

Serveurs LDAP pour AAA

Ce chapitre décrit comment configurer les serveurs LDAP utilisés dans AAA.

- À propos de LDAP et de l'ASA, à la page 1
- Lignes directrices relatives aux serveurs LDAP pour AAA, à la page 5
- Configurer les serveurs LDAP pour AAA, à la page 6
- Tester l'authentification et l'autorisation du serveur LDAP, à la page 10
- Supervision des serveurs LDAP pour AAA, à la page 10
- Historique des serveurs LDAP pour AAA, à la page 11

À propos de LDAP et de l'ASA

L'ASA est compatible avec la plupart des serveurs de répertoire LDAPv3, notamment :

- Sun Microsystems JAVA System Directory Server, fait désormais partie de l'édition Enterprise du serveur de répertoire Oracle, et anciennement nommé serveur de répertoire Sun ONE
- Microsoft Active Directory
- Novell
- OpenLDAP

Par défaut, l'ASA détecte automatiquement s'il est connecté à Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP ou à un serveur de répertoire LDAPv3 générique. Toutefois, si la détection automatique ne parvient pas à déterminer le type de serveur LDAP, vous pouvez le configurer manuellement.

Fonctionnement de l'authentification avec LDAP

Pendant l'authentification, l'ASA agit comme mandataire client auprès du serveur LDAP pour l'utilisateur et s'authentifie auprès du serveur LDAP en texte brut ou à l'aide du protocole SASL. Par défaut, l'ASA transmet les paramètres d'authentification, généralement un nom d'utilisateur et un mot de passe, au serveur LDAP en texte brut.

L'ASA prend en charge les mécanismes SASL suivants, répertoriés par ordre croissant de puissance :

- Digest-MD5 : l'ASA répond au serveur LDAP par une valeur MD5 calculée à partir du nom d'utilisateur et du mot de passe.

- Kerberos : l'ASA répond au serveur LDAP en envoyant le nom d'utilisateur et le domaine à l'aide du mécanisme GSSAPI Kerberos.

L'ASA et le serveur LDAP prennent en charge toutes les combinaisons possibles de ces mécanismes SASL. Si vous configurez plusieurs mécanismes, l'ASA récupère la liste des mécanismes SASL configurés sur le serveur et définit le mécanisme d'authentification le plus puissant configuré à la fois sur l'ASA et le serveur. Par exemple, si le serveur LDAP et l'ASA prennent en charge les deux mécanismes, l'ASA sélectionne Kerberos, le plus fort des deux.

Une fois l'authentification LDAP de l'utilisateur réussie, le serveur LDAP renvoie les attributs pour l'utilisateur authentifié. Pour l'authentification VPN, ces attributs incluent généralement des données d'autorisation appliquées à la session VPN. Dans ce cas, l'utilisation de LDAP permet d'effectuer l'authentification et l'autorisation en une seule étape.

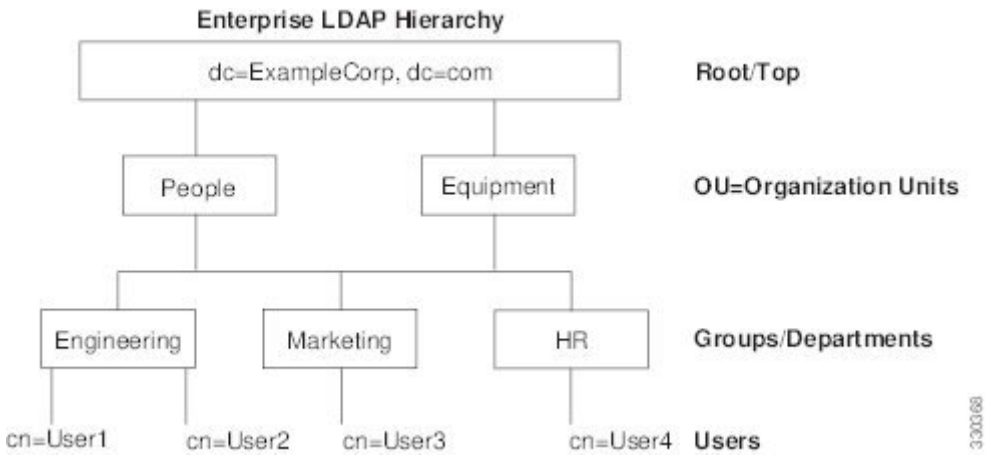
Remarque Pour en savoir plus sur LDAP, consultez les RFC 1777, 2251 et 2849.

