مثال LDAP على أجهزة IOS التي تستخدم سمات الديناميكية تكوين خرائط

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
مسألة أساسية
الحل
التكوين
عينة من التكوين
أدوات الإعلان
مشاكل محتملة
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية إستخدام مصادقة بروتوكول الوصول إلى الدليل (LDAP) في نهايات الاستقبال الرئيسية من Cisco IOS® وتغيير الاسم المميز النسبي الافتراضي (RDN) من الاسم الشائع (CN) إلى sAMAccountName.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز Cisco IOS الذي يشغل برنامج Cisco IOS Software، الإصدار 15.0 أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

مسألة أساسية

معظم Microsoft Active Directory (AD) مع مستخدمي LDAP يقومون عادة بتعريف RDN الخاص بهم ليصبح sAMAccountName. إذا كنت تستخدم وكيل المصادقة (وكيل المصادقة) وأجهزة الأمان المعدلة (ASA) كنقطة وصول لعملاء VPN، فهذا يتم إصلاحه بسهولة إذا قمت بتعريف نوع خادم AD عند تعريف خادم AAA أو إذا قمت بإدخال الأمر ldap-label-attribute. ومع ذلك، في برنامج Cisco IOS software، لا يتوفر أي من هذه الخيارات. افتراضيا، يستخدم برنامج Cisco IOS قيمة سمة CN في AD لمصادقة اسم المستخدم. على سبيل المثال، يتم إنشاء مستخدم في AD باسم *جون فيرناندیز*، لكن هوية المستخدم الخاصة به مخزنة على هيئة *JFERN*. بشكل افتراضي، يتحقق برنامج Cisco IOS software من قيمة CN. وهذا يعني أن البرنامج يتحقق من *جون فيرناندیز* لمصادقة اسم المستخدم وليس من قيمة sAMAccountName الخاصة ب *jfern* للمصادقة. لإجبار برنامج Cisco IOS software على التحقق من اسم المستخدم من قيمة سمة sAMAccountName، أستخدم خرائط السمات الديناميكية كما هو مفصل في هذا المستند.

الحل

وعلى الرغم من أن أجهزة Cisco IOS لا تدعم هذه الطرق الخاصة بتعديل RDN، فيمكنك إستخدام خرائط السمات الديناميكية في برنامج Cisco IOS software لتحقيق نتيجة مماثلة. إذا قمت بإدخال الأمر **show ldap attribute** على وحدة الاستقبال والبث من Cisco IOS، فسترى هذا الإخراج:

سمة LDAP	**تنسيق**	**سمة AAA**
AirespaceBwDataBurst Contract	أولونغ	BSN- بروتوكول تدفق بيانات النطاق الترددي
مستخدم password	السلسلة	كلمة المرور
AirespaceBwRealBurst Contract	أولونغ	BSN- بروتوكول Realtime-bandwidth-burst-C
نوع الموظف	السلسلة	نوع الموظف
AirespaceServiceType	أولونغ	نوع الخدمة
AirespaceACLName	السلسلة	BSN-ACL اسم
priv-lvl	أولونغ	priv-lvl
عضو	DN للسلسلة	جماعة متملصة
سي إن	**السلسلة**	**username**
AirespaceDSCP	أولونغ	BSN-DSCP
PolicyTag	السلسلة	اسم العلامة
AirespaceQOSLevel	أولونغ	BSN-QoS مستوى
Airespace8021PtYpe	أولونغ	bsn-8021p-type
AirespaceBwRealAveContract	أولونغ	متوسط عرض النطاق الترددي في الوقت الحقيقي ل BSN
AirespaceVlanInterface Name	السلسلة	bsn-vlan-interface-name

AirespaceVapId	أولونغ	bsn-wlan-id
AirespaceBwDataAveContract	أولونغ	BSN-data-bandwidth-average-con
sAMAccountName	السلسلة	اسم حساب سام
meetingContactInfo	السلسلة	معلومات الاتصال
رقم الهاتف	السلسلة	رقم الهاتف

كما يمكنك أن ترى من السمة المميزة، يستخدم جهاز الوصول إلى الشبكة (NAD) من Cisco IOS خريطة السمة هذه لطلبات المصادقة والاستجابات. وبشكل أساسي، يعمل مخطط سمة LDAP الديناميكي في جهاز Cisco IOS بشكل ثنائي الإتجاه. بمعنى آخر، لا يتم تعيين الخصائص فقط عند تلقي إستجابة، بل أيضا عند إرسال طلبات LDAP. بدون أي خرائط لسمات معرفة من قبل المستخدم، أو تكوين LDAP أساسي على NAD، سترى رسالة السجل هذه عند إرسال الطلب:

```
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*
```

