



Concepts

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

- 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 3
 - Gestion des accès avec les services d'annuaire 4
 - Gestion des accès avec SAML 5

Concepts

Fonctionnement de Access Management

Utilisez Access Management pour établir l'authentification des utilisateurs dans 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.



Lors de la première connexion, le nom d'utilisateur `admin` s'affiche automatiquement et ne peut pas être modifié. L'`admin` 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.
 - **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 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 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. |

| 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 fonction SAML intégrée à la baie de stockage est conforme à la norme SAML2.0 pour l'assertion, l'authentification et l'autorisation d'identité. |
| 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 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 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.



L'administrateur 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.



L'administrateur 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.

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 Unified Manager avec un profil utilisateur qui inclut des autorisations d'administrateur de sécurité.



L'administrateur 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 à partir du système IDP, puis utilise Unified 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 Unified Manager pour exporter un fichier de métadonnées du fournisseur de services pour le contrôleur. À partir du système IDP, l'administrateur importe ensuite le fichier de métadonnées dans ce dernier.



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 Unified 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. À partir d'Unified Manager, l'administrateur active 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 SAML est activé, les utilisateurs ne peuvent pas détecter ou gérer le stockage de cette baie à partir de l'interface Storage Manager héritée.

En outre, les clients suivants ne peuvent pas accéder aux ressources et aux services 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

Informations sur le copyright

Copyright © 2024 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 DÉLICTEUELLE (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.