Contenu

Introduction

Ce document décrit comment utiliser l'authentification de Protocole LDAP (Lightweight Directory Access Protocol) sur des headends de Cisco IOS® et changer le nom unique relatif par défaut (RDN) du nom commun (NC) au sAMAccountName.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur un périphérique de Cisco IOS qui exécute la version du logiciel Cisco IOS 15.0 ou plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Principale question

La plupart de Microsoft Active Directory (AD) avec des utilisateurs de LDAP définissent typiquement leur RDN pour être le sAMAccountName. Si vous utilisez le Seveur mandataire d'authentification (proxy d'authentification) et une appliance de sécurité adaptable (ASA) comme headend pour vos clients vpn, ceci est facilement réparé si vous définissez le type de serveur d'AD quand vous définissez le serveur d'AAA ou si vous sélectionnez la commande de LDAP-nommer-attribut. Cependant, en logiciel de Cisco IOS, ni l'un ni l'autre de ces options n'est disponible. Par défaut, le logiciel de Cisco IOS utilise la valeur d'attribut NC dans l'AD pour l'authentification de nom d'utilisateur. Par exemple, un utilisateur est créé dans l'AD comme *John Fernandes*, mais son user-id est enregistré comme *jfern*. Par défaut, le logiciel de Cisco IOS vérifie la valeur NC. C'est-à-dire, le logiciel vérifie *John Fernandes* pour l'authentification de nom d'utilisateur et pas la valeur de sAMAccountName de *jfern* pour l'authentification. Afin de forcer le logiciel de Cisco IOS pour vérifier le nom d'utilisateur de la valeur d'attribut de sAMAccountName, utilisez les cartes dynamiques d'attribut comme détaillé dans ce document.

Solution

Bien que les périphériques de Cisco IOS ne prennent en charge pas ces méthodes de modification RDN, vous pouvez employer les cartes dynamiques d'attribut en logiciel de Cisco IOS afin de réaliser un résultat similaire. Si vous sélectionnez la commande d'**attribut de show ldap** sur le headend de Cisco IOS, vous verrez cette sortie :

Attribut de LDAP	**Format**	**Aaa attribute**
airespaceBwDataBurstContract	Ulong	donnée-bande passante-rafale-contr de bsn-
userPassword	Chaîne	mot de passe
airespaceBwRealBurstContract	Ulong	bsn-en temps réel-bande passante-rafale-C
employeeType	Chaîne	employé-type
airespaceServiceType	Ulong	type de service
airespaceACLName	Chaîne	bsn-acl-nom
priv-LVL	Ulong	priv-LVL
memberOf	DN de chaîne	suppliant-groupe
NC	**Chaîne**	**nom d'utilisateur**

airespaceDSCP	Ulong	bsn-dscp
policyTag	Chaîne	balise-nom
airespaceQOSLevel	Ulong	niveau bsn qos
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-en temps réel-bande passante-moyen
airespaceVlanInterfaceName	Chaîne	bsn-VLAN-interface-nom
airespaceVapId	Ulong	bsn-WLAN-id
airespaceBwDataAveContract	Ulong	bsn-donnée-bande passante-moyen-escroquerie
sAMAccountName	Chaîne	Sam-compte-nom
meetingContactInfo	Chaîne	contact-information
telephoneNumber	Chaîne	téléphone-nombre

Comme vous pouvez voir de l'attribut mis en valeur, le périphérique d'Access de réseau Cisco IOS (NAD) utilise cette carte d'attribut pour des demandes d'authentification et pour des réponses. Fondamentalement, une carte dynamique d'attribut de LDAP dans le périphérique de Cisco IOS fonctionne bidirectionnel. En d'autres termes, des attributs sont tracés non seulement quand une réponse est reçue, mais également quand des demandes de LDAP sont envoyées. Sans aucune carte définie par l'utilisateur d'attribut, une configuration de base de LDAP sur le NAD, vous voyez ce message de log quand la demande est envoyée :

Afin de changer ce comportement et le forcer pour utiliser l'attribut de sAMAccountName pour la vérification de nom d'utilisateur, sélectionnez la commande de **nom d'utilisateur de carte d'attribut de LDAP** de créer cette carte dynamique d'attribut d'abord :

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

Une fois que cette carte d'attribut a été définie, sélectionnez la commande de <dynamic-attribute-map-name> de **carte d'attribut** de tracer cette carte d'attribut au Groupe de serveurs AAA sélectionné (AAA-serveur).

