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. Des contrôles RBAC sont appliqués sur la baie de stockage et incluent des rôles prédéfinis.

Durée	Description
SAML	Le langage SAML (Security assertion Markup Language) est une norme XML pour l'authentification et l'autorisation entre deux entités. SAML permet l'authentification multifacteur, dans laquelle les utilisateurs doivent fournir au moins deux éléments pour prouver leur identité (par exemple, un mot de passe et une empreinte digitale). La fonctionnalité SAML intégrée de la baie de stockage est conforme à la norme SAML2.0 pour l'assertion d'identité, l'authentification et l'autorisation.
SP	Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités.
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.

Autorisations pour les rôles mappés

Les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées sur la baie de stockage incluent des profils utilisateur prédéfinis avec un ou plusieurs rôles qui leur sont mappés. Chaque rôle inclut des autorisations d'accès aux tâches dans SANtricity System Manager.

Les profils utilisateur et les rôles mappés sont accessibles à partir du **Paramètres › Access Management › local User Roles** dans l'interface utilisateur de System Manager.

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

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. 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 tâche donnée, cette tâche est grisée ou ne s'affiche pas dans l'interface utilisateur.

Gestion des accès avec rôles d'utilisateur local

Pour la gestion des accès, les administrateurs peuvent utiliser les fonctionnalités RBAC (contrôle d'accès basé sur des rôles) appliquées dans la baie de stockage. Ces fonctionnalités sont appelées « rôles utilisateur locaux ».

Flux de travail de configuration

Les rôles utilisateur locaux sont préconfigurés pour la matrice de stockage. Pour utiliser les rôles d'utilisateur local pour l'authentification, les administrateurs peuvent effectuer les opérations suivantes :

1. Un administrateur se connecte à SANtricity System 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

Pour la gestion des accès, les administrateurs peuvent utiliser un serveur LDAP (Lightweight Directory Access Protocol) et un service d'annuaire, tel que l'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 System 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 la matrice de

stockage.

4. Une fois la connexion au serveur établie, l'administrateur mappe les groupes d'utilisateurs sur les rôles de la matrice de stockage. Ces rôles sont prédéfinis et ne peuvent pas être modifiés.
5. L'administrateur teste la connexion entre le serveur LDAP et la matrice de stockage.
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.

Gestion des accès avec SAML

Pour Access Management, les administrateurs peuvent utiliser les fonctionnalités SAML 2.0 intégrées à la baie.

Flux de travail de configuration

La configuration SAML fonctionne comme suit :

1. Un administrateur se connecte à System 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 de System Manager.

2. L'administrateur accède à l'onglet **SAML** sous Access Management.
3. Un administrateur configure les communications avec le fournisseur d'identité (IDP). Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Pour configurer les communications avec la baie de stockage, l'administrateur télécharge le fichier de métadonnées IDP depuis le système IDP, puis utilise System Manager pour télécharger le fichier vers la baie de stockage.
4. Un administrateur établit une relation de confiance entre le fournisseur de services et le PDI. Un fournisseur de services contrôle les autorisations utilisateur. Dans ce cas, le contrôleur de la baie de stockage fait office de fournisseur de services. Pour configurer les communications, l'administrateur utilise System Manager pour exporter un fichier de métadonnées Service Provider pour chaque contrôleur. À partir du système IDP, l'administrateur importe ensuite ces fichiers de métadonnées vers le IDP.

   > Les administrateurs doivent également s'assurer que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.

5. L'administrateur mappe les rôles de la baie de stockage avec les attributs utilisateur définis dans le IDP. Pour ce faire, l'administrateur utilise System Manager pour créer les mappages.

6. L'administrateur teste la connexion SSO à l'URL IDP. Ce test garantit que la matrice de stockage et le IDP peuvent communiquer.

> Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

7. Depuis System Manager, l'administrateur active le langage SAML pour la baie de stockage.
8. Les utilisateurs se connectent au système à l'aide de leurs identifiants SSO.

