Exemple de configuration de LDAP sur des périphériques IOS utilisant des mappages d'attributs dynamiques

Contenu

Introduction

Ce document décrit comment utiliser l'authentification LDAP (Lightweight Directory Access Protocol) sur les têtes de réseau Cisco IOS® et modifier le nom distinctif relatif (RDN) par défaut de Common Name (CN) à sAMAccountName.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur un périphérique Cisco IOS qui exécute le logiciel Cisco IOS Version 15.0 ou ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Problème principal

La plupart des utilisateurs de Microsoft Active Directory (AD) avec LDAP définissent généralement leur RDN comme sAMAccountName. Si vous utilisez le proxy d'authentification (auth-proxy) et un dispositif de sécurité adaptatif (ASA) comme tête de réseau pour vos clients VPN, ceci est facilement réparable si vous définissez le type de serveur AD lorsque vous définissez le serveur AAA ou si vous entrez la commande ldap-naming-attribute. Cependant, dans le logiciel Cisco IOS, aucune de ces options n'est disponible. Par défaut, le logiciel Cisco IOS utilise la valeur d'attribut CN dans AD pour l'authentification des noms d'utilisateur. Par exemple, un utilisateur est créé dans AD en tant que *John Fernandes*, mais son ID utilisateur est stocké en tant que *jfern*. Par défaut, le logiciel Cisco IOS vérifie la valeur CN. Autrement dit, le logiciel vérifie l'authentification par nom d'utilisateur *John Fernandes* et non la valeur sAMAccountName de *jfern* pour l'authentification. Afin de forcer le logiciel Cisco IOS à vérifier le nom d'utilisateur à partir de la valeur d'attribut sAMAccountName, utilisez des mappages d'attributs dynamiques comme indiqué dans ce document.

Solution

Bien que les périphériques Cisco IOS ne prennent pas en charge ces méthodes de modification RDN, vous pouvez utiliser des mappages d'attributs dynamiques dans le logiciel Cisco IOS afin d'obtenir un résultat similaire. Si vous entrez la commande **show ldap attribute** sur la tête de réseau Cisco IOS, vous verrez ce résultat :

Attribut LDAP	Format	Attribut AAA
airespaceBwDataBurstContract	Longue	bsn-data-bandwidth-burst-contrt
userPassword	Chaîne (string)	mot de passe
airespaceBwRealBurstContract	Longue	bsn-realtime-bandwidth-burst-c
TypeEmployé	Chaîne (string)	type d'employé
airespaceServiceType	Longue	service-type
nomACLairespace	Chaîne (strin	bsn-acl-name

	g)	
priv-lvl	Longue	priv-lvl
membreDe	DN de chaîne	groupe de demandeurs
cn	**Chaîne (string)**	**username (nom d'utilisateur)**
airespaceDSCP	Longue	bsn-dscp
policyTag	Chaîne (string)	tag-name
airespaceQOSLevel	Longue	bsn-qos-level
airespace8021PType	Longue	type bsn-8021p
airespaceBwRealAveContract	Longue	bsn-realtime-bandwidth-moyenne
airespaceNomInterfaceVlan	Chaîne (string)	bsn-vlan-interface-name
airespaceVapId	Longue	bsn-wlan-id
airespaceBwDataAveContract	Longue	bsn-data-bandwidth-moyenne-con
sAMAccountName	Chaîne (string)	sam-account-name
infosContactRéunion	Chaîne (string)	coordonnées-info
NuméroTéléphone	Chaîne (string)	numéro de téléphone

Comme vous pouvez le voir dans l'attribut mis en surbrillance, le périphérique d'accès au réseau (NAD) Cisco IOS utilise cette carte d'attribut pour les demandes d'authentification et les réponses. En gros, une carte dynamique des attributs LDAP dans le périphérique Cisco IOS fonctionne de manière bidirectionnelle. En d'autres termes, les attributs sont mappés non seulement lorsqu'une réponse est reçue, mais également lorsque des requêtes LDAP sont envoyées. Sans mappages

d'attributs définis par l'utilisateur, configuration LDAP de base sur la NAD, vous voyez ce message de journal lorsque la demande est envoyée :

```
*Jul 24 11:04:50.568: LDAP: Check the default map for aaa type=username
*Jul 24 11:04:50.568: LDAP: Ldap Search Req sent
ld 1054176200
base dn DC=csco,DC=com
scope 2
filter (&(objectclass=*)(cn=xyz))ldap_req_encode
put_filter "(&(objectclass=person)(cn=xyz))"
put_filter: AND
put_filter_list "(objectclass=person)(cn=xyz)"
put_filter "(objectclass=person)"
put_filter: simple
put_filter "(cn=xyz)"
put_filter: simple
Doing socket write
*Jul 24 11:04:50.568: LDAP: LDAP search request sent successfully (reqid:13)
```