Remarque: Afin de faciliter ce processus complet, l'ID de bogue Cisco CSCtr45874 (clients enregistrés seulement) a été classé. Si cette demande d'amélioration est mise en application, elle permettra aux utilisateurs d'identifier ce qu'un peu le serveur LDAP est utilisé et de changer automatiquement certaines de ces cartes par défaut pour refléter les valeurs utilisées par ce serveur particulier.

Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Exemple de configuration

Ce document utilise les configurations suivantes :

- Sélectionnez cette commande afin de définir la carte dynamique d'attribut :**ldap attribute map** <dynamic-attribute-map-name> **map type sAMAccountName username**
- Sélectionnez cette commande afin de définir le Groupe de serveurs AAA :**aaa group server ldap** <server-group-name> **server** <server-name>
- Sélectionnez cette commande afin de définir le serveur :**ldap server** <server-name> **ipv4** <host-address> **attribute map** <dynamic-attribute-map-name> **bind authentication root-dn** <complete-dn-root-user> **password** <root-user-pwd> **base-dn** <complete-dn-search-base>
- Sélectionnez cette commande afin de définir la liste de méthodes d'authentification pour l'utiliser :**aaa authentication login** <name> **group** <server-group-name>

Outils d'AD

Afin de vérifier le nom absolu de Distinguised (DN) d'un utilisateur, sélectionnez une de ces commandes de l'invite de commande d'AD :

```
dsquery user -name user1
```

OU

```
dsquery user -samid user1
```

Remarque: "user1" mentionné ci-dessus est dans la chaîne d'expression régulière. Vous pouvez également enrôler tous les dn du nom d'utilisateur commençant par l'utilisateur à l'aide de la chaîne d'expression régulière en tant que « user* ».

Afin d'enrôler tous les attributs d'un seul utilisateur, sélectionnez cette commande de l'invite de commande d'AD :

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

Problèmes potentiels

Dans un déploiement de LDAP, l'exécution de recherche est exécutée d'abord, et l'exécution de grippage est exécutée plus tard. Cette exécution est exécutée parce que, si l'attribut de mot de passe est retourné en tant qu'élément de l'exécution de recherche, la vérification de mot de passe peut être faite localement sur le client de LDAP et il n'y a aucun besoin d'exécution supplémentaire de grippage. Si l'attribut de mot de passe n'est pas retourné, une exécution de grippage peut être exécutée plus tard. Un autre avantage quand vous exécutez l'exécution de recherche d'abord et l'exécution de grippage est plus tard que le DN reçu dans le résultat de la recherche peut être utilisé comme DN d'utilisateur au lieu de la formation d'un DN quand le nom d'utilisateur (valeur NC) est préfixé avec un DN de base.

Il pourrait y avoir des questions quand la grippage-**première** commande d'**authentification** est utilisée avec un attribut défini par l'utilisateur qui change où la carte d'attribut de nom d'utilisateur se dirige. Par exemple, si vous utilisez cette configuration, vous êtes susceptible de voir une panne dans votre tentative d'authentification :

