Exemple de configuration de mappages d'attributs LDAP

Table des matières

Introduction

Ce document décrit comment n'importe quel attribut Microsoft/AD peut être mappé à un attribut Cisco.

Procédure

1. Sur le serveur Active Directory (AD)/LDAP (Lightweight Directory Access Protocol) :Sélectionnez **user1**.Cliquez avec le bouton droit sur **> Propriétés**.Choisissez un onglet à utiliser afin de définir un attribut (par exemple, onglet Général).Choisissez un champ/attribut, par exemple, le champ Office, à utiliser afin d'appliquer la plage de temps, et entrez le texte de la bannière (par exemple, Bienvenue dans LDAP !!!!). La configuration Office sur l'interface utilisateur graphique est stockée dans l'attribut AD/LDAP physicalDeliveryOfficeName.
2. Sur l'appareil de sécurité adaptatif (ASA), afin de créer une table de mappage d'attributs LDAP, mappez l'attribut AD/LDAP physicalDeliveryOfficeName à l'attribut ASA Banner1 :

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. Associez le mappage d'attribut LDAP à l'entrée aaa-server :

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. Établissez la session d'accès à distance et vérifiez que la bannière Bienvenue dans LDAP !!!! est présentée à l'utilisateur VPN.

Placer les utilisateurs LDAP dans une stratégie de groupe spécifique (exemple générique)

Cet exemple illustre l'authentification de user1 sur le serveur AD-LDAP et récupère la valeur du champ department afin qu'elle puisse être mappée à une stratégie de groupe ASA/PIX à partir de laquelle les stratégies peuvent être appliquées.

1. Sur le serveur AD/LDAP :Sélectionnez **user1**.Cliquez avec le bouton droit sur **> Propriétés**.Sélectionnez un onglet à utiliser pour définir un attribut (par exemple, l'onglet Organisation).Choisissez un champ/attribut, par exemple, Service, à utiliser afin d'appliquer une stratégie de groupe, et entrez la valeur de la stratégie de groupe (Stratégie de groupe1) sur l'ASA/PIX. La configuration du service sur l'interface utilisateur graphique est stockée dans le service d'attribut AD/LDAP.
2. Définissez une table ldap-attribute-map.

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. Définissez la stratégie de groupe, Group_policy1, sur l'appliance et les attributs de stratégie requis.
4. Établissez le tunnel d'accès à distance VPN et vérifiez que la session hérite des attributs de Group-Policy1 (et de tous les autres attributs applicables de la stratégie de groupe par défaut). **Remarque** : ajoutez d'autres attributs au mappage, si nécessaire. Cet exemple montre seulement le minimum pour contrôler cette fonction spécifique (placer un utilisateur dans une politique de groupe ASA/PIX 7.1.x spécifique). Le troisième exemple illustre ce type de carte.

Configurer une stratégie de groupe NOACCESS

Vous pouvez créer une stratégie de groupe NOACCESS afin de refuser la connexion VPN lorsque l'utilisateur ne fait partie d'aucun des groupes LDAP. Cet extrait de configuration est affiché à titre de référence :

```
group-policy NOACCESS internal
group-policy NOACCESS attributes
vpn-simultaneous-logins 0
vpn-tunnel-protocol IPSec webvpn
```

Vous devez appliquer cette stratégie de groupe en tant que stratégie de groupe par défaut au

groupe de tunnels. Ceci permet aux utilisateurs qui obtiennent un mappage à partir du mappage d'attributs LDAP, par exemple, ceux qui appartiennent à un groupe LDAP souhaité, d'obtenir leurs stratégies de groupe souhaitées, et aux utilisateurs qui n'obtiennent aucun mappage, par exemple, ceux qui n'appartiennent à aucun des groupes LDAP souhaités, d'obtenir NOACCESS group-policy à partir du groupe de tunnels, ce qui bloque l'accès pour eux.

> **Conseil** : puisque l'attribut vpn-simultané-logins est défini à 0 ici, il doit être explicitement défini dans toutes les autres politiques de groupe ; sinon, il peut être hérité de la politique de groupe par défaut pour ce groupe de tunnel, qui dans ce cas est la politique NOACCESS.

