LDAP em dispositivos IOS usando o exemplo de configuração de mapas de atributos dinâmicos

Contents

Introduction

Este documento descreve como usar a autenticação LDAP (Lightweight Diretory Access Protocol) em headends do Cisco IOS® e alterar o RDN (Relative Distinguished Name) padrão de Common Name (CN) para sAMAccountName.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em um dispositivo Cisco IOS que executa o Cisco IOS Software Release 15.0 ou 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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Problema principal

A maioria dos usuários do Microsoft Ative Diretory (AD) com LDAP normalmente define seu RDN como o sAMAccountName. Se você usar proxy de autenticação (auth-proxy) e um Adaptive Security Appliance (ASA) como headend para seus clientes VPN, isso será facilmente corrigido se você definir o tipo de servidor AD quando definir o servidor AAA ou se você inserir o comando ldap-naming-attribute. No entanto, no software Cisco IOS, nenhuma dessas opções está disponível. Por padrão, o software Cisco IOS usa o valor de atributo CN no AD para autenticação de nome de usuário. Por exemplo, um usuário é criado no AD como *John Fernandes*, mas sua ID de usuário é armazenada como *jfern*. Por padrão, o software Cisco IOS verifica o valor CN. Ou seja, o software verifica *John Fernandes* para a autenticação de nome de usuário e não o valor sAMAccountName de *jfern* para a autenticação. Para forçar o software Cisco IOS a verificar o nome de usuário do valor do atributo sAMAccountName, use mapas de atributos dinâmicos conforme detalhado neste documento.

Solução

Embora os dispositivos Cisco IOS não suportem esses métodos de modificação de RDN, você pode usar mapas de atributos dinâmicos no software Cisco IOS para obter um resultado semelhante. Se você inserir o comando **show ldap attribute** no headend do Cisco IOS, verá esta saída:

Atributo LDAP	Formato	Atributo AAA
contratoBwDataBurstEspaço	Ulong	bsn-data-bandwidth-burst-contr
userPassword	Série	senha
contratoBwRealBurstEspaço	Ulong	bsn-realtime-bandwidth-burst-c
tipoDefuncionário	Série	tipo de funcionário
airespaceServiceType	Ulong	tipo de serviço
nomeACLNdoespaçodeataque	Série	bsn-acl-name
priv-lvl	Ulong	priv-lvl
membroDe	DN da cadeia de caracteres	grupo suplicante
cn	**Série**	**nome do usuário**
airespaceDSCP	Ulong	bsn-dscp
policyTag	Série	tag-name

nívelQOSLdoespaçoASIC	Ulong	bsn-qos-level
airespace8021PType	Ulong	bsn-8021p-type
ContratoRealAveEspaçoAtivo	Ulong	bsn-realtime-bandwidth-média
espaçoVlanInterfaceName	Série	bsn-vlan-interface-name
airespaceVapId	Ulong	bsn-wlan-id
contratoAveDadosEspaçoAtivo	Ulong	bsn-data-bandwidth-média-con
sAMAccountName	Série	sam-account-name
MeetingContactInfo	Série	contact-info
número de telefone	Série	número de telefone

Como você pode ver no atributo destacado, o NAD (Network Access Device, dispositivo de acesso à rede) do Cisco IOS usa esse mapa de atributos para solicitações de autenticação e para respostas. Basicamente, um mapa de atributos LDAP dinâmico no dispositivo Cisco IOS funciona bidirecionalmente. Em outras palavras, os atributos são mapeados não apenas quando uma resposta é recebida, mas também quando as solicitações LDAP são enviadas. Sem mapas de atributos definidos pelo usuário, uma configuração LDAP básica no NAD, você verá esta mensagem de log quando a solicitação for enviada:

```
*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 alterar esse comportamento e forçá-lo a usar o atributo sAMAccountName para verificação de nome de usuário, insira o comando **ldap attribute map username** para criar primeiro esse mapa de atributos dinâmicos:

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

Depois que este mapa de atributos tiver sido definido, digite o comando *attribute map <dynamic-attribute-map-name> para mapear esse mapa de atributos para o grupo de servidores AAA (aaa-server) selecionado.*

Observação: para facilitar todo esse processo, a ID de bug da Cisco CSCtr45874 (somente clientes registrados) foi arquivada. Se essa solicitação de aprimoramento for implementada, ela

permitirá que os usuários identifiquem que tipo de servidor LDAP está sendo usado e alterem automaticamente alguns desses mapas padrão para refletir os valores usados por esse servidor específico.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configuração de exemplo

Este documento utiliza as seguintes configurações:

- Insira este comando para definir o mapa de atributos dinâmicos:

```
ldap attribute map

   map type sAMAccountName username
```

- Insira este comando para definir o grupo de servidores AAA:

```
aaa group server ldap

   server
```

- Insira este comando para definir o servidor:

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- Insira este comando para definir a lista de métodos de autenticação a serem usados:

```
aaa authentication login group
```

Ferramentas do AD

Para verificar o DN absoluto de um usuário, insira um destes comandos no prompt de comando do AD:

```
dsquery user -name user1
```

OU

```
dsquery user -samid user1
```

Observação: "user1" mencionado acima está na string regex. Você também pode inscrever todos os DNs de nome de usuário começando com o usuário usando a string regex como "user*".

Para inscrever todos os atributos de um único usuário, insira este comando no prompt de comando do AD:

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

Problemas potenciais

Em uma implantação LDAP, a operação de pesquisa é executada primeiro, e a operação de associação é executada posteriormente. Esta operação é executada porque, se o atributo de senha for retornado como parte da operação de pesquisa, a verificação de senha pode ser feita localmente no cliente LDAP e não há necessidade de uma operação de associação extra. Se o atributo de senha não for retornado, uma operação de associação poderá ser executada posteriormente. Outra vantagem quando você executa a operação de pesquisa primeiro e a operação de associação posterior é que o DN recebido no resultado da pesquisa pode ser usado como o DN do usuário em vez da formação de um DN quando o nome do usuário (valor CN) é prefixado com um DN base.

Pode haver problemas quando o comando **authentication bind-first** é usado junto com um atributo definido pelo usuário que muda onde o mapa de atributos do nome de usuário aponta. Por exemplo, se você usa essa configuração, é provável que você veja uma falha na tentativa de autenticação:

```
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, você verá a mensagem `de` erro `Credenciais inválidas, Código do resultado =49`. As mensagens de log serão semelhantes a estas:

```
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
```

As linhas realçadas indicam o que está errado com a associação inicial antes da autenticação. Ele funcionará corretamente se você remover o comando **authentication bind-first** da configuração acima.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show ldap attribute**
- **show ldap server all**

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

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

Informações Relacionadas

- Guia de configuração LDAP AAA Cisco IOS versão 15.1MT
- ASA 8.0: Configurar a autenticação LDAP para usuários WebVPN
- Suporte Técnico e Documentação - Cisco Systems