동적 특성 맵을 사용하는 IOS 디바이스의 LDAP 컨피그레이션 예

목차

소개

이 문서에서는 Cisco IOS® 헤드엔드에서 LDAP(Lightweight Directory Access Protocol) 인증을 사용하고 기본 RDN(Relative Distinguished Name)을 CN(Common Name)에서 sAMAccountName으로 변경하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Software Release 15.0 이상을 실행하는 Cisco IOS 디바이스를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

핵심 문제

LDAP 사용자가 있는 대부분의 Microsoft AD(Active Directory)는 일반적으로 RDN을 sAMAccountName으로 정의합니다.VPN 클라이언트의 헤드엔드로 인증 프록시(auth-proxy) 및 ASA(Adaptive Security Appliance)를 사용하는 경우 AAA 서버를 정의할 때 또는 ldap-naming-attribute **명령**을 입력할 때 AD 서버 유형을 정의할 경우 이**를** 쉽게 수정할 수 있습니다.그러나 Cisco IOS 소프트웨어에서는 이러한 옵션을 사용할 수 없습니다.기본적으로 Cisco IOS 소프트웨어는 사용자 이름 인증에 AD의 CN 특성 값을 사용합니다.예를 들어, 사용자는 *John Fernandes*로 AD에 *생성되지만*, 사용자 ID는 *jafern*으로 저장됩니다.기본적으로 Cisco IOS 소프트웨어는 CN 값을 확인합니다.즉, 소프트웨어는 *John Fernandes*에게 사용자 이름 인증을 확인하지만 인증을 위해 jfern의 sAMAccountName 값*이* 아닙니다.Cisco IOS 소프트웨어가 sAMAccountName 특성 값에서 사용자 이름을 확인하도록 하려면 이 문서에 설명된 대로 동적 특성 맵을 사용합니다.

솔루션

Cisco IOS 디바이스는 이러한 RDN 수정 방법을 지원하지 않지만, Cisco IOS 소프트웨어에서 동적 특성 맵을 사용하여 유사한 결과를 얻을 수 있습니다.Cisco IOS 헤드엔드에서 **show ldap attribute** 명령을 입력하면 다음 출력이 표시됩니다.

LDAP 특성	형식	AAA 특성
대소문자 구분bw데이터Burst계약	우롱	bsn- data-bandwidth-burst-conter
사용자 암호	문자열	암호
응답BwRealBurst계약	우롱	bsn-realtime-bandwidth-burst-c
직원 유형	문자열	직원 유형
airespace서비스 유형	우롱	서비스 유형
ACLN이름	문자열	bsn-acl-name
priv lvl	우롱	priv lvl
구성원	문자열 DN	신청자 그룹
cn	**문자열**	**사용자 이름**
airespaceDSCP	우롱	bsn-dscp
정책 태그	문자열	태그 이름
airespaceQOSLevel	우롱	bsn-qos 레벨
airespace8021PType	우롱	bsn-8021p 유형
응답BwRealAve계약	우롱	bsn 실시간 대역폭 평균

airespaceVlan인터페이스 이름	문자열	bsn-vlan-interface-name
airespaceVapId	우롱	bsn-wlan-id
대소문자bw데이터Ave계약	우롱	bsn-data-bandwidth-average-con
sAMAccount이름	문자열	sam 계정 이름
모임 연락처 정보	문자열	연락처 정보
전화 번호	문자열	전화 번호

강조 표시된 속성에서 볼 수 있듯이 Cisco IOS NAD(Network Access Device)는 인증 요청 및 응답에 이 특성 맵을 사용합니다.기본적으로 Cisco IOS 디바이스의 동적 LDAP 특성 맵은 양방향으로 작동합니다.즉, 특성은 응답이 수신될 때뿐만 아니라 LDAP 요청이 전송될 때도 매핑됩니다.사용자 정의 특성 맵이 없는 경우 NAD의 기본 LDAP 컨피그레이션이 없으면 요청이 전송될 때 다음 로그 메시지가 표시됩니다.

```
*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)
```

이 동작을 변경하고 사용자 이름 확인을 위해 sAMAccountName 특성을 사용하도록 하려면 ldap attribute **map username** 명령을 입력하여 이 동적 특성 맵을 먼저 생성합니다.