Gestion

Lorsque vous utilisez SAML pour l'authentification, les administrateurs peuvent effectuer les tâches de gestion suivantes :

- Modifiez ou créez de nouveaux mappages de rôles
- Exporter les fichiers du fournisseur de services

Restrictions d'accès

Lorsque le langage SAML est activé, les clients suivants ne peuvent pas accéder aux services et ressources de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Comment

Afficher les rôles d'utilisateur local

Dans l'onglet rôles utilisateur local, vous pouvez afficher les mappages des profils utilisateur avec les rôles par défaut. Ces mappages font partie du RBAC (contrôle d'accès basé sur des rôles) appliqué dans la baie de stockage.

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 profils utilisateur et les mappages ne peuvent pas être modifiés. Seuls les mots de passe peuvent être modifiés.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.

2. Sélectionnez l'onglet **rôles d'utilisateur local**.

   Les profils utilisateur sont affichés dans le tableau :

   - **Root admin** (admin) — Super administrateur qui a accès à toutes les fonctions du système. Ce profil utilisateur inclut tous les rôles.
   - **Storage admin** (stockage) — l'administrateur responsable de l'ensemble du provisionnement du stockage. Ce profil utilisateur inclut les rôles suivants : administrateur du stockage, administrateur du support et moniteur.
   - **Security admin** (sécurité) — l'utilisateur responsable de la configuration de la sécurité, y compris la gestion des accès, la gestion des certificats et les fonctions de lecteur sécurisées. Ce profil utilisateur inclut les rôles suivants : Security Admin et Monitor.
   - **Support admin** (support) — l'utilisateur responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Ce profil utilisateur inclut les rôles suivants : support Admin et Monitor.
   - **Moniteur** (moniteur) — Un utilisateur avec accès en lecture seule au système. Ce profil utilisateur inclut uniquement le rôle Monitor.

Modifier les mots de passe

Vous pouvez modifier les mots de passe utilisateur de chaque profil 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 de fin ne sont pas dépouillés 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.

> La modification du mot de passe dans System Manager modifie également celui-ci dans l'interface de ligne de commande. En outre, les modifications de mot de passe entraînent la fin de la session active de l'utilisateur.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
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 sélectionné d'entrer un mot de passe pour accéder à la matrice de stockage, puis vous pouvez saisir le nouveau mot de passe pour l'utilisateur sélectionné.
6. Entrez votre mot de passe administrateur local, puis cliquez sur **Modifier**.

Résultat

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 sur la matrice de stockage. Vous pouvez également autoriser les utilisateurs locaux à accéder à la matrice de stockage 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 à la matrice de stockage sans saisir de mot de passe.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **rôles d'utilisateur local**.
3. Sélectionnez le bouton **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 à la matrice de stockage *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 case à cocher 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 pouvez établir des communications entre la matrice de stockage et un serveur LDAP, puis mapper les groupes d'utilisateurs LDAP aux rôles prédéfinis de la baie.

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 prédéfinis de la matrice de stockage.

> Lors de la procédure d'ajout d'un serveur LDAP, l'interface de gestion héritée est désactivée. L'interface de gestion héritée (symbole) est une méthode de communication entre la baie de stockage et le client de gestion. Lorsque cette option est désactivée, la baie de stockage et le client de gestion utilisent une méthode de communication plus sécurisée (API REST via https).

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
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)
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 alors entrer une valeur telle que « CN=bindacct,CN=Users,DC=cpoc,DC=local ».	Liaison du mot de passe (facultatif)
Ce champ s'affiche lorsque vous saisissez un compte de liaison ci-dessus. Saisissez le mot de passe du compte de liaison.	Testez la connexion au serveur avant d'ajouter

Réglage	Description
Cochez cette case pour vous assurer que la matrice de stockage 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. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

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 **Paramètres › gestion des accès**.
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)
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 la matrice de stockage peut communiquer avec la configuration du serveur LDAP. Le test se produit après avoir cliqué sur Enregistrer en bas de la boîte de dialogue. Si cette case est cochée et que le test échoue, la configuration n'est pas modifiée. Vous devez résoudre l'erreur ou désélectionner la case à cocher 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=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. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

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

Résultat

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 la matrice de stockage, 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 **Paramètres › gestion des accès**.
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.