Hiérarchie LDAP

Votre configuration LDAP doit refléter la hiérarchie logique de votre organisation. Par exemple, supposons qu'un employé de votre entreprise, Exemple Société, s'intitule Employé1. Employé 1 travaille dans le groupe d'ingénierie. Votre hiérarchie LDAP peut comporter un ou plusieurs niveaux. Vous pourriez décider de configurer une hiérarchie à un seul niveau dans laquelle Employé1 est considéré comme membre d'Exemple Société. Ou vous pouvez configurer une hiérarchie à plusieurs niveaux dans laquelle Employé1 est considéré comme un membre du service d'ingénierie, qui est lui-même membre d'une unité organisationnelle appelée Personnel, qui est elle-même membre d'Exemple Société. Consultez la figure suivante pour obtenir un exemple de hiérarchie à plusieurs niveaux.

Une hiérarchie à plusieurs niveaux est plus détaillée, mais les recherches renvoient des résultats plus rapidement dans une hiérarchie à un seul niveau.

Illustration 1 : Une hiérarchie LDAP à plusieurs niveaux



Rechercher dans la hiérarchie LDAP

L'ASA vous permet d'adapter la recherche dans la hiérarchie LDAP. Vous devez configurer les trois champs suivants sur l'ASA pour définir à quel niveau de la hiérarchie LDAP votre recherche doit commencer, son étendue et le type de renseignements que vous recherchez. Ensemble, ces champs limitent la recherche dans la hiérarchie à la partie qui inclut les autorisations des utilisateurs.

- Le DN de base LDAP définit à quel niveau de la hiérarchie LDAP le serveur doit commencer à rechercher les renseignements de l'utilisateur lorsqu'il reçoit une demande d'autorisation de l'ASA.
- La portée de recherche définit l'étendue de la recherche dans la hiérarchie LDAP. La recherche se poursuit sur ces nombreux niveaux dans la hiérarchie sous le DN de base LDAP. Vous pouvez choisir de demander au serveur de rechercher uniquement le niveau immédiatement en dessous, ou il peut rechercher dans toute la sous-arborescence. Une recherche à un seul niveau est plus rapide, mais une recherche dans la sous-arborescence est plus approfondie.
- Les attributs de nommage définissent le RDN qui identifie de manière unique une entrée dans le serveur LDAP. Les attributs de nommage courants peuvent inclure cn (nom commun), sAMAccountName et userPrincipalName.

La figure montre un exemple de hiérarchie LDAP pour l'exemple de société. Compte tenu de cette hiérarchie, vous pouvez définir votre recherche de différentes manières. Le tableau suivant présente deux exemples de configuration de recherche.

Dans le premier exemple de configuration, lorsque Employé1 établit le tunnel IPsec avec l'autorisation LDAP requise, l'ASA envoie une demande de recherche au serveur LDAP, indiquant qu'il doit rechercher Employé1 dans le groupe d'ingénierie. Cette recherche est rapide.

Dans le deuxième exemple de configuration, l'ASA envoie une demande de recherche indiquant que le serveur doit rechercher Employé1 dans l'exemple de société. Cette recherche prend plus de temps.

