Ejemplo de Configuración de LDAP en Dispositivos IOS Usando Mapas de Atributo Dinámico

Contenido

Introducción

Este documento describe cómo utilizar la autenticación LDAP (protocolo ligero de acceso a directorios) en los cabeceras de Cisco IOS® y cambiar el nombre distinguido relativo predeterminado (RDN) de Nombre común (CN) a NombreContable de Cisco.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un dispositivo Cisco IOS que ejecuta Cisco IOS Software Release 15.0 o posterior.

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.

Convenciones

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

Problema principal

La mayoría de los usuarios de Microsoft Active Directory (AD) con LDAP suelen definir su RDN como sAMAccountName. Si utiliza el proxy de autenticación (auth-proxy) y un dispositivo de seguridad adaptable (ASA) como cabecera para sus clientes VPN, esto se soluciona fácilmente si define el tipo de servidor AD cuando define el servidor AAA o si ingresa el comando **ldap-names-attribute**. Sin embargo, en el Cisco IOS Software, ninguna de estas opciones está disponible. De forma predeterminada, el software Cisco IOS utiliza el valor de atributo CN en AD para la autenticación de nombre de usuario. Por ejemplo, un usuario se crea en AD como *John Fernandes*, pero su ID de usuario se almacena como *jfern*. De forma predeterminada, el software Cisco IOS verifica el valor CN. Es decir, el software verifica *John Fernandes* para la autenticación de nombre de usuario y no el valor sAMAccountName de *jfern* para la autenticación. Para obligar al Cisco IOS Software a verificar el nombre de usuario del valor del atributo sAMAccountName, utilice mapas de atributos dinámicos como se detalla en este documento.

Solución

Aunque los dispositivos Cisco IOS no soportan estos métodos de modificación de RDN, puede utilizar mapas de atributos dinámicos en el software Cisco IOS para lograr un resultado similar. Si ingresa el comando **show ldap attribute** en la cabecera de Cisco IOS, verá este resultado:

Atributo LDAP	Formato	Atributo AAA
airespaceBwDataBurstContract	Ulong	bsn-data-bandwidth-burst-æ
userPassword	String (cadena)	contraseña
airespaceBwRealBurstContract	Ulong	bsn-realtime-bandwidth-burst-c
Tipo de empleado	String (cadena)	tipo de empleado
airespaceServiceType	Ulong	service-type
airespaceACLName	String (cadena)	bsn-acl-name
priv-lvl	Ulong	priv-lvl
miembroOf	DN de caden	supplicant-group

	a	
cn	**String (cadena)**	**Nombre de usuario**
airespaceDSCP	Ulong	bsn-dscp
policyTag	String (cadena)	tag-name
airespaceQOSLevel	Ulong	bsn-qos-level
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-realtime-bandwidth-promedio
airespaceVlanInterfaceName	String (cadena)	bsn-vlan-interface-name
airespaceVapId	Ulong	bsn-wlan-id
airespaceBwDataAveContract	Ulong	bsn-data-bandwidth-promedio-con
sAMAccountName	String (cadena)	sam-account-name
MeetingContactInfo	String (cadena)	información de contacto
NúmeroTeléfono	String (cadena)	número de teléfono

Como puede ver en el atributo resaltado, el dispositivo de acceso de red (NAD) de Cisco IOS utiliza este mapa de atributos para las solicitudes de autenticación y para las respuestas. Básicamente, un mapa de atributos LDAP dinámico en el dispositivo Cisco IOS funciona bidireccionalmente. En otras palabras, los atributos se mapean no sólo cuando se recibe una respuesta, sino también cuando se envían solicitudes LDAP. Sin ningún mapa de atributos definido por el usuario, una configuración LDAP básica en NAD, verá este mensaje de registro cuando se envíe la solicitud:

```
*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)
```

Para cambiar este comportamiento y obligarlo a utilizar el atributo sAMAccountName para la verificación del nombre de usuario, ingrese el comando **ldap attribute map username** para crear este mapa de atributo dinámico primero:

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

Una vez definido este mapa de atributos, ingrese el comando *attribute map <dynamic-attribute-map-name>* para asignar este mapa de atributos al grupo de servidores AAA seleccionado (aaa-server).

Nota: Para facilitar todo este proceso, el ID de bug de Cisco CSCtr45874 (sólo clientes registrados) ha sido archivado. Si se implementa esta solicitud de mejora, permitirá a los usuarios identificar qué tipo de servidor LDAP se está utilizando y cambiar automáticamente algunos de estos mapas predeterminados para reflejar los valores usados por ese servidor en particular.

Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) 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 el mapa de atributos dinámico:

```
ldap attribute map

   map type sAMAccountName username
```

- Ingrese este comando para definir el grupo de servidores AAA:

```
aaa group server ldap

   server
```

- Ingrese este comando para definir el servidor:

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Ingrese este comando para definir la lista de métodos de autenticación que se utilizarán:

  aaa authentication login group

Herramientas AD

Para comprobar el nombre absoluto distinguido (DN) de un usuario, introduzca uno de estos comandos desde el símbolo del sistema de AD:

```
dsquery user -name user1
```

O

```
dsquery user -samid user1
```

Nota: "user1" mencionado anteriormente se encuentra en la cadena regex. También puede ingresar todos los DNs de nombre de usuario comenzando por el usuario usando la cadena de registro como "usuario*".

Para enumerar todos los atributos de un único usuario, ingrese este comando desde el símbolo del sistema de AD:

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

Problemas posibles

En una implementación LDAP, la operación de búsqueda se realiza primero y la operación de enlace se realiza más tarde. Esta operación se realiza porque, si se devuelve el atributo password como parte de la operación de búsqueda, la verificación de contraseña se puede realizar localmente en el cliente LDAP y no hay necesidad de una operación de enlace adicional. Si no se devuelve el atributo password, se puede realizar una operación bind más tarde. Otra ventaja cuando realiza primero la operación de búsqueda y luego la operación de enlace es que el DN recibido en el resultado de la búsqueda se puede utilizar como DN de usuario en lugar de la formación de un DN cuando el nombre de usuario (valor CN) está precedido de un DN base.

Puede haber problemas cuando el comando **authentication bind-first** se utiliza junto con un atributo definido por el usuario que cambia donde apunta el mapa del atributo username. Por ejemplo, si utiliza esta configuración, es probable que vea un error en su intento de autenticación:

```
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
```

Como resultado, verá el mensaje de error `Invalid credentials, Result code =49`. Los mensajes de registro serán similares a estos:

```
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
```

Las líneas resaltadas indican lo que está mal con el enlace inicial antes de la autenticación. Funcionará correctamente si quita el comando **authentication bind-first** de la configuración anterior.

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.

- **show ldap atributos**
- **show ldap server all**

Troubleshoot

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 Debug antes de utilizar los comandos **debug**.

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

Información Relacionada

- Guía de Configuración de AAA LDAP Cisco IOS Release 15.1MT
- ASA 8.0: Configuración de la Autenticación LDAP para Usuarios de WebVPN
- Soporte Técnico y Documentación - Cisco Systems