Afin de modifier ce comportement et de le forcer à utiliser l'attribut sAMAccountName pour la vérification du nom d'utilisateur, entrez la commande **ldap attribute map username** pour créer d'abord cette carte d'attribut dynamique :

```
ldap attribute map username
   map type sAMAccountName username
```

Une fois cette carte d'attribut définie, entrez la commande *attribute map <dynamic-attribute-map-name> pour mapper cette carte d'attribut au groupe de serveurs AAA sélectionné (aaa-server).*

Remarque : Afin de faciliter tout ce processus, l'ID de bogue Cisco CSCtr45874 (clients enregistrés uniquement) a été enregistré. Si cette demande d'amélioration est implémentée, elle permettra aux utilisateurs d'identifier le type de serveur LDAP utilisé et de modifier automatiquement certaines de ces cartes par défaut pour refléter les valeurs utilisées par ce serveur particulier.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Exemple de configuration

Ce document utilise les configurations suivantes :

- Entrez cette commande afin de définir la carte d'attribut dynamique :

```
ldap attribute map

   map type sAMAccountName username
```

- Entrez cette commande afin de définir le groupe de serveurs AAA :

```
aaa group server ldap

   server
```

- Entrez cette commande afin de définir le serveur :

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Entrez cette commande afin de définir la liste des méthodes d'authentification à utiliser :

```
aaa authentication login group
```

Outils AD

Afin de vérifier le DN absolu d'un utilisateur, entrez l'une des commandes suivantes à partir de l'invite de commandes AD :

```
dsquery user -name user1
```

OU

```
dsquery user -samid user1
```

Note : « user1 » mentionné ci-dessus est dans une chaîne regex. Vous pouvez également inscrire tous les DN du nom d'utilisateur en commençant par user en utilisant la chaîne regex comme « user*« .

Afin d'inscrire tous les attributs d'un seul utilisateur, entrez cette commande à partir de l'invite de commandes AD :

```
dsquery * -filter "(&(objectCategory=Person)(sAMAccountName=username))" -attr *
```

Problèmes potentiels

Dans un déploiement LDAP, l'opération de recherche est effectuée en premier et l'opération de

liaison est effectuée ultérieurement. Cette opération est effectuée car, si l'attribut de mot de passe est retourné dans le cadre de l'opération de recherche, la vérification du mot de passe peut être effectuée localement sur le client LDAP et il n'est pas nécessaire d'effectuer une opération de liaison supplémentaire. Si l'attribut de mot de passe n'est pas retourné, une opération de liaison peut être effectuée ultérieurement. Un autre avantage lorsque vous effectuez l'opération de recherche en premier et l'opération de liaison plus tard est que le DN reçu dans le résultat de la recherche peut être utilisé comme DN utilisateur au lieu de la formation d'un DN lorsque le nom d'utilisateur (valeur CN) est préfixé avec un DN de base.

Il peut y avoir des problèmes lorsque la commande **authentication bind-first** est utilisée avec un attribut défini par l'utilisateur qui change où pointe la carte d'attribut username. Par exemple, si vous utilisez cette configuration, il est probable que votre tentative d'authentification échoue :

```
ldap server ss-ldap
ipv4 192.168.1.3
attribute map ad-map
transport port 3268
bind authenticate root-dn CN=abcd,OU=Employees,OU=qwrt Users,DC=qwrt,DC=com
   password blabla
base-dn DC=qwrt,DC=com
authentication bind-first
ldap attribute-map ad-map
 map type sAMAccountName username
```