Application de stratégie d'attributs basés sur des groupes (exemple)

1. Sur le serveur AD-LDAP Utilisateurs et ordinateurs Active Directory, configurez un enregistrement utilisateur (VPNUserGroup) qui représente un groupe où les attributs VPN sont configurés.
2. Sur le serveur AD-LDAP, Utilisateurs et ordinateurs Active Directory, définissez le champ Service de chaque enregistrement d'utilisateur pour pointer vers l'enregistrement de groupe (VPNUserGroup) à l'étape 1. Dans cet exemple, le nom d'utilisateur est web1. **Remarque** : l'attribut AD du service a été utilisé uniquement parce que logiquement le service fait référence à la stratégie de groupe. En réalité, n'importe quel champ peut être utilisé. Ce champ doit obligatoirement correspondre à l'attribut VPN Cisco Group-Policy, comme indiqué dans cet exemple.
3. Définissez une table ldap-attribute-map :

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

   Les deux attributs AD-LDAP, Description et Office (représentés par les noms AD description et PhysicalDeliveryOfficeName) sont les attributs d'enregistrement de groupe (pour VPUNSerGroup) qui correspondent aux attributs VPN Cisco Banner1 et IETF-Radius-Session-Timeout.L'attribut department permet à l'enregistrement d'utilisateur d'être mappé au nom de la stratégie de groupe externe sur l'ASA (VPUNSer), qui est ensuite mappé à l'enregistrement VPNuserGroup sur le serveur AD-LDAP, où les attributs sont définis.**Remarque** : l'attribut Cisco (Group-Policy) doit être défini dans ldap-attribute-map. Son attribut AD mappé peut être n'importe quel attribut AD définissable. Cet exemple utilise department, car il s'agit du nom le plus logique qui fait référence à la stratégie de groupe.
4. Configurez le serveur aaa avec le nom ldap-attribute-map à utiliser pour les opérations AAA (Authentication, Authorization, and Accounting) LDAP :

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 10.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. Définissez un groupe de tunnels avec l'authentification LDAP ou l'autorisation LDAP. Exemple avec authentification LDAP. Exécute l'authentification + (autorisation) application de la stratégie d'attribut si des attributs sont définis.
```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
5520-1(config)#
```
Exemple avec autorisation LDAP. Configuration utilisée pour les certificats numériques.
```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```
6. Définissez une stratégie de groupe externe. Le nom de la stratégie de groupe est la valeur de l'enregistrement d'utilisateur AD-LDAP qui représente le groupe (VPNUserGroup).
```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```
7. Établissez le tunnel et vérifiez que les attributs sont appliqués. Dans ce cas, la bannière et le délai d'expiration de session sont appliqués à partir de l'enregistrement VPNuserGroup sur AD.

Application Active Directory de l'attribution d'une adresse IP statique pour les tunnels IPsec et SVC

L'attribut AD est msRADIUSFramedIPAddress. L'attribut est configuré dans Propriétés utilisateur Active Directory, onglet Appel entrant, Attribuer une adresse IP statique.

Voici les étapes à suivre :

1. Sur le serveur AD, sous Propriétés utilisateur, onglet Accès à distance, Attribuer une adresse IP statique, entrez la valeur de l'adresse IP afin de l'attribuer à la session IPsec/SVC (10.20.30.6).
2. Sur l'ASA, créez un mappage d'attribut ldap avec ce mappage :
```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```
3. Sur l'ASA, vérifiez que vpn-address-allocation est configuré pour inclure vpn-addr-assign-aaa :
```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```
4. Établissez les sessions IPsec/SVC Remote Authority (RA) et vérifiez dans show vpn-sessiondb remote|svc que le champ Assigned IP est correct (10.20.30.6).

Application Active Directory de « Accès à distance, accès entrant autorisé, accès

autorisé/refusé »

Prend en charge toutes les sessions d'accès à distance VPN : IPSec, WebVPN et SVC. Allow Access a la valeur TRUE. La valeur de Refuser l'accès est FALSE. Le nom de l'attribut AD est msNPAllowDialin.

Cet exemple illustre la création d'un ldap-attribute-map qui utilise les protocoles Cisco Tunneling-Protocols pour créer des conditions Allow Access (TRUE) et Deny (FALSE). Par exemple, si vous mappez le tunnel-protocol=L2TPover IPsec (8), vous pouvez créer une condition FALSE si vous essayez d'imposer l'accès pour WebVPN et IPsec. La logique inverse s'applique également.

