Contenido

Introducción

Este documento describe cómo utilizar la autenticación del Lightweight Directory Access Protocol (LDAP) en los headends del ® del Cisco IOS y cambiar el nombre distintivo relativo predeterminado (RDN) del Common Name (CN) al sAMAccountName.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un dispositivo Cisco IOS que funcione con el Cisco IOS Software Release 15.0 o Posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Cuestión central

La mayoría del Microsoft Active Directory (AD) con los usuarios LDAP define típicamente su RDN para ser el sAMAccountName. Si usted utiliza el Proxy de autenticación (auténtico-proxy) y un dispositivo de seguridad adaptante (ASA) como headend para sus clientes VPN, esto se repara fácilmente si usted define el tipo de servidor AD cuando usted define al servidor de AAA o si usted ingresa el comando del ldap-nombrar-atributo. Sin embargo, en el Cisco IOS Software, ningunas de estas opciones están disponibles. Por abandono, el Cisco IOS Software utiliza el valor de atributo CN en el AD para la autenticación del nombre de usuario. Por ejemplo, crean a un usuario en el AD como *Juan Fernandes*, pero su identificación del usuario se salva como *jfern*. Por abandono, el Cisco IOS Software marca el valor CN. Es decir, el software marca a *Juan Fernandes* para la autenticación del nombre de usuario y no el valor del sAMAccountName de *jfern* para la autenticación. Para forzar el Cisco IOS Software a marcar el nombre de usuario del valor de atributo del sAMAccountName, utilice las correspondencias dinámicas del atributo como se detalla en este documento.

Solución

Aunque los dispositivos Cisco IOS no soporten estos métodos de modificación RDN, usted puede utilizar las correspondencias dinámicas del atributo en el Cisco IOS Software para alcanzar un resultado similar. Si usted ingresa el comando del **atributo del ldap de la demostración** en el headend del Cisco IOS, usted verá esta salida:

Atributo LDAP	**Formato**	**Atributo AAA**
airespaceBwDataBurstContract	Ulong	DATA-ancho de banda-explosión-contr del bsn-
userPassword	String (cadena)	contraseña
airespaceBwRealBurstContract	Ulong	bsn-en tiempo real-ancho de banda-explosión-C
employeeType	String (cadena)	empleado-tipo
airespaceServiceType	Ulong	tipo de servicio
airespaceACLName	String (cadena)	bsn-ACL-nombre
priv-LVL	Ulong	priv-LVL
memberOf	Cadena DN	supplicant-grupo
cn	**String (cadena)**	**nombre de usuario**

airespaceDSCP	Ulong	bsn-DSCP
policyTag	String (cadena)	etiqueta-nombre
airespaceQOSLevel	Ulong	bsn-qos-nivel
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-en tiempo real-ancho de banda-medio
airespaceVlanInterfaceName	String (cadena)	bsn-VLAN-interfaz-nombre
airespaceVapId	Ulong	bsn-WLAN-identificación
airespaceBwDataAveContract	Ulong	bsn-DATA-ancho de banda-medio-estafa
sAMAccountName	String (cadena)	SAM-cuenta-nombre
meetingContactInfo	String (cadena)	contacto-Info
telephoneNumber	String (cadena)	número de teléfono

Como usted puede ver del atributo resaltado, el dispositivo de acceso del Cisco IOS Network (NAD) utiliza esta correspondencia del atributo para los pedidos de autenticación y para las respuestas. Básicamente, una correspondencia dinámica del atributo LDAP en el dispositivo Cisco IOS funciona bidireccional. Es decir los atributos se asocian no sólo cuando se recibe una respuesta, pero también cuando se envían las peticiones LDAP. Sin ningunas correspondencias definidas por el usario del atributo, una Configuración LDAP básica en el NAD, usted ve este mensaje del registro cuando se envía la petición:

Para cambiar este comportamiento y forzarlo para utilizar el atributo del sAMAccountName para la verificación del nombre de usuario, ingrese el **comando username de la correspondencia del atributo del ldap** de crear esta correspondencia dinámica del atributo primero:

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

Una vez que se ha definido esta correspondencia del atributo, ingrese el comando del <dynamic-attribute-map-name> de la **correspondencia del atributo** de asociar esta correspondencia del atributo al Grupo de servidores AAA seleccionado (AAA-servidor).

Nota: Para hacer este todo el proceso más fácil, se ha clasifiado el Id. de bug Cisco CSCtr45874 (clientes registrados solamente). Si se implementa este pedido de mejora, permitirá que los usuarios identifiquen están utilizando a qué clase de servidor LDAP y que cambien automáticamente algunas de estas correspondencias predeterminadas para reflejar los valores usados por ese servidor determinado.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuración de muestra:

En este documento, se utilizan estas configuraciones:

- Ingrese este comando para definir la correspondencia dinámica del atributo:**ldap attribute map** <dynamic-attribute-map-name> **map type sAMAccountName username**
- Ingrese este comando para definir al Grupo de servidores AAA:**aaa group server ldap** <server-group-name> **server** <server-name>
- Ingrese este comando para definir el servidor:**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>
- Ingrese este comando para definir la lista de métodos de autentificación para utilizar:**aaa authentication login** <name> **group** <server-group-name>

Herramientas AD

Para marcar el nombre absoluto de Distinguised (DN) de un usuario, ingrese uno de estos comandos del comando prompt AD:

```
dsquery user -name user1
```

O

```
dsquery user -samid user1
```

Nota: el "user1" mencionado anteriormente está en la cadena del regex. Usted puede también alistar todos los DN del nombre de usuario que comienzan con el usuario usando la cadena del regex como “user*”.

Para alistar todos los atributos de un único usuario, ingrese este comando del comando prompt AD:

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

Problemas posibles

En un despliegue LDAP, la operación de búsqueda se realiza primero, y la operación del lazo se realiza más adelante. Se realiza esta operación porque, si el atributo de la contraseña se vuelve como parte de la operación de búsqueda, la verificación de contraseña se puede hacer localmente en el cliente LDAP y no hay necesidad de una operación adicional del lazo. Si el atributo de la contraseña no se vuelve, una operación del lazo se puede realizar más adelante. Otra ventaja cuando usted realiza la operación de búsqueda primero y la operación del lazo es más adelante que el DN recibido en el resultado de la búsqueda se puede utilizar como el usuario DN en vez de la formación de un DN cuando el nombre de usuario (valor CN) se prefija con una base DN.

Pudo haber problemas cuando el lazo-**primer** comando de la **autenticación** se utiliza junto con un atributo definido por el usario que cambie donde la correspondencia del atributo del nombre de usuario señala. Por ejemplo, si usted utiliza esta configuración, usted es probable ver un error en su intento de autenticación:

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

Como consecuencia, usted verá los `Invalid credentiales (Credencial no válida),` mensaje de error del `código de resultado =49`. Los mensajes del registro parecerán similares a éstos:

```
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 =49Oct  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
```

Las líneas resaltadas indican cuál es incorrecto con el lazo inicial antes de la autenticación. Trabajará correctamente si usted quita el lazo-**primer** comando de la **autenticación de la** configuración antedicha.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre los atributos del ldap**
- **muestre al servidor LDAP todo**

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug del ldap todo**
- **haga el debug del evento del ldap**
- **debug aaa authentication**
- **debug aaa authorization**

Información Relacionada

- Cisco IOS Release 15.1MT de la guía de Configuración LDAP AAA
- ASA 8.0: Autenticación ldap de la configuración para los usuarios de WebVPN
- Soporte Técnico y Documentación - Cisco Systems