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

En conséquence, vous verrez les `qualifications non valides,` message d'erreur du `code =49 de résultat`. Les messages de log sembleront semblables à ces derniers :

```
Oct  4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processingOct  4 13:03:08.503: LDAP:
Received queue event, new AAA requestOct  4 13:03:08.503: LDAP: LDAP authentication requestOct
4 13:03:08.503: LDAP: Attempting first  next available LDAP serverOct  4 13:03:08.503: LDAP: Got
next LDAP server :ss-ldapOct  4 13:03:08.503: LDAP: First Task: Send bind req
Oct  4 13:03:08.503: LDAP: Authentication policy: bind-firstOct  4 13:03:08.503: LDAP: Dynamic map
configuredOct  4 13:03:08.503: LDAP: Dynamic map found for aaa type=usernameOct  4 13:03:08.503:
LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=comldap_req_encodeDoing socket writeOct  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 serverOct  4 13:03:08.951: LDAP: Received socket eventOct  4
13:03:08.951: LDAP: Checking the conn statusOct  4 13:03:08.951: LDAP: Socket read event
socket=0Oct  4 13:03:08.951: LDAP: Found socket ctxOct  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_resultwait4msg (timeout 0 sec, 1 usec)ldap_select_fd_wait
(select)ldap_read_activity lc 0x296EA104Doing socket readLDAP-TCP:Bytes read =
109ldap_match_request succeeded for msgid 36 h 0changing lr 0x300519E0 to COMPLETE as no
continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:08.951: LDAP:LDAP Messages to be processed: 1Oct  4
13:03:08.951: LDAP: LDAP Message type: 97Oct  4 13:03:08.951: LDAP: Got ldap transaction context
from reqid    36ldap_parse_resultOct  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 connectionOct  4 13:03:08.951: LDAP: Performing Root-Dn bind
operationldap_req_encodeDoing socket writeOct  4 13:03:08.951: LDAP: Root Bind on
CN=abcd,DC=qwrt,DC=cominitiated.ldap_msgfreeOct  4 13:03:08.951: LDAP: Closing transaction and
reporting error to AAAOct  4 13:03:08.951: LDAP: Transaction context removed from list [ldap
reqid=36]Oct  4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILEDOct  4 13:03:08.951: LDAP:
Received socket eventOct  4 13:03:09.491: LDAP: Received socket eventOct  4 13:03:09.491: LDAP:
Checking the conn statusOct  4 13:03:09.491: LDAP: Socket read event socket=0Oct  4
13:03:09.491: LDAP: Found socket ctxOct  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_resultwait4msg
(timeout 0 sec, 1 usec)ldap_select_fd_wait (select)ldap_read_activity lc 0x296EA104Doing socket
readLDAP-TCP:Bytes read= 22ldap_match_request succeeded for msgid 37 h 0changing lr 0x300519E0
to COMPLETE as no continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:09.495: LDAP: LDAP Messages to be processed: 1Oct  4
13:03:09.495: LDAP: LDAP Message type: 97Oct  4 13:03:09.495: LDAP: Got ldap transaction context
from reqid    37ldap_parse_resultOct  4 13:03:09.495: LDAP: resultCode:    0     (Success)P:
Received Bind    ResponseOct  4 13:03:09.495: LDAP: Received Root Bind Response
ldap_parse_resultOct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0Oct  4
13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=comOct  4 13:03:09.495: LDAP:
Transaction context removed from list [ldap reqid=37]ldap_msgfreeldap_resultwait4msg (timeout 0
sec, 1 usec)ldap_select_fd_wait (select)ldap_err2stringOct  4 13:03:09.495: LDAP: Finished
processing ldap msg, Result:SuccessOct  4 13:03:09.495: LDAP: Received socket event
```

Les lignes mises en surbrillance indiquent ce qui est erroné avec le grippage initial avant l'authentification. Cela fonctionnera correctement si vous retirez la grippage-**première** commande d'**authentification de la** configuration ci-dessus.

Vérifiez

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** .

- **attributs de show ldap**
- **serveur tout de show ldap**

Dépannez

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: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **mettez au point le LDAP tout**
- **mettez au point l'événement de LDAP**
- **debug aaa authentication**
- **debug aaa authorization**

Informations connexes

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