لتغيير هذا السلوك وإرغامه على إستخدام السمة sAMAccountName للتحقق من اسم المستخدم، أدخل الأمر **ldap attribute map username** لإنشاء خريطة السمة الديناميكية هذه أولا:

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

بمجرد تحديد خريطة السمات هذه، أدخل الأمر dynamic-attribute-map-name> **attribute map**> لتعيين خريطة هذه السمة إلى مجموعة خوادم aaa-server) AAA) المحددة.

ملاحظة: لتسهيل هذه العملية بالكامل، تم تصنيف معرف تصحيح الأخطاء من CSCtr45874 Cisco (العملاء المسجلون فقط). إذا تم تنفيذ طلب التحسين هذا، فسيسمح للمستخدمين بتحديد نوع خادم LDAP الذي يتم إستخدامه وتغيير بعض هذه الخرائط الافتراضية تلقائيا لتعكس القيم المستخدمة من قبل هذا الخادم المعين.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

عينة من التكوين

يستخدم هذا المستند التكوينات التالية:

- أدخل هذا الأمر لتحديد خريطة السمات الديناميكية:

```
ldap attribute map

map type sAMAccountName username
```

- أدخل هذا الأمر لتحديد مجموعة خوادم AAA:

```
aaa group server ldap

server
```

- أدخل هذا الأمر لتحديد الخادم:

```
ldap server

ipv4
attribute map

bind authentication root-dn password

base-dn
```

- دخلت هذا أمر in order to عينت القائمة ميلان إلى جانب من صحة هوية طريقة أن يستعمل:

```
aaa authentication login group
```

أدوات الإعلان

للتحقق من الاسم المميز المطلق (DN) لمستخدم، أدخل أحد هذه الأوامر من موجه أمر AD:

```
dsquery user -name user1
```

أو

```
dsquery user -samid user1
```

ملاحظة: "user1" المذكور أعلاه موجود في سلسلة regex. يمكنك أيضا إدراج جميع DNs لاسم المستخدم بدءا من المستخدم باستخدام سلسلة regex ك "user*".

دخلت in order to عددت all the شعار من وحيد مستعمل، هذا أمر من ال ad أمر رسالة حث:

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

مشاكل محتملة

في نشر LDAP، يتم إجراء عملية البحث أولا، ويتم تنفيذ عملية الربط لاحقا. يتم تنفيذ هذه العملية لأنه، إذا تم إرجاع سمة كلمة المرور كجزء من عملية البحث، يمكن إجراء التحقق من كلمة المرور محليا على عميل LDAP ولا توجد حاجة إلى عملية ربط إضافية. إذا لم يتم إرجاع سمة كلمة المرور، يمكن تنفيذ عملية ربط لاحقا. هناك ميزة أخرى عند إجراء عملية البحث أولا وعملية الربط لاحقا هي أنه يمكن إستخدام DN الذي تم إستلامه في نتيجة البحث ك DN للمستخدم بدلا من تكوين DN عندما يكون اسم المستخدم (قيمة CN) تم إصلاحه مسبقا مع DN أساسي.

قد تكون هناك مشاكل عند إستخدام الأمر **authentication bind-first** مع سمة معرفة من قبل المستخدم والتي تتغير حيث نقاط خريطة سمة اسم المستخدم. على سبيل المثال، إذا كنت تستخدم هذا التكوين، فمن المحتمل أن ترى فشلا في محاولة المصادقة الخاصة بك:

```
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
```

نتيجة لذلك، سترى = رسالة الخطأ 49. ستبدو رسائل السجل مماثلة لما يلي:

```
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
```

تشير الخطوط المبرزة إلى الخطأ في الربط الأولي قبل المصادقة. سيعمل بشكل صحيح إذا قمت بإزالة الأمر **authentication bind-first** من التكوين أعلاه.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- إظهار سمات ldap
- show ldap server all

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- debug ldap all
- debug ldap حدث
- تصحيح أخطاء مصادقة aaa (المصادقة والتفويض والمحاسبة)
- تخويل debug aaa

معلومات ذات صلة

- دليل تكوين Cisco IOS AAA LDAP، الإصدار 15.1MT
- ASA 8.0: تكوين مصادقة LDAP لمستخدمي WebVPN
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).