Par conséquent, vous verrez le message d'erreur `Invalid, Result code =49`. Les messages du journal seront similaires à ceux-ci :

```
Oct  4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processing
Oct  4 13:03:08.503: LDAP: Received queue event, new AAA request
Oct  4 13:03:08.503: LDAP: LDAP authentication request
Oct  4 13:03:08.503: LDAP: Attempting first  next available LDAP server
Oct  4 13:03:08.503: LDAP: Got next LDAP server :ss-ldap
Oct  4 13:03:08.503: LDAP: First Task: Send bind req
Oct  4 13:03:08.503: LDAP: Authentication policy: bind-first
Oct  4 13:03:08.503: LDAP: Dynamic map configured
Oct  4 13:03:08.503: LDAP: Dynamic map found for aaa type=username
Oct  4 13:03:08.503: LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=com
ldap_req_encode
Doing socket write
Oct  4 13:03:08.503: LDAP:  LDAP bind request sent successfully (reqid=36)
Oct  4 13:03:08.503: LDAP: Sent the LDAP request to server
Oct  4 13:03:08.951: LDAP: Received socket event
Oct  4 13:03:08.951: LDAP: Checking the conn status
Oct  4 13:03:08.951: LDAP: Socket read event socket=0
Oct  4 13:03:08.951: LDAP: Found socket ctx
Oct  4 13:03:08.951: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct  4 13:03:08.951: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read = 109
ldap_match_request succeeded for msgid 36 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct  4 13:03:08.951: LDAP:LDAP Messages to be processed: 1
Oct  4 13:03:08.951: LDAP: LDAP Message type: 97
```

```
Oct  4 13:03:08.951: LDAP: Got ldap transaction context from reqid
   36ldap_parse_result
Oct  4 13:03:08.951: LDAP: resultCode:    49     (Invalid credentials)
Oct  4 13:03:08.951: LDAP: Received Bind Responseldap_parse_result
   ldap_err2string
Oct  4 13:03:08.951: LDAP: Ldap Result Msg: FAILED:Invalid credentials,
   Result code =49
Oct  4 13:03:08.951: LDAP: LDAP Bind operation result : failed
Oct  4 13:03:08.951: LDAP: Restoring root bind status of the connection
Oct  4 13:03:08.951: LDAP: Performing Root-Dn bind operationldap_req_encode
Doing socket write
Oct  4 13:03:08.951: LDAP: Root Bind on CN=abcd,DC=qwrt,DC=com
initiated.ldap_msgfree
Oct  4 13:03:08.951: LDAP: Closing transaction and reporting error to AAA
Oct  4 13:03:08.951: LDAP: Transaction context removed from list [ldap reqid=36]
Oct  4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILED
Oct  4 13:03:08.951: LDAP: Received socket event
Oct  4 13:03:09.491: LDAP: Received socket event
Oct  4 13:03:09.491: LDAP: Checking the conn status
Oct  4 13:03:09.491: LDAP: Socket read event socket=0
Oct  4 13:03:09.491: LDAP: Found socket ctx
Oct  4 13:03:09.495: LDAP: Receive event: read=1, errno=9 (Bad file number)
Oct  4 13:03:09.495: LDAP: Passing the client ctx=314BA6ECldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_read_activity lc 0x296EA104
Doing socket read
LDAP-TCP:Bytes read= 22
ldap_match_request succeeded for msgid 37 h 0
changing lr 0x300519E0 to COMPLETE as no continuations
removing request 0x300519E0 from list as lm 0x296C5170 all 0
ldap_msgfree
ldap_msgfree
Oct  4 13:03:09.495: LDAP: LDAP Messages to be processed: 1
Oct  4 13:03:09.495: LDAP: LDAP Message type: 97
Oct  4 13:03:09.495: LDAP: Got ldap transaction context from reqid
   37ldap_parse_result
Oct  4 13:03:09.495: LDAP: resultCode:    0     (Success)P: Received Bind
   Response
Oct  4 13:03:09.495: LDAP: Received Root Bind Response ldap_parse_result
Oct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0
Oct  4 13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=com
Oct  4 13:03:09.495: LDAP: Transaction context removed from list [ldap reqid=37]
ldap_msgfree
ldap_result
wait4msg (timeout 0 sec, 1 usec)
ldap_select_fd_wait (select)
ldap_err2string
Oct  4 13:03:09.495: LDAP: Finished processing ldap msg, Result:Success
Oct  4 13:03:09.495: LDAP: Received socket event
```

Les lignes en surbrillance indiquent ce qui ne va pas avec la liaison initiale avant l'authentification. Cela fonctionnera correctement si vous supprimez la commande **authentication bind-first** de la configuration ci-dessus.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show ldap attributs**
- **show ldap server all**

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug ldap all**
- **debug ldap event**
- **debug aaa authentication**
- **debug aaa authorization**

Informations connexes

- Guide de configuration LDAP AAA Cisco IOS version 15.1MT
- ASA 8.0 : Configurer l'authentification LDAP pour les utilisateurs WebVPN
- Support et documentation techniques - Cisco Systems