Tableau 1 : Exemples de configuration de recherche

Non.	DN de base LDAP	Portée de la recherche	Attribut de nommage	Résultat
1	group= Ingénierie,ou=Personnes,dc=ExempleSociété, dc=com	Un niveau	cn=Employé1	Recherche plus rapide
2	dc=ExempleSociété,dc=com	Sous-arborescence	cn=Employé1	Recherche plus longue

Lier à un serveur LDAP

L'ASA utilise le nom de domaine (DN) de connexion et le mot de passe de connexion pour établir la confiance (liaison) avec un serveur LDAP. Lors d'une opération en lecture seule Microsoft Active Directory (comme l'authentification, l'autorisation ou la recherche de groupe), l'ASA peut se lier à l'aide d'un DN de connexion avec moins de privilèges. Par exemple, le DN de connexion peut être un utilisateur dont la désignation AD « Membre de » fait partie des utilisateurs de domaine. Pour les opérations de gestion des mots de passe VPN, le nom de domaine de connexion a besoin de privilèges élevés et doit faire partie du groupe AD des opérateurs de compte.

Remarque Lors de la configuration de l'authentification LDAP sur les périphériques Firepower 1000/2100, évitez d'utiliser une barre oblique inverse (« \ ») dans le mot de passe de liaison. La présence d'une barre oblique inverse dans le mot de passe entraîne l'échec du processus de liaison LDAP, ce qui entraîne l'échec de l'authentification extérieure.

Voici un exemple de DN de connexion :

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

L'ASA prend en charge les méthodes d'authentification suivantes :

- Authentification LDAP simple avec un mot de passe non chiffré sur le port 389
- LDAP sécurisé (LDAP-S) sur le port 636
- Couche d'authentification et de sécurité simple (SASL) MD5
- SASL Kerberos

L'ASA ne prend pas en charge l'authentification anonyme.

Remarque En tant que client LDAP, l'ASA ne prend pas en charge la transmission de liaisons ou de demandes anonymes.

Cartes d'attribut LDAP

L'ASA peut utiliser un répertoire LDAP pour authentifier les utilisateurs pour :

- Les utilisateurs VPN d'accès à distance
- Les sessions d'accès au réseau du pare-feu/de mandataire direct
- La définition des autorisations de politique (également appelées attributs d'autorisation), telles que les ACL, les listes de signets, les paramètres DNS ou WINS et les minuteries de session.
- La définition des attributs clés dans une stratégie de groupe locale

L'ASA utilise des cartes d'attributs LDAP pour traduire les attributs des utilisateurs LDAP natifs en attributs ASA. Vous pouvez lier ces cartes d'attributs aux serveurs LDAP ou les supprimer. Vous pouvez également afficher ou effacer les cartes d'attributs.

La carte d'attributs LDAP ne prend pas en charge les attributs à valeurs multiples. Par exemple, si un utilisateur est membre de plusieurs groupes AD et que la carte d'attributs LDAP correspond à plusieurs groupes, la valeur choisie est basée sur l'ordre alphabétique des entrées correspondantes.

Pour utiliser correctement les fonctionnalités de mappage d'attributs, vous devez comprendre les noms et les valeurs des attributs LDAP, ainsi que les noms et les valeurs des attributs définis par l'utilisateur.

Les noms des attributs LDAP fréquemment mappés et le type d'attributs définis par l'utilisateur auxquels ils sont généralement mappés sont les suivants :

- IETF-Radius-Class (Group_Policy dans ASA version 8.2 et ultérieure) : définit la stratégie de groupe en fonction de la valeur d'attribut du service répertoire ou du groupe d'utilisateurs (par exemple, Microsoft Active Directory memberOf). L'attribut de stratégie de groupe a remplacé l'attribut IETF-Radius-Class par ASDM version 6.2/ASA version 8.2 ou ultérieure.
- IETF-Radius-Filter-Id : applique une liste de contrôle d'accès ou une ACL aux clients VPN, IPsec et SSL.
- IETF-Radius-Framed-IP-Address : attribue une adresse IP statique à un client d'accès à distance VPN, IPsec et SSL.
- Banner1 : affiche une bannière de texte lorsque l'utilisateur d'accès à distance VPN se connecte.
- Tunneling-Protocols : autorise ou refuse la session d'accès à distance VPN en fonction du type d'accès.