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

이 특성 맵이 정의되면 **특성 맵 *<dynamic-attribute-map-name>*** 명령을 입력하여 이 특성 맵을 선택한 AAA 서버 그룹(aaa-server)에 매핑합니다.

참고: 이 전체 프로세스를 보다 쉽게 만들기 위해 Cisco 버그 ID CSCtr45874(등록된 고객만 해당)가 접수되었습니다.이 개선 요청을 구현하면 사용자가 어떤 종류의 LDAP 서버가 사용되고 있는지 식별하고 이러한 기본 맵 중 일부를 자동으로 변경하여 해당 특정 서버에서 사용하는 값을 반영할 수 있습니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

샘플 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

- 동적 특성 맵을 정의하려면 다음 명령을 입력합니다.

```
ldap attribute map

   map type sAMAccountName username
```

- AAA 서버 그룹을 정의하려면 다음 명령을 입력합니다.

```
aaa group server ldap

   server
```

- 서버를 정의하려면 다음 명령을 입력합니다.

```
ldap server

   ipv4
   attribute map

   bind authentication root-dn password

   base-dn
```

- 사용할 인증 방법 목록을 정의하려면 다음 명령을 입력합니다.

```
aaa authentication login group
```

AD 툴

사용자의 절대 DN(Distinguished Name)을 확인하려면 AD 명령 프롬프트에서 다음 명령 중 하나를 입력합니다.

```
dsquery user -name user1
```

또는

```
dsquery user -samid user1
```

참고: 위에서 언급한 "user1"은 regex 문자열에 있습니다.또한 regex 문자열을 "user*"로 사용하여

사용자로 시작하는 사용자 이름의 모든 DN을 등록할 수 있습니다.

단일 사용자의 모든 특성을 등록하려면 AD 명령 프롬프트에서 다음 명령을 입력합니다.

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

잠재적 문제

LDAP 구축에서 검색 작업이 먼저 수행되고 바인딩 작업이 나중에 수행됩니다.이 작업은 검색 작업의 일부로 password 특성이 반환되면 LDAP 클라이언트에서 비밀번호 확인을 로컬로 수행할 수 있으며 추가 바인딩 작업을 수행할 필요가 없기 때문에 수행됩니다.password 특성이 반환되지 않으면 나중에 바인딩 작업을 수행할 수 있습니다.검색 작업을 먼저 수행하고 나중에 바인딩 작업을 수행할 때 또 다른 장점은 사용자 이름(CN 값)이 기본 DN으로 접두사로 붙으면 검색 결과에서 수신된 DN을 사용자 DN으로 사용할 수 있다는 것입니다.

authentication bind-first 명령을 사용자 이름 특성 맵이 가리키는 위치를 변경하는 사용자 정의 특성과 함께 사용할 때 문제가 발생할 수 있습니다.예를 들어, 이 컨피그레이션을 사용하는 경우 인증 시도에 오류가 발생할 수 있습니다.

```
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
```

따라서 Invalid credentials, `Result code = 49` 오류 메시지가 표시됩니다.로그 메시지는 다음과 유사합니다.

```
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
```

강조 표시된 행은 인증 전에 초기 바인드에 문제가 있음을 나타냅니다.위 컨피그레이션에서 **authentication bind-first** 명령을 제거하면 제대로 작동합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **ldap 특성 표시**
- **ldap 서버 모두 표시**

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **ldap 모두 디버그**
- **ldap 이벤트 디버그**
- **디버그 aaa 인증**
- **디버그 aaa 권한 부여**

관련 정보

- AAA LDAP 컨피그레이션 가이드 Cisco IOS 릴리스 15.1MT
- ASA 8.0:WebVPN 사용자를 위한 LDAP 인증 구성
- 기술 지원 및 문서 – Cisco Systems