Voici les étapes à suivre :

1. Dans Propriétés utilisateur1 du serveur AD, Compos., sélectionnez l'option Autoriser l'accès ou Refuser l'accès appropriée pour chaque utilisateur. **Remarque** : si vous choisissez la troisième option, Contrôler l'accès via la stratégie d'accès à distance, aucune valeur n'est retournée du serveur AD, de sorte que les autorisations qui sont appliquées sont basées sur le paramètre de stratégie de groupe interne de l'ASA/PIX.
2. Sur l'ASA, créez un ldap-attribute-map avec ce mappage :
   ```
   ldap attribute-map LDAP-MAP
   map-name msNPAllowDialin Tunneling-Protocols
   map-value msNPAllowDialin FALSE 8
   map-value msNPAllowDialin TRUE 20
   5540-1#
   ```
   Remarque : ajoutez d'autres attributs au mappage, si nécessaire. Cet exemple montre uniquement le minimum requis pour contrôler cette fonction spécifique (Autoriser ou Refuser l'accès en fonction du paramètre d'accès entrant).Que signifie ou applique la commande ldap-attribute-map ?map-value msNPAllowDialin FALSE 8Refuser l'accès à un utilisateur1. La condition de valeur FALSE correspond au protocole de tunnel L2TPoverIPsec (valeur 8).Autoriser l'accès pour l'utilisateur 2 . La condition de valeur TRUE correspond à tunnel-protocol WebVPN + IPsec, (valeur 20).Un utilisateur WebVPN/IPsec, authentifié en tant qu'utilisateur1 sur Active Directory, échouerait en raison d'une non-correspondance de protocole de tunnel.Un L2TPoverIPsec, authentifié en tant qu'utilisateur 1 sur AD, échouerait en raison de la règle Deny.Un utilisateur WebVPN/IPsec, authentifié en tant qu'utilisateur2 sur AD, réussirait (Autoriser la règle + le protocole de tunnel correspondant).Un L2TPoverIPsec, authentifié en tant qu'utilisateur 2 sur AD, échouerait en raison d'une non-correspondance de protocole de tunnel.
   Prise en charge du protocole de tunnel, tel que défini dans les documents RFC 2867 et 2868.

Application Active Directory de l'appartenance à un groupe ou à un membre pour autoriser ou refuser l'accès

Ce cas est étroitement lié au cas 5, et fournit un flux plus logique, et est la méthode recommandée, puisqu'il établit la vérification de l'appartenance à un groupe comme une condition.

1. Configurez l'utilisateur Active Directory en tant que membre d'un groupe spécifique. Utilisez un nom qui le place au sommet de la hiérarchie de groupes (ASA-VPN-Consultants). Dans AD-LDAP, l'appartenance à un groupe est définie par l'attribut AD memberOf. Il est important que le groupe soit en haut de la liste, car vous ne pouvez actuellement appliquer les règles

qu'à la première chaîne group/memberOf. Dans la version 7.3, vous pouvez effectuer le filtrage et l'application de groupes multiples.

2. Sur l'ASA, créez un ldap-attribute-map avec le mappage minimum :
```
ldap attribute-map LDAP-MAP
map-name memberOf Tunneling-Protocols
map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
5540-1#
```
Remarque : ajoutez d'autres attributs au mappage, si nécessaire. Cet exemple montre uniquement le minimum requis pour contrôler cette fonction spécifique (autoriser ou refuser l'accès en fonction de l'appartenance au groupe).Que signifie ou applique la commande ldap-attribute-map ?User=joe_consultant, qui fait partie d'AD et qui est membre du groupe AD. ASA-VPN-Consultants ne peut être autorisé à accéder qu'à condition que l'utilisateur utilise IPsec (tunnel-protocol=4=IPSec).User=joe_consultant, faisant partie d'Active Directory, peut bloquer l'accès VPN pendant tout autre client d'accès à distance (PPTP/L2TP, L2TP/IPSec, WebVPN/SVC, etc.).User=bill_the_hacker ne peut PAS être autorisé à entrer car l'utilisateur n'est pas membre AD.

Application Active Directory des « règles d'heures de connexion/d'heure du jour »

Cet exemple d'utilisation décrit comment configurer et appliquer les règles d'heure sur AD/LDAP.

Voici la procédure à suivre pour ce faire :