Remarque Une seule carte d'attributs LDAP peut contenir un ou plusieurs attributs. Vous ne pouvez mapper qu'un seul attribut LDAP à partir d'un serveur LDAP donné.

Lignes directrices relatives aux serveurs LDAP pour AAA

Cette section inclut des lignes directrices et des limites que vous devez vérifier avant de configurer les serveurs LDAP pour l'AAA.

IPv6

Le serveur AAA peut utiliser une adresse IPv4 ou IPv6.

Directives supplémentaires

- Le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACL sur la politique de mot de passe par défaut.
- Vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec les serveurs Microsoft Active Directory et Sun.
- L'ASA ne prend pas en charge la gestion des mots de passe avec Novell, OpenLDAP et les autres serveurs de répertoire LDAPv3.
- À partir de la version 7.1(x), l'ASA effectue l'authentification et l'autorisation à l'aide du schéma LDAP natif, et le schéma Cisco n'est plus nécessaire.
- Vous pouvez avoir jusqu'à 200 groupes de serveurs en mode unique ou 4 groupes de serveurs par contexte en mode multiple.
- Chaque groupe peut avoir jusqu'à 16 serveurs en mode unique ou 8 serveurs en mode multiple.
- Lorsqu'un utilisateur se connecte, les serveurs LDAP sont accessibles un par un en commençant par le premier serveur que vous spécifiez dans la configuration, jusqu'à ce qu'un serveur réponde. Si tous les serveurs du groupe sont indisponibles, l'ASA essaie la base de données locale si vous l'avez configurée

comme méthode de secours (authentification et autorisation de gestion uniquement). Si vous n'avez pas de méthode de secours, l'ASA continue d'essayer les serveurs LDAP.

Configurer les serveurs LDAP pour AAA

Cette section décrit comment configurer les serveurs LDAP pour AAA.

Procédure

Étape 1 Configurez les cartes d'attributs LDAP. Consultez Configurer les cartes d'attribut LDAP, à la page 6.

Étape 2 Ajoutez un groupe de serveurs LDAP. Consultez Configurer les groupes de serveurs LDAP, à la page 7.

Étape 3 Ajoutez un serveur au groupe, puis configurez les paramètres du serveur. Consultez Ajouter un serveur LDAP à un groupe de serveurs , à la page 8.

Configurer les cartes d'attribut LDAP

Pour configurer les cartes d'attributs LDAP, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA Local Users (Utilisateurs locaux AAA)** > **LDAP Attribute Map (Carte d'attributs LDAP)** (pour les utilisateurs locaux) ou **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **LDAP Attribute Map (Carte d'attributs LDAP)** (pour tous les autres utilisateurs), puis cliquez sur **Add**.

La boîte de dialogue **Add LDAP Attribute Map** (Ajouter une carte d'attributs LDAP) s'affiche et l'onglet **Mapping of Attribute Name** (Mappage du nom d'attribut) est actif.

Étape 2 Créez un nom pour cette carte d'attributs.

Étape 3 Ajoutez le nom de l'un des attributs LDAP à mapper.

Étape 4 Choisissez un attribut Cisco.

Étape 5 Cliquez sur **Add** (ajouter).

Étape 6 Pour mapper d'autres attributs, répétez les étapes 1 à 5.

Étape 7 Cliquez sur l'onglet **Mappage of Attribute Value** (Mappage de la valeur d'attribut) pour mapper la valeur de l'un des attributs LDAP à une nouvelle valeur dans l'attribut Cisco mappé.

Étape 8 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Mapping of Attribute Value** (Ajouter le mappage de la valeur d'attribut).

Étape 9 Saisissez la valeur de cet attribut LDAP que vous souhaitez renvoyer par le serveur LDAP.