Configurez SAML

Pour configurer l'authentification pour Access Management, vous pouvez utiliser les fonctionnalités SAML (Security assertion Markup Language) intégrées à la matrice de stockage. Cette configuration établit une connexion entre un fournisseur d'identité et le fournisseur de stockage.

Description de la tâche

Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI. Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités. Pour établir une connexion entre le IDP et la matrice de stockage, vous partagez les fichiers de métadonnées entre ces deux entités. Ensuite, vous associez les entités utilisateur IDP aux rôles de baie de stockage. Enfin, vous testez la connexion et les connexions SSO avant d'activer SAML.

> **SAML et les services d'annuaire**. Si vous activez SAML lorsque Directory Services est configuré en tant que méthode d'authentification, SAML remplace Directory Services dans System Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

Modification et désactivation. une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

La configuration de l'authentification SAML est une procédure en plusieurs étapes :

- Étape 1 : téléchargez le fichier de métadonnées IDP
- Étape 2 : exporter les fichiers du fournisseur de services
- Étape 3 : rôles de carte
- Étape 4 : testez la connexion SSO
- Étape 5 : activer SAML

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez ces métadonnées dans System 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.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.

Description de la tâche

Dans cette tâche, vous téléchargez un fichier de métadonnées depuis l'IDP dans System Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues. Il vous suffit de charger un seul fichier de métadonnées pour la baie de stockage, même s'il existe deux contrôleurs.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.

   La page affiche un aperçu des étapes de configuration.

3. Cliquez sur le lien **Import Identity Provider (IDP) file**.

   La boîte de dialogue **Importer le fichier du fournisseur d'identités** s'ouvre.

4. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier de métadonnées IDP que vous avez copié sur votre système local.

   Une fois le fichier sélectionné, l'ID entité IDP s'affiche.

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le fournisseur de services intégré.

Avant de commencer

- Vous connaissez l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l'adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

1. Cliquez sur le lien **Exporter les fichiers du fournisseur de services**.

   La boîte de dialogue **Exporter les fichiers du fournisseur de services** s'ouvre.

2. Entrez l'adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local. Si la matrice de stockage comprend deux contrôleurs, répétez cette étape pour le second contrôleur dans le champ **Controller B**.

   Après avoir cliqué sur Exporter, les métadonnées du fournisseur de services sont téléchargées sur votre système local. Notez l'emplacement de stockage du fichier.

3. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

4. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur à partir des fichiers.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l'autorisation et l'accès à System Manager, vous devez mapper les attributs d'utilisateur du fournisseur intégré et les membres de groupes aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Description de la tâche

Dans cette tâche, vous utilisez System Manager pour mapper les groupes IDP aux rôles d'utilisateur local.

Étapes

1. Cliquez sur le lien permettant de mapper les rôles de System Manager.

   La boîte de dialogue **Role Mapping** s'ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

   Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

   Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

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

   Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

   Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Rechercher un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

   Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations supplémentaires. Assurez-vous que :

   - L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
   - Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
   - Les adresses de contrôleur dans les fichiers de métadonnées du processeur de service sont correctes.

Étape 5 : activer SAML

La dernière étape consiste à activer l'authentification utilisateur SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.
- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.

Description de la tâche

Cette tâche décrit comment terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

> **Modification et désactivation.** une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

Étapes

1. Dans l'onglet **SAML**, sélectionnez le lien **Activer SAML**.

   La boîte de dialogue **confirmer l'activation de SAML** s'ouvre.

2. Type `enable`, Puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultat

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

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 administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

   La boîte de dialogue **Role Mapping** s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

   Veillez à ne pas supprimer vos autorisations lorsque le langage SAML est activé, ou vous perdez l'accès à System Manager.

   Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles

   Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

5. **Facultativement :** cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. Cliquez sur **Enregistrer**.

