كيف يمكن إستخدام استعلام قبول LDAP للتحقق من صحة مستلمي الرسائل الواردة باستخدام Microsoft Active Directory (LDAP)؟

المحتويات

سؤال:

كيف يمكن إستخدام استعلام قبول LDAP للتحقق من صحة مستلمي الرسائل الواردة باستخدام Microsoft Active Directory (LDAP)؟

ملاحظة: يتكامل المثال التالي مع نشر Microsoft Active Directory قياسي، رغم إمكانية تطبيق المبادئ على أنواع عديدة من عمليات تنفيذ LDAP.

ستقوم أولا بإنشاء إدخال خادم LDAP، وعند هذه النقطة يجب عليك تحديد خادم الدليل الخاص بك وكذلك الاستعلام الذي سيقوم به جهاز أمان البريد الإلكتروني. يتم بعد ذلك تمكين الاستعلام أو تطبيقه على موزع الرسائل (العام) الوارد. يمكن مشاركة إعدادات خادم LDAP هذه بواسطة مستمعين مختلفين وأجزاء أخرى من التكوين مثل الوصول إلى العزل الخاص بالمستخدم النهائي.

لتسهيل تكوين استعلامات LDAP على جهاز IronPort، نوصي باستخدام مستعرض LDAP، الذي يسمح لك بإلقاء نظرة على المخطط الخاص بك بالإضافة إلى جميع السمات التي يمكنك الاستعلام عنها.

بالنسبة لأنظمة التشغيل Microsoft Windows، يمكنك إستخدام:

بالنسبة لنظام التشغيل Linux أو UNIX، يمكنك إستخدام erasecat4000_flash `ldapsearch`:.

أولا، تحتاج إلى تعريف خادم LDAP للاستعلام. في هذا المثال، يتم توفير الاسم المستعار "PublicLDAP" لخادم LDAP *myldapserver.example.com*. يتم توجيه الاستعلامات إلى منفذ TCP رقم 389 (الافتراضي).

ملاحظة: إذا كان تنفيذ Active Directory الخاص بك يحتوي على مجالات فرعية، فلن تتمكن من الاستعلام عن المستخدمين في مجال فرعي باستخدام DN الأساسي للمجال الجذر. ومع ذلك، عند إستخدام Active Directory، يمكنك أيضا الاستعلام عن LDAP مقابل خادم الكتالوج العمومي (GC) على منفذ TCP رقم 3268. يحتوي GC على معلومات جزئية ل *all* كائنات في غابة Active Directory ويوفر إحالات إلى المجال الفرعي المعني عندما تكون هناك حاجة إلى مزيد من المعلومات. إذا تعذر عليك "العثور" على المستخدمين في المجالات الفرعية الخاصة بك، فاترك DN الأساسي عند الجذر وقم بتعيين IronPort لاستخدام منفذ GC.

:GUI

1. قم بإنشاء ملف تعريف خادم LDAP جديد بقيم موجودة مسبقا من خادم الدليل (إدارة النظام > LDAP). على سبيل المثال: اسم ملف تعريف الخادم: *PublicLDAP*اسم المضيف: *myldapserver.example.com*أسلوب المصادقة: *إستخدام كلمة المرور: ممكن*username:*cn=esa،cn=users،dc=example،dc=com*كلمة المرور: *كلمة المرور*نوع الخادم: خدمة *Active Directory*المنفذ: 3268تأكد من BaseDN:*dc=example،dc=com* إستخدام الزر "خادم (خوادم) الاختبار" للتحقق من إعداداتك قبل المتابعة. يجب أن تبدو المخرجات الناجحة كما يلي:

```
Connecting to myldapserver.example.com at port 3268
Bound successfullywithDNCN=ESA,CN=Users,DC=example,DC=com
Result: succeeded
```

2. أستخدم نفس الشاشة لتعريف استعلام قبول LDAP. يتحقق المثال التالي من عنوان المستلم مقابل السمات الأكثر شيوعا، إما "mail" أو "proxyAddress":الاسم:
QueryString:*(|(mail={a})(proxyAddress=smtp:{a*)*{PublicLDAP.ACCEPT*يمكنك إستخدام الزر "إختبار الاستعلام" للتحقق من أن استعلام البحث الخاص بك يقوم بإرجاع النتائج لحساب صالح. يجب أن يبدو الإخراج الناجح الذي يتم البحث فيه عن عنوان حساب الخدمة esa.admin@example.com" كما يلي:

```
Query results for host:myldapserver.example.com
(Query (mail=esa.admin@example.com) >to server PublicLDAP (myldapserver.example.com:3268
Query (mail=esa.admin@example.com) lookup success, (myldapserver.example.com:3268) returned
1 results
Success: Action: Pass
```

3. تطبيق استعلام القبول الجديد هذا على المصغي الوارد (الشبكة > المستمعين). قم بتوسيع الخيارات استعلامات LDAP > قبول، واختر استعلامك PublicLDAP.قبول.

4. أخيرا، قم بتطبيق التغييرات لتمكين هذه الإعدادات.

:CLI

1. **أولا، يمكنك إستخدام الأمر *ldapconfig* لتعريف خادم LDAP للجهاز الذي سيتم الربط به، كما يتم تكوين الاستعلامات عن قبول المستلم (الأمر الفرعي ldapaccept)، والتوجيه (الأمر الفرعي ldaprouting)، والتنكر (الأمر الفرعي الخاص بالتخفي).**

```
mail3.example.com> ldapconfig
.No LDAP server configurations
:Choose the operation you want to perform
.NEW - Create a new server configuration -
new <[]
:("Please create a name for this server configuration (Ex: "PublicLDAP
PublicLDAP <[]
:Please enter the hostname
myldapserver.example.com <[]
Use SSL to connect to the LDAP server? [N]> n
:Please enter the port number
389 <[389]
:Please enter the base
dc=example,dc= com]>dc=example,dc=com]
:Select the authentication method to use for this server configuration
Anonymous .1
```

```
                                                    Password based .2
                                                              2 