Étape 10 Saisissez la valeur que vous souhaitez utiliser dans l'attribut Cisco lorsque cet attribut LDAP contient la valeur d'attribut LDAP précédente.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Pour mapper d'autres valeurs d'attribut, répétez les étapes 8 à 11.

Étape 13 Cliquez sur **OK** deux fois pour fermer chaque boîte de dialogue.

Étape 14 Cliquez sur **Apply** (Appliquer) pour enregistrer les paramètres dans la configuration d'exécution.

Configurer les groupes de serveurs LDAP

Pour créer et configurer un groupe de serveurs LDAP, puis ajouter un serveur LDAP à ce groupe, procédez comme suit :

Avant de commencer

Vous devez ajouter une mise en correspondance d'attributs avant de pouvoir ajouter un serveur LDAP à un groupe de serveurs LDAP.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)** ou **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **AAA Server Groups (Groupes de serveurs AAA)** pour les utilisateurs VPN.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez un nom pour le groupe de serveurs AAA.

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur LDAP.

Étape 5 Cliquez sur le bouton radio du mode de réactivation que vous souhaitez utiliser (**Depletion** (Épuisement) ou **Timed** (Temporisé)).

En mode Depletion (Épuisement), les serveurs défaillants ne sont réactivés qu'une fois que tous les serveurs du groupe sont inactifs.

En mode Timed (Temporisé), les serveurs défaillants sont réactivés après 30 secondes de temps d'arrêt.

a) Si vous avez choisi le mode de réactivation Depletion (Épuisement), saisissez un intervalle de temps dans le champ **Dead Time** (Temps mort).

Le temps mort est la durée, en minutes, qui s'écoule entre la désactivation du dernier serveur d'un groupe et la réactivation ultérieure de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort.

Étape 6 Ajoutez le nombre maximum de transactions AAA échouées avec le serveur à autoriser.

Cette option définit le nombre de tentatives de connexion échouées autorisées avant de déclarer inactif un serveur qui ne répond pas.

Étape 7 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server Group** (Ajouter un groupe de serveurs AAA) se ferme et le nouveau groupe de serveurs est ajouté au groupe de serveurs AAA.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un serveur LDAP à un groupe de serveurs

Pour ajouter un serveur LDAP à un groupe de serveurs, procédez comme suit :

Procédure

Étape 1 Effectuez l'une des opérations suivantes :

- **Configuration Remote Access VPN (VPN d'accès à distance) AAA/Local Users (AAA/Utilisateurs locaux) AAA Server Groups (Groupes de serveurs AAA)** pour les utilisateurs VPN.
- **Configuration** >**Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**

Étape 2 Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter un serveur, puis cliquez sur **Add**.

La boîte de dialogue **Add AAA Server** (Ajouter un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 3 Choisissez le nom de l'interface qui se connecte au serveur LDAP.

Étape 4 Ajoutez le nom du serveur ou l'adresse IP du serveur LDAP.

Étape 5 Ajoutez une valeur de délai d'expiration ou conservez la valeur par défaut. Le délai d'expiration est la durée, en secondes, pendant laquelle l'ASA attend une réponse du serveur principal avant d'envoyer la demande au serveur de sauvegarde.

Étape 6 Dans la zone **LDAP Parameters for authentication/authorization** (Paramètres LDAP pour l'authentification/l'autorisation), configurez les paramètres suivants :

- **Enable LDAP over SSL** (Activer LDAP sur SSL) (également appelé LDAP sécurisé ou LDAP-S) : cochez cette case pour utiliser SSL pour sécuriser les communications entre l'ASA et le serveur LDAP.

Remarque Si vous ne configurez pas le protocole SASL, nous vous conseillons fortement de sécuriser les communications LDAP avec SSL.