Résultat

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

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du Service Provider pour la matrice de stockage et réimporter le(s) fichier(s) dans le système IDP (Identity Provider).

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.

- SAML est configuré et activé.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **Exporter**.

   La boîte de dialogue **Exporter les fichiers du fournisseur de services** s'ouvre.

4. Pour chaque contrôleur, cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Les champs de nom de domaine de chaque contrôleur sont en lecture seule.

   Notez l'emplacement de stockage du fichier.

5. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

   Il existe un fichier au format XML pour chaque contrôleur.

6. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur.
7. Cliquez sur **Fermer**.

Afficher l'activité du journal d'audit

En affichant les journaux d'audit, les utilisateurs disposant d'autorisations d'administrateur de sécurité peuvent surveiller les actions des utilisateurs, les échecs d'authentification, les tentatives de connexion non valides et la durée de vie des sessions utilisateur.

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.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.

   L'activité Journal d'audit apparaît sous forme de tableau, qui inclut les colonnes d'informations suivantes :

   - **Date/heure** — horodatage du moment où la matrice de stockage a détecté l'événement (en GMT).

- **Nom d'utilisateur** — le nom d'utilisateur associé à l'événement. Pour toute action non authentifiée sur la matrice de stockage, « N/A » apparaît comme nom d'utilisateur. Les actions non authentifiées peuvent être déclenchées par le proxy interne ou un autre mécanisme.
- **Code d'état** — Code d'état HTTP de l'opération (200, 400, etc.) et texte descriptif associé à l'événement.
- **URL accédée** — URL complète (y compris l'hôte) et chaîne de requête.
- **Adresse IP du client** — adresse IP du client associé à l'événement.
- **Source** — Source de consignation associée à l'événement, qui peut être System Manager, CLI, Web Services ou support Shell.

3. Utilisez les sélections de la page Journal d'audit pour afficher et gérer les événements.

Détails de la sélection

Sélection	Description
Afficher les événements du…	Événements de limite indiqués par plage de dates (24 dernières heures, 7 derniers jours, 30 derniers jours ou une plage de dates personnalisée).
Filtre	Limiter les événements indiqués par les caractères saisis dans le champ. Utilisez les guillemets ("") pour une correspondance exacte, entrez `OR` pour retourner un ou plusieurs mots, ou entrez un tiret (--) pour omettre des mots.
Actualisez	Sélectionnez **Actualiser** pour mettre à jour la page avec les événements les plus courants.
Afficher/modifier les paramètres	Sélectionnez **Afficher/Modifier les paramètres** pour ouvrir une boîte de dialogue qui vous permet de spécifier une stratégie de journalisation complète et le niveau d'actions à enregistrer.
Supprimer des événements	Sélectionnez **Supprimer** pour ouvrir une boîte de dialogue qui vous permet de supprimer d'anciens événements de la page.
Afficher/masquer les colonnes	Cliquez sur l'icône de colonne **Afficher/Masquer** pour sélectionner des colonnes supplémentaires à afficher dans le tableau. Les colonnes supplémentaires incluent : • **Méthode** — la méthode HTTP (PAR exemple, POST, GET, DELETE, etc.). • **Commande CLI exécutée** — la commande CLI (grammaire) exécutée pour les requêtes Secure CLI. • **CLI Return Status** — Un code d'état CLI ou une demande de fichiers d'entrée du client. • **Symbole procédure** — la procédure de symbole exécutée. • **Type d'événement SSH** — Type d'événements Secure Shell (SSH), tels que login, logout et login_fail. • **SSH session PID** — Numéro d'ID de processus de la session SSH. • **Durée(s) de session SSH** — nombre de secondes pendant lesquelles l'utilisateur a été connecté.
Activer/désactiver les filtres de colonne	Cliquez sur l'icône **basculer** pour ouvrir des champs de filtrage pour chaque colonne. Entrez des caractères dans un champ de colonne pour limiter les événements affichés par ces caractères. Cliquez à nouveau sur l'icône pour fermer les champs de filtrage.
Annuler les modifications	Cliquez sur l'icône **Annuler** pour rétablir la configuration par défaut de la table.

