Содержание

Введение

Этот документ описывает, как использовать аутентификацию Протокола LDAP на головных узлах Cisco IOS® и изменить Относительное составное имя (RDN) по умолчанию от Общего имени (CN) до sAMAccountName.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на устройстве Cisco IOS, которое выполняет Cisco IOS Software Release 15.0 или позже.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Базовая проблема

Большая часть Microsoft Active Directory (AD) с пользователями LDAP, как правило, определяет их RDN, чтобы быть sAMAccountName. Если вы вводите команду атрибута именования ldap, при использовании аутентификации прокси-сервера (auth-proxy) и Устройство адаптивной защиты (ASA) как головной узел для клиентов VPN это легко исправлено при определении AD типа сервера при определении AAA-сервера или. Однако в программном обеспечении Cisco IOS, ни одна из этих опций не доступна. По умолчанию программное обеспечение Cisco IOS использует значение атрибута CN в AD для аутентификации имени пользователя. Например, пользователь создан в AD как *Джон Фернандес*, но его идентификатор пользователя сохранен как *jfern*. По умолчанию программное обеспечение Cisco IOS проверяет значение CN. Т.е. программное обеспечение проверяет *Джона Фернандеса* для аутентификации имени пользователя а не sAMAccountName значения *jfern* для аутентификации. Чтобы вынудить программное обеспечение Cisco IOS проверить имя пользователя от sAMAccountName значения атрибута, используйте динамические карты атрибута, как детализировано в этом документе.

Решение

Несмотря на то, что устройства Cisco IOS не поддерживают эти методы модификации RDN, можно использовать динамические карты атрибута в программном обеспечении Cisco IOS для достижения похожего результата. При вводе **команды show ldap attribute** в головную станцию Cisco IOS вы будете видеть эти выходные данные:

Атрибут LDAP	**Формат**	**Атрибут AAA**
airespaceBwDataBurstContract	Ulong	bsn-data-bandwidth-burst-contr
user password	Строка	password
airespaceBwRealBurstContract	Ulong	bsn-realtime-bandwidth-burst-c
employeeType	Строка	тип сотрудника
airespaceServiceType	Ulong	service type
airespaceACLName	Строка	bsn-acl-name
priv-lvl	Ulong	priv-lvl
memberOf	DN строки	группа соискателя
cn	**Строка**	**имя пользователя**
airespaceDSCP	Ulong	bsn-dscp

policyTag	Строка	имя тега
airespaceQOSLevel	Ulong	bsn-qos-level
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-realtime-bandwidth-average
airespaceVlanInterfaceName	Строка	bsn-vlan-interface-name
airespaceVapId	Ulong	bsn-wlan-id
airespaceBwDataAveContract	Ulong	bsn-data-bandwidth-average-con
sAMAccountName	Строка	sam-учетное-имя
meetingContactInfo	Строка	контактная информация
telephoneNumber	Строка	номер телефона

Как вы можете видеть от выделенного атрибута, Устройство доступа Cisco IOS network (NAD) использует эту карту атрибута для запросов аутентификации и для ответов. В основном динамическая Карта атрибутов LDAP в устройстве Cisco IOS функционирует двунаправленным образом. Другими словами, атрибуты сопоставлены, не только когда ответ получен, но также и когда отосланы запросы LDAP. Когда запрос отослан, без любых определяемых пользователем карт атрибута, основной Конфигурации LDAP на NAD, вы видите это сообщение журнала:

Чтобы изменить это поведение и вынудить его использовать атрибут sAMAccountName для проверки имени пользователя, введите **команду ldap attribute map username** для создания этой динамической карты атрибута сначала:

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

Как только эта карта атрибута была определена, введите команду **<dynamic-attribute-map-name> карты атрибута** для сопоставления этой карты атрибута с выбранной группой AAA-серверов (aaa-server).

Примечание: Для создания этого полного процесса легче, идентификатор ошибки Cisco, CSCtr45874 (только зарегистрированные клиенты) был подан. Если этот запрос на расширение будет внедрен, то он позволит пользователям определять, какой Сервер LDAP используется, и автоматически измените некоторые из этих схем по умолчанию для отражения значений, используемых тем индивидуальным сервером.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Пример конфигурации

Эти конфигурации используются в данном документе:

- Введите эту команду для определения динамической карты атрибута: **LDAP** <dynamic-attribute-map-name> **sAMAccountName**
- Введите эту команду для определения группы AAA-серверов:**ldap aaa group server** < > < >
- Введите эту команду для определения сервера:**ldap server** <server-name> **ipv4** <host-address> <dynamic-attribute-map-name> **dn** <complete-dn-root-user> <pwd > **dn** <complete-dn-search-base>
- Введите эту команду для определения списка методов аутентификации для использования: <name> **aaa authentication login** < >

AD программные средства

Для проверки абсолютного Названия Distinguised (DN) пользователя введите одну из этих команд от AD командной строки:

```
dsquery user -name user1
```

Или

```
dsquery user -samid user1
```

Примечание: упомянутый выше "user1" находится в строке regex. Можно также включить в список все DN имени пользователя начиная с пользователя при помощи строки regex как "пользователь*".

Для включения в список всех атрибутов одиночного пользователя введите эту команду от AD командной строки:

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

Возможные проблемы

В развертываниях LDAP поисковая операция выполнена сначала, и связывать операция выполнена позже. Эта операция выполнена, потому что, если атрибут пароля возвращен как часть поисковой операции, проверка пароля может быть сделана локально на клиенте LDAP и нет никакой потребности в дополнительном, связывают операцию. Если атрибут пароля не возвращен, связывать операция может быть выполнена позже. Другое преимущество при выполнении поисковой операции сначала и связывать операции позже состоит в том, что DN, полученный в результате поиска, может использоваться в качестве пользовательского DN вместо формирования DN, когда имя пользователя (значение CN) снабжено префиксом основной DN.

Могли бы быть проблемы, когда **команда authentication bind-first** используется наряду с определяемым пользователем атрибутом, который изменяется, где указывает карта атрибута имени пользователя. Например, при использовании этой конфигурации вы, вероятно, будете видеть сбой в своей попытке аутентификации:

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

В результате вы будете видеть сообщение об ошибках `Invalid credentials, Result code =49.` Сообщения журнала будут выглядеть подобными им:

```
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=com
ldap_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
```

Выделенные линии указывают что не так с начальной буквой, связывают перед аутентификацией. Это будет работать должным образом при удалении **команды authentication bind-first** из вышеупомянутой конфигурации.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- атрибуты show ldap
- сервер show ldap все

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- ldap отладки все
- событие ldap отладки
- debug aaa authentication
- debug aaa authorization

Дополнительные сведения

- Cisco IOS Release руководства конфигурации LDAP AAA 15.1 мт
- ASA 8.0: Настройка проверки подлинности LDAP для пользователей WebVPN
- Cisco Systems – техническая поддержка и документация