Serveurs LDAP pour AAA

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

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.

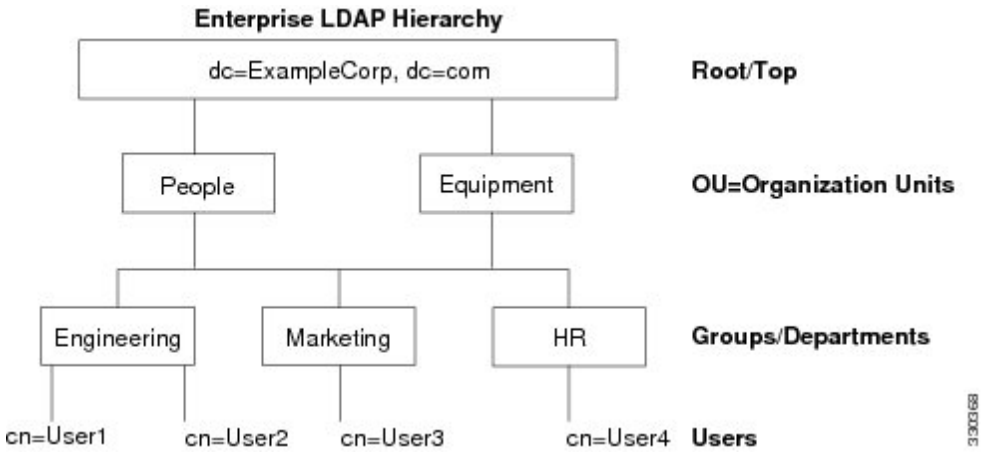
Remarque Pour en savoir plus sur LDAP, consultez les RFC 1777, 2251 et 2849.

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.

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 8.

Étape 3 (Facultatif) Configurez l'autorisation à partir d'un serveur LDAP distinct du mécanisme d'authentification. Consultez Configurer l'autorisation avec LDAP pour le VPN, à la page 10.

Configurer les cartes d'attribut LDAP

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

Procédure

Étape 1 Créez un tableau de cartes d'attributs LDAP non rempli.

ldap-attribute-map *map-name*

Exemple :

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

Étape 2 Mappez le service de nom d'attribut défini par l'utilisateur avec l'attribut Cisco.

map-name *user-attribute-name Cisco-attribute-name*

Exemple :

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

Étape 3 Mappez le service de valeur de carte définie par l'utilisateur avec la valeur de l'attribut définie par l'utilisateur et la valeur de l'attribut Cisco.

map-value *user-attribute-name Cisco-attribute-name*

Exemple :

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

Étape 4 Identifiez le serveur et le groupe de serveurs AAA auquel il appartient.

aaa-server *server_group* [*interface_name*] **host** *server_ip*

Exemple :

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

Étape 5 Liez la carte d'attributs au serveur LDAP.

ldap-attribute-map *map-name*

Exemple :

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

Exemples

L'exemple suivant montre comment limiter les sessions de gestion à l'ASA en fonction d'un attribut LDAP appelé accessType. L'attribut accessType peut avoir l'une des valeurs suivantes :

- VPN
- admin
- centre d'assistance

L'exemple suivant montre comment chaque valeur est mappée à l'un des attributs IETF-Radius-Service-Type valides que l'ASA prend en charge : remote-access (Service-Type 5) Outbound, admin (Service-Type 6) Administrative et nas-prompt (Service-Type 7) NAS Prompt.

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

L'exemple suivant montre comment afficher la liste complète des noms d'attributs LDAP de Cisco :

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

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 Identifiez le nom du groupe de serveurs et le protocole.

aaa-server *server_tag* **protocol ldap**

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

Lorsque vous saisissez la commande **aaa-server protocol**, vous passez en mode de configuration du groupe aaa-server.

Étape 2 Précisez le nombre maximum de transactions AAA échouées avec un serveur LDAP du groupe avant d'essayer le serveur suivant.

max-failed-attempts *number*

Exemple :

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

L'argument *number* peut aller de 1 à 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement) afin de configurer le mécanisme de secours, et que tous les serveurs du groupe ne répondent pas ou que leurs réponses ne sont pas valides, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

Étape 3 Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Exemple :

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

Le mot clé **depletion** réactive les serveurs défaillants uniquement après que tous les serveurs du groupe sont inactifs.

La paire mot clé-argument **deadtime** *minutes* spécifie le temps en minutes, entre 0 et 1 440, qui s'écoule entre la désactivation du dernier serveur du 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. La valeur par défaut est 10 minutes.

Le mot clé **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

Étape 4 Identifiez le serveur LDAP et le groupe de serveurs AAA auquel il appartient.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Exemple :

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

Si vous ne spécifiez pas de **(***nom d'interface***)**, l'ASA utilise la de l'interface **interne** par défaut.

Lorsque vous saisissez la commande **aaa-server host**, vous passez en mode de configuration de l'hôte aaa-server. Au besoin, utilisez les commandes du mode de configuration de l'hôte pour configurer davantage le serveur AAA.

Le tableau suivant répertorie les commandes disponibles pour les serveurs LDAP et indique si une nouvelle définition de serveur LDAP a une valeur par défaut ou non. Si aucune valeur par défaut n'est fournie (indiquée par « — »), utilisez la commande pour spécifier la valeur.