Sélection	Description
Exporter	Cliquez sur **Exporter** pour enregistrer les données de la table dans un fichier CSV (valeurs séparées par des virgules).

Définissez des règles de journal d'audit

Vous pouvez modifier la stratégie d'écrasement et les types d'événements enregistrés dans le journal d'audit.

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

Cette tâche décrit comment modifier les paramètres du journal d'audit, qui incluent la stratégie de remplacement des anciens événements et la stratégie d'enregistrement des types d'événements.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

   La boîte de dialogue **Paramètres du journal d'audit** s'ouvre.

4. Modifiez la politique de remplacement ou les types d'événements enregistrés.

Détails du champ

Réglage	Description
Politique d'écrasement	Détermine la stratégie d'écrasement des anciens événements lorsque la capacité maximale est atteinte : • **Permettre l'écrasement des événements les plus anciens du journal d'audit lorsque le journal d'audit est plein** — écrase les anciens événements lorsque le journal d'audit atteint 50,000 enregistrements. • **Exiger la suppression manuelle des événements du journal d'audit** — indique que les événements ne seront pas automatiquement supprimés ; un avertissement de seuil apparaît au pourcentage défini. Les événements doivent être supprimés manuellement. Si la stratégie de remplacement est désactivée et que les entrées du journal d'audit atteignent la limite maximale, l'accès à System Manager est refusé aux utilisateurs sans les autorisations d'administrateur de sécurité. Pour restaurer l'accès au système aux utilisateurs sans autorisations d'administrateur de sécurité, un utilisateur affecté au rôle d'administrateur de sécurité doit supprimer les anciens enregistrements d'événements. Les règles d'écrasement ne s'appliquent pas si un serveur syslog est configuré pour l'archivage des journaux d'audit.

Réglage	Description
Niveau des actions à consigner	Détermine les types d'événements à enregistrer : • **Événements de modification d'enregistrement uniquement** — affiche uniquement les événements où une action utilisateur implique d'effectuer un changement dans le système. • **Enregistrer tous les événements de modification et de lecture seule** — affiche tous les événements, y compris une action utilisateur qui implique la lecture ou le téléchargement d'informations.

5. Cliquez sur **Enregistrer**.

Supprimer des événements du journal d'audit

Vous pouvez effacer le journal d'audit des anciens événements, ce qui facilite la recherche à travers les événements. Vous avez la possibilité d'enregistrer les anciens événements dans un fichier CSV (valeurs séparées par des virgules) lors de la suppression.

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

Cette tâche décrit comment supprimer d'anciens événements du journal d'audit.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Supprimer**.

   La boîte de dialogue **Supprimer le journal d'audit** s'ouvre.

4. Sélectionnez ou entrez le nombre d'événements les plus anciens que vous souhaitez supprimer.
5. Si vous souhaitez exporter les événements supprimés dans un fichier CSV (recommandé), cochez la case. Vous êtes invité à saisir un nom de fichier et un emplacement lorsque vous cliquez sur **Supprimer** à l'étape suivante. Sinon, si vous ne souhaitez pas enregistrer les événements dans un fichier CSV, cochez la case pour le désélectionner.
6. Cliquez sur **Supprimer**.

   Une boîte de dialogue de confirmation s'ouvre.

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

Les événements les plus anciens sont supprimés de la page Journal d'audit.

Configuration du serveur syslog pour les journaux d'audit

Si vous souhaitez archiver les journaux d'audit sur un serveur syslog externe, vous pouvez configurer les communications entre ce serveur et la matrice de stockage. Une fois la connexion établie, les journaux d'audit sont automatiquement enregistrés sur le serveur syslog.

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.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet **Audit Log**, sélectionnez **configurer les serveurs Syslog**.

   La boîte de dialogue **configurer les serveurs Syslog** s'ouvre.

3. Cliquez sur **Ajouter**.

   La boîte de dialogue **Ajouter serveur Syslog** s'ouvre.