1. Sur le serveur AD/LDAP :Sélectionnez l'utilisateur.Cliquez avec le bouton droit sur **> Propriétés**.Choisissez un onglet à utiliser afin de définir un attribut (par exemple, onglet Général).Choisissez un champ/attribut, par exemple, le champ Office, à utiliser afin d'appliquer la plage horaire, et entrez le nom de la plage horaire (par exemple, Boston). La configuration Office sur l'interface utilisateur graphique est stockée dans l'attribut AD/LDAP physicalDeliveryOfficeName.
2. Sur l'ASA Créez une table de mappage d'attributs LDAP.Mappez l'attribut AD/LDAP « physicalDeliveryOfficeName » à l'attribut ASA « Access-Hours ».Exemple :
```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```
3. Sur l'ASA, associez le mappage d'attribut LDAP à l'entrée aaa-server :
```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```
4. Sur l'ASA, créez un objet de plage de temps dont la valeur de nom est attribuée à l'utilisateur (valeur Office à l'étape 1) :
```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```
5. Établissez la session d'accès à distance VPN : La session peut aboutir si elle se situe dans la plage de temps.La session peut échouer si elle se trouve en dehors de la plage de temps.

Utilisez la configuration ldap-map pour mapper un utilisateur dans une stratégie de groupe spécifique et utilisez la commande authorization-server-group dans le cas d'une double authentification

1. Dans ce scénario, une double authentification est utilisée. Le premier serveur d'authentification utilisé est RADIUS et le second serveur d'authentification est un serveur LDAP. Configurez le serveur LDAP ainsi que le serveur RADIUS. Voici un exemple :

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

   Définissez le mappage d'attributs LDAP. Voici un exemple :

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

   Définissez le groupe de tunnels et associez les serveurs RADIUS et LDAP pour l'authentification. Voici un exemple :

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

   Affichez la stratégie de groupe utilisée dans la configuration du groupe de tunnels :

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

   Avec cette configuration, les utilisateurs AnyConnect correctement mappés avec l'utilisation d'attributs LDAP n'étaient pas placés dans la stratégie de groupe Test-Policy-Safenet. Au lieu de cela, ils étaient toujours placés dans la stratégie de groupe par défaut, en l'occurrence NoAccess.Reportez-vous à l'extrait des débogages (debug ldap 255) et aux syslogs au niveau informatif :

```
----------------------------------------------------------------------------
```

```
memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

--------------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123

%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

Ces syslogs affichent un échec car l'utilisateur a reçu la stratégie de groupe NoAccess dont la connexion simultanée a été définie sur 0, même si les syslogs disent qu'il a récupéré une stratégie de groupe spécifique à l'utilisateur.Pour que l'utilisateur soit assigné dans la stratégie de groupe, basée sur le mappage LDAP, vous devez avoir cette commande : **authorization-server-group test-ldap** (dans ce cas, **test-ldap** est le nom du serveur LDAP). Voici un exemple :

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. Maintenant, si le premier serveur d'authentification (RADIUS, dans cet exemple) a envoyé les attributs spécifiques à l'utilisateur, par exemple, l'attribut IEFT-class, dans ce cas, l'utilisateur peut être mappé à la stratégie de groupe envoyée par RADIUS. Ainsi, même si le serveur secondaire dispose d'une carte LDAP configurée et que les attributs LDAP de l'utilisateur mappent l'utilisateur à une stratégie de groupe différente, la stratégie de groupe envoyée par le premier serveur d'authentification peut être appliquée. Pour que l'utilisateur soit placé dans une stratégie de groupe basée sur l'attribut de mappage LDAP, vous devez spécifier cette commande sous le tunnel-group : **authorization-server-group test-ldap**.
3. Si le premier serveur d'authentification est SDI ou OTP, qui ne peut pas passer l'attribut spécifique à l'utilisateur, alors l'utilisateur tomberait dans la stratégie de groupe par défaut du groupe de tunnels. Dans ce cas, NoAccess même si le mappage LDAP est correct. Dans ce cas, vous avez également besoin de la commande, **authorization-server-group test-ldap**, sous le tunnel-group pour que l'utilisateur soit placé dans la stratégie de groupe correcte.
4. Si les deux serveurs sont les mêmes serveurs RADIUS ou LDAP, alors vous n'avez pas besoin de la commande **authorization-server-group** pour que le verrouillage de stratégie de

groupe fonctionne.

Vérifier

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Dépannage

Utilisez cette section pour dépanner votre configuration.

Déboguer la transaction LDAP

Ces débogages peuvent être utilisés afin d'aider à isoler les problèmes avec la configuration DAP :

- debug ldap 255
- debug dap trace
- debug aaa authentication

ASA ne peut pas authentifier les utilisateurs à partir du serveur LDAP

Si l'ASA n'est pas en mesure d'authentifier les utilisateurs à partir du serveur LDAP, voici quelques exemples de débogages :

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context
0xcd66c028, reqType = 1[1555805]
Fiber started[1555805] Creating LDAP context with uri=ldaps://172.30.74.70:636
[1555805] Connect to LDAP server:
ldaps://172.30.74.70:636, status = Successful[1555805] supportedLDAPVersion:
value = 3[1555805]
supportedLDAPVersion: value = 2[1555805] Binding as administrator[1555805]
Performing Simple
authentication for sysservices to 172.30.74.70[1555805] Simple authentication
for sysservices returned code (49)
Invalid credentials[1555805] Failed to bind as administrator returned code
(-1) Can't contact LDAP server[1555805]
Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

Àpartir de ces débogages, soit le format DN de connexion LDAP est incorrect, soit le mot de

passe est incorrect. Vérifiez donc les deux afin de résoudre le problème.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.