Tableau 2 : Commandes et valeurs par défaut du mode d'hôte

Commande	Valeur par défaut	Description
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	Si cette option n'est pas définie, l'ASA utilise sAMAccountName pour les demandes LDAP. Que ce soit en utilisant SASL ou du texte brut, vous pouvez sécuriser les communications entre l'ASA et le serveur LDAP avec SSL. Enable SSL (Activer SSL) : nous vous conseillons fortement de sécuriser les communications LDAP avec SSL. Vous pouvez utiliser la commande de sous-mode **reference-identity** pour configurer le nom d'identité de référence que l'ASA utilisera pour valider l'identité du serveur LDAPS (SSL). Une fois configuré, l'ASA valide le serveur aaa-ldap avec les critères de correspondance configurés sous **crypto ca reference-identity** <*name*>. Si aucune correspondance n'a été trouvée dans le nom d'objet ou le SAN du certificat, ou si l'hôte spécifié par l'identité de référence ne se résout pas, la connexion est terminée.

Commande	Valeur par défaut	Description
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—
server-type	détection automatique	Si la détection automatique ne parvient pas à déterminer le type de serveur LDAP et que vous savez que le serveur est un serveur Microsoft, Sun ou LDAP générique, vous pouvez configurer manuellement le type de serveur.
ssl-client-certificate	—	Le certificat que l'ASA doit présenter au serveur LDAP en tant que certificat client. Ce certificat est nécessaire si vous configurez le serveur LDAP pour vérifier le certificat client. Vous devez également activer **ldap-over-ssl**. 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.
timeout	10secondes	—

Exemple

L'exemple suivant montre comment configurer un groupe de serveurs LDAP nommé watchdogs et ajouter un serveur LDAP au groupe. Comme l'exemple ne définit pas d'intervalle de nouvelle tentative ni le port d'écoute du serveur LDAP, l'ASA utilise les valeurs par défaut pour ces deux paramètres propres au serveur.

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

Configurer l'autorisation avec LDAP pour le VPN

Lorsque l'authentification de l'utilisateur LDAP pour l'accès VPN a réussi, l'ASA interroge le serveur LDAP, qui renvoie les attributs LDAP. Ces attributs comprennent généralement des données d'autorisation qui s'appliquent à la session VPN. L'utilisation de LDAP de cette manière permet d'effectuer l'authentification et l'autorisation en une seule étape.

Il peut arriver que vous ayez besoin de l'autorisation d'un serveur de répertoire LDAP distinct du mécanisme d'authentification. Par exemple, si vous utilisez un serveur SDI ou de certificat pour l'authentification, aucune information d'autorisation n'est renvoyée. Pour les autorisations d'utilisateur dans ce cas, vous pouvez interroger un répertoire LDAP après une authentification réussie, ce qui effectue l'authentification et l'autorisation en deux étapes.

Pour configurer l'autorisation d'utilisateur du VPN à l'aide de LDAP, procédez comme suit.

Procédure

Étape 1 Créez un groupe de tunnels d'accès à distance IPsec nommé remotegrp.

tunnel-group *groupname*

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp
```

Étape 2 Associez le groupe de serveurs et le groupe de tunnels.

tunnel-group *groupname* **general-attributes**

Exemple :

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

Étape 3 Affectez un nouveau groupe de tunnels à un groupe de serveurs AAA précédemment créé pour l'autorisation.

authorization-server-group *group-tag*

Exemple :

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

Exemple

Bien que d'autres commandes et options liées à l'autorisation soient disponibles pour des exigences spécifiques, l'exemple suivant montre les commandes pour activer l'autorisation de l'utilisateur avec LDAP. L'exemple crée ensuite un groupe de tunnels d'accès à distance IPsec nommé remote-1 et affecte ce nouveau groupe de tunnels au groupe de serveurs AAA ldap_dir_1 précédemment créé pour l'autorisation :

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

Après avoir terminé ce travail de configuration, vous pouvez configurer des paramètres d'autorisation LDAP supplémentaires tels que un mot de passe de répertoire, un point de départ pour la recherche dans un répertoire et la portée d'une recherche dans le répertoire en saisissant les commandes suivantes :

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

```
ciscoasa(config-aaa-server-host)#
```

Supervision des serveurs LDAP pour AAA

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

- **show aaa-server**

  Cette commande affiche les statistiques du serveur AAA configuré. Utilisez la commande **clear aaa-server statistics** pour effacer les statistiques du serveur AAA.

- **show running-config aaa-server**

  Cette commande montre la configuration en cours d'exécution du serveur AAA. Utilisez la commande **clear configure aaa-server** pour effacer la configuration du serveur AAA.

Historique des serveurs LDAP pour AAA

Tableau 3 : 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 commandes suivantes : **username**, **aaa authorization exec authentication-server**, **aaa authentication console LOCAL**, **aaa authorization exec LOCAL**, **service-type, ldap attribute-map**, **aaa-server protocol**, **aaa authentication telnet** | **ssh** | **serial**} **console LOCAL**, **aaa authentication http console LOCAL**, **aaa authentication enable console LOCAL**, **max-failed-attempts**, **reactivation-mode**, **accounting-mode simultaneous**, **aaa-server host**, **authorization-server-group**, **tunnel-group**, **tunnel-group general-attributes**, **map-name**, **map-value**, **ldap-attribute-map**.
Serveurs LDAP avec adresses IPv6 pour AAA	9.7(1)	Vous pouvez maintenant utiliser une adresse IPv4 ou IPv6 pour le serveur AAA.

Nom de la caractéristique	Versions de plateforme	Description
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 commandes suivantes pour accepter ces nouvelles limites : **aaa-server**, **aaa-server host**.
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 ajouté la commande suivante : **ssl-client-certificate**.

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.