4. Entrez les informations relatives au serveur, puis cliquez sur **Ajouter**.
   - Adresse du serveur — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - Protocol — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - Télécharger le certificat (facultatif) — si vous avez sélectionné le protocole TLS et que vous n'avez pas encore téléchargé de certificat d'autorité de certification signé, cliquez sur Parcourir pour télécharger un fichier de certificat. Les journaux d'audit ne sont pas archivés sur un serveur syslog sans certificat de confiance.

     > Si le certificat devient non valide ultérieurement, l'établissement de liaison TLS échouera. Par conséquent, un message d'erreur est affiché dans le journal d'audit et les messages ne sont plus envoyés au serveur syslog. Pour résoudre ce problème, vous devez corriger le certificat sur le serveur syslog, puis aller dans le menu Paramètres[Journal d'audit > configurer les serveurs Syslog > tout tester].

   - Port — saisissez le numéro de port du récepteur syslog. Après avoir cliqué sur **Ajouter**, la boîte de dialogue **configurer les serveurs Syslog** s'ouvre et affiche votre serveur syslog configuré sur la page.
5. Pour tester la connexion du serveur avec la matrice de stockage, sélectionnez **Tester tout**.

Résultat

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

Modifier les paramètres du serveur syslog pour les enregistrements du journal d'audit

Vous pouvez modifier les paramètres du serveur syslog utilisé pour l'archivage des journaux d'audit et télécharger également un nouveau certificat d'autorité de certification (CA) pour le 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.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si vous téléchargez un nouveau certificat d'autorité de certification, celui-ci doit être disponible sur votre système local.

Étapes

1. Sélectionnez **Paramètres › gestion des accès**.
2. Dans l'onglet **Audit Log**, sélectionnez **configurer les serveurs Syslog**.

   Les serveurs syslog configurés sont affichés sur la page.

3. Pour modifier les informations sur le serveur, sélectionnez l'icône **Modifier** (crayon) à droite du nom du serveur, puis apportez les modifications souhaitées dans les champs suivants :
   - Adresse du serveur — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
   - Protocol — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
   - Port — saisissez le numéro de port du récepteur syslog.
4. Si vous avez modifié le protocole en protocole TLS sécurisé (UDP ou TCP), cliquez sur **Importer un certificat approuvé** pour télécharger un certificat d'autorité de certification.
5. Pour tester la nouvelle connexion avec la matrice de stockage, sélectionnez **Tester tout**.

Résultat

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

FAQ

Pourquoi ne puis-je pas me connecter ?

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

Des erreurs de connexion à System 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.
- Une condition de verrouillage a été déclenchée et votre journal d'audit est peut-être plein. Accédez à Access Management et supprimez les anciens événements du journal d'audit.
- L'authentification SAML est activée. Actualisez votre navigateur pour vous connecter.

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, assurez-vous de respecter les exigences suivantes.

- 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 suivantes.

Les fonctionnalités RBAC intégrées de la baie de stockage (contrôle d'accès basé sur des rôles) incluent les rôles suivants :

- **Storage admin** — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.
- **Security admin** — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).
- **Support admin** — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. 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.

Services d'annuaire

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.
- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

SAML

Si vous utilisez les fonctionnalités SAML intégrées à la baie de stockage, vérifiez que :

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance à un groupe dans le système IDP.
- Vous connaissez les noms d'appartenance à un groupe.
- Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

Quels outils de gestion externe peuvent être affectés par ce changement ?

Lorsque vous apportez certaines modifications à System Manager, par exemple le basculement de l'interface de gestion ou l'utilisation de SAML pour une méthode d'authentification, certains outils et fonctionnalités externes peuvent être limités d'utilisation.

Interface de gestion

Les outils qui communiquent directement avec l'interface de gestion héritée (symbole), tels que le fournisseur SMI-S SANtricity ou OnCommand Insight (OCI), ne fonctionnent pas si le paramètre d'interface de gestion héritée est activé. En outre, vous ne pouvez pas utiliser de commandes CLI héritées ou effectuer des opérations de mise en miroir si ce paramètre est désactivé.