- **Reference Identity Name** (Nom d'identité de référence) : saisissez le nom d'identité de référence pour valider l'identité du serveur LDAP.
- **Server Port** (Port du serveur) : saisissez le numéro de port TCP 389, le port utilisé par l'ASA pour accéder au serveur LDAP pour l'authentification simple (non sécurisée), ou le port TCP 636 pour l'authentification sécurisée (LDAP-S). Tous les serveurs LDAP prennent en charge l'authentification et l'autorisation. Seuls les serveurs Microsoft AD et Sun LDAP fournissent en outre une fonctionnalité de gestion des mots de passe d'accès à distance VPN, qui nécessite LDAP-S.

- **Server Type** (Type de serveur) : spécifiez le type de serveur LDAP dans la liste déroulante. Les options disponibles sont les suivantes :
  - **Détection automatique/Utilisation du type générique**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun, qui fait désormais partie d'Oracle Directory Server Enterprise Edition**
- **Base DN** (DN de base) : saisissez le nom distinctif (DN) de base ou l'emplacement dans la hiérarchie LDAP où le serveur doit commencer la recherche lorsqu'il reçoit une demande LDAP (par exemple, OU=people, dc=cisco, dc=com).
- **Scope** (Portée) : spécifiez l'étendue de la recherche que le serveur doit effectuer dans la hiérarchie LDAP lorsqu'il reçoit une demande d'autorisation à partir de la liste déroulante. Les options suivantes sont disponibles :
  - **One Level** (Un niveau) : recherche dans un seul niveau sous le DN de base. Cette option est plus rapide.
  - **All Levels** (Tous les niveaux) : recherche dans tous les niveaux sous le DN de base (c'est-à-dire dans la hiérarchie complète des sous-arborescences). Cette option prend plus de temps.
- **Naming Attribute(s)** (Attribut(s) de dénomination) : saisissez le ou les attributs de nom distinctif relatifs qui identifient de manière unique une entrée sur le serveur LDAP. Les attributs de dénomination courants sont Common Name (CN), sAMAccountName, userPrincipalName et User ID (uid).
- **Login DN and Login Password** (DN de connexion et mot de passe de connexion) : l'ASA utilise le DN de connexion et le mot de passe de connexion pour établir la confiance (liaison) avec un serveur LDAP. Précisez le mot de passe de connexion, qui est le mot de passe du compte d'utilisateur DN de connexion.
- **LDAP Attribute Map** (Carte d'attributs LDAP) : sélectionnez l'une des cartes d'attributs que vous avez créées pour ce serveur LDAP à utiliser. Ces cartes d'attributs mappent les noms d'attributs LDAP aux noms et aux valeurs d'attributs Cisco.
- **SASL MD5 authentication** (Authentification SASL MD5) : cela permet au mécanisme MD5 du SASL d'authentifier les communications entre l'ASA et le serveur LDAP.
- **SASL Kerberos authentication** (Authentification SASL Kerberos) : permet au mécanisme Kerberos du SASL de sécuriser les communications d'authentification entre l'ASA et le serveur LDAP. Vous devez avoir défini un serveur Kerberos pour activer cette option.
- **LDAP Parameters for Group Search** (Paramètres LDAP pour la recherche de groupes) : les champs de cette zone configurent la façon dont l'ASA demande les groupes AD.
  - **Group Base DN** (DN de base du groupe) : spécifie l'emplacement dans la hiérarchie LDAP pour commencer la recherche des groupes AD (c'est-à-dire la liste des énumérations memberOf). Si ce champ n'est pas configuré, l'ASA utilise le DN de base pour la récupération du groupe AD. ASDM utilise la liste des groupes AD récupérés pour définir les critères de sélection AAA pour les politiques d'accès dynamique. Pour en savoir plus, consultez la page de la commande **show ad-groups**.
  - **Group Search Timeout** (Délai d'expiration de la recherche de groupe) : spécifiez le temps d'attente maximum d'une réponse d'un serveur AD qui a été interrogé pour les groupes disponibles.

