



Utiliser les services d'annuaire

SANtricity 11.7

NetApp
February 12, 2024

Sommaire

- Utiliser les services d'annuaire 1
- Ajouter un serveur de répertoire 1
- Modifier les paramètres du serveur d'annuaire et les mappages de rôles 6
- Supprimer le serveur de répertoire 10

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 Web Services Proxy pour 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 (<i>username@domain</i>) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
Saisissez l'URL d'accès au serveur LDAP sous la forme de <code>ldap[s]://host:port*</code> .	Télécharger le certificat (facultatif)

Réglage	Description
<div data-bbox="245 394 302 453" style="border: 1px solid black; border-radius: 50%; width: 20px; height: 20px; display: flex; align-items: center; justify-content: center; margin-bottom: 10px;">i</div> <p data-bbox="358 170 480 674">Ce champ apparaît uniquement si un protocole LDAPS est spécifié dans le champ URL du serveur ci-dessus.</p> <p data-bbox="212 726 496 1062">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.</p>	<p data-bbox="529 159 846 191">Lier un compte (facultatif)</p>
<p data-bbox="212 1115 513 1661">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.</p>	<p data-bbox="529 1115 959 1146">Liaison du mot de passe (facultatif)</p>

Réglage	Description
 <p>Ce champ s'affiche lorsque vous entrez un compte de liaison.</p> <p>Saisissez le mot de passe du compte de liaison.</p>	<p>Testez la connexion au serveur avant d'ajouter</p>
<p>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.</p> <p>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.</p>	<p>Paramètres des privilèges</p>
<p>Rechercher un NA de base</p>	<p>Entrez le contexte LDAP pour rechercher des utilisateurs, généralement sous la forme de CN=Users, DC=cpoc, DC=local.</p>
<p>Attribut de nom d'utilisateur</p>	<p>Saisissez l'attribut lié à l'ID utilisateur pour l'authentification. Par exemple : sAMAccountName.</p>
<p>Attribut(s) de groupe</p>	<p>Entrez une liste d'attributs de groupe sur l'utilisateur, qui est utilisée pour le mappage groupe-rôle. Par exemple : memberOf, managedObjects.</p>

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 échappés avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulier : <code>\.[]{}()<>*+.-=!/?^\$</code>	
Rôles	<p>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 :</p> <ul style="list-style-type: none">• 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 (<i>username@domain</i>) pour spécifier le serveur de répertoire à authentifier.	URL du serveur
URL d'accès au serveur LDAP sous la forme de <code>ldap[s]://host:port</code> .	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 : <code>\.[]{}()<>*+.=!?^\$</code>	
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 : <ul style="list-style-type: none">• 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.

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 DÉLICTELLE (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.