Contactez le support technique pour plus d'informations.

Authentification SAML

Lorsque le langage SAML est activé, les clients suivants ne peuvent pas accéder aux services et ressources de la baie de stockage :

- Fenêtre de gestion Enterprise (EMW)
- Interface de ligne de commandes
- Clients SDK (Software Developer kits)
- Clients intrabande
- Clients API REST HTTP Basic Authentication
- Connectez-vous à l'aide d'un terminal API REST standard

Contactez le support technique pour plus d'informations.

Que dois-je savoir avant de configurer et d'activer le langage SAML ?

Avant de configurer et d'activer les fonctionnalités SAML pour l'authentification, assurez-vous de respecter les exigences suivantes et de comprendre les restrictions SAML.

De formation

Avant de commencer, assurez-vous que :

- Un fournisseur d'identité (IDP) est configuré dans votre réseau. Un IDP est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si l'utilisateur est authentifié avec succès. Votre équipe de sécurité est responsable du maintien du PDI.
- Un administrateur IDP a configuré des attributs utilisateur et des groupes dans le système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.
- Vous connaissez l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.

Restrictions

Outre les exigences ci-dessus, assurez-vous de bien comprendre les restrictions suivantes :

- Une fois le langage SAML activé, vous ne pouvez pas le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide. Nous vous recommandons de tester les connexions SSO avant d'activer SAML lors de l'étape de configuration finale. (Le système exécute également un test de connexion SSO avant d'activer SAML.)
- Si vous désactivez SAML à l'avenir, le système restaure automatiquement la configuration précédente (rôles d'utilisateur local et/ou Services d'annuaire).
- Si les services d'annuaire sont actuellement configurés pour l'authentification des utilisateurs, le langage SAML remplace cette configuration.
- Lorsque le langage SAML est configuré, les clients suivants ne peuvent pas accéder aux ressources de la baie de stockage :
  - Fenêtre de gestion Enterprise (EMW)
  - Interface de ligne de commandes
  - Clients SDK (Software Developer kits)
  - Clients intrabande
  - Clients API REST HTTP Basic Authentication
  - Connectez-vous à l'aide d'un terminal API REST standard

Quels types d'événements sont enregistrés dans le journal d'audit ?

Le journal d'audit peut enregistrer les événements de modification ou les événements de modification et de lecture seule.

Selon les paramètres de la stratégie, les types d'événements suivants sont affichés :

- **Événements de modification** — actions de l'utilisateur depuis System Manager qui impliquent des modifications du système, telles que le provisionnement du stockage.

- **Événements de modification et de lecture seule** — actions utilisateur impliquant des modifications du système, ainsi que des événements impliquant l'affichage ou le téléchargement d'informations, tels que l'affichage des affectations de volume.

Que dois-je savoir avant de configurer un serveur syslog ?

Vous pouvez archiver les journaux d'audit sur un serveur syslog externe.

Avant de configurer un serveur syslog, gardez les consignes suivantes à l'esprit.

- Assurez-vous de connaître l'adresse du serveur, le protocole et le numéro de port. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.
- Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.
- Les paramètres **Overwrite Policy** (disponible dans View/Edit Settings) n'affectent pas la façon dont les journaux sont gérés avec une configuration de serveur syslog.
- Les journaux d'audit suivent le format de messagerie RFC 5424.

Le serveur syslog ne reçoit plus les journaux d'audit. Que dois-je faire ?

Si vous avez configuré un serveur syslog avec un protocole TLS, le serveur ne peut pas recevoir de messages si le certificat devient non valide pour une raison quelconque. Un message d'erreur concernant le certificat non valide est affiché dans le journal d'audit.

Pour résoudre ce problème, vous devez d'abord corriger le certificat du serveur syslog. Une fois qu'une chaîne de certificats valide est en place, accédez au **Paramètres › Journal d'audit › configurer les serveurs Syslog › tout tester**.