- **LDAP SSL Client Certificate/Client Identity Certificate Trustpoint** (Point de confiance du certificat client SSL LDAP/certificat d'identité du client) : si vous activez LDAP sur SSL, vous pouvez sélectionner le point de confiance du certificat que le client ASA doit présenter au serveur LDAP pour authentification. Un point de confiance est requis si vous configurez le serveur LDAP pour authentifier les certificats clients. Si vous ne configurez pas de certificat, l'ASA n'en présente pas lorsque le serveur LDAP le demande. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront.

Étape 7 Cliquez sur **OK**.

La boîte de dialogue **Add AAA Server** (Ajouter un serveur AAA) se ferme et le serveur AAA est ajouté au groupe de serveurs AAA.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Tester l'authentification et l'autorisation du serveur LDAP

Pour déterminer si l'ASA peut communiquer avec un serveur LDAP et authentifier ou autoriser un utilisateur, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Étape 2 Sélectionnez le groupe de serveurs dans lequel se trouve le serveur.

Étape 3 Sélectionnez le serveur que vous souhaitez tester.

Étape 4 Cliquez sur **Test**.

La boîte de dialogue **Test AAA Server** (Tester un serveur AAA) s'affiche pour le groupe de serveurs sélectionné.

Étape 5 Cliquez sur le type de test que vous souhaitez effectuer : **Authentication** (Authentification) ou **Authorization** (Autorisation).

Étape 6 Saisissez un nom d'utilisateur.

Étape 7 Si vous testez l'authentification, saisissez le mot de passe correspondant au nom d'utilisateur.

Étape 8 Cliquez sur **OK**.

L'ASA envoie un message de test d'authentification ou d'autorisation au serveur. Si le test échoue, un message d'erreur s'affiche.

Supervision des serveurs LDAP pour AAA

Consultez les commandes suivantes pour superviser les serveurs LDAP pour AAA :

- **Monitoring (Supervision) > Properties (Propriétés) > AAA Servers (Serveurs AAA)**

  Ce volet affiche les statistiques du serveur AAA configuré.

- **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**

  Ce volet vous permet d'exécuter diverses commandes non interactives et d'afficher les résultats.

Historique des serveurs LDAP pour AAA

Tableau 2 : Historique des serveurs AAA

Nom de la caractéristique	Versions de plateforme	Description
Serveurs LDAP pour AAA	7.0(1)	Les serveurs LDAP décrivent la prise en charge d'AAA et la configuration des serveurs LDAP. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Server Groups Configuration (Configuration des groupes de serveurs AAA) > Remote Access VPN (VPN d'accès à distance) > AAA Local Users (Utilisateurs locaux AAA) > LDAP Attribute Map (Carte d'attributs LDAP).
Serveurs LDAP avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.
Augmentation des limites pour les groupes de serveurs AAA et le nombre de serveurs par groupe.	9.13(1)	Vous pouvez configurer d'autres groupes de serveurs AAA. En mode de contexte unique, vous pouvez configurer 200 groupes de serveurs AAA (l'ancienne limite était de 100). En mode de contexte multiple, vous pouvez en configurer 8 (l'ancienne limite était de 4). En outre, en mode de contexte multiple, vous pouvez configurer 8 serveurs par groupe (l'ancienne limite était de 4 serveurs par groupe). La limite de 16 par groupe en mode de contexte unique reste inchangée. Nous avons modifié les écrans AAA pour accepter ces nouvelles limites.

Nom de la caractéristique	Versions de plateforme	Description
Authentification LDAPS mutuelle.	9.18(1)	Vous pouvez configurer un certificat client que l'ASA doit présenter au serveur LDAP lorsqu'il demande un certificat pour l'authentification. Cette fonctionnalité s'applique lorsque vous utilisez LDAP sur SSL. Si un serveur LDAP est configuré pour nécessiter un certificat homologue, la session LDAP sécurisée ne se terminera pas, et les demandes d'authentification ou d'autorisation échoueront. Nous avons modifié l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > > **AAA Server Groups (Groupes de serveurs AAA)**, Add/Edit LDAP server (Ajouter/modifier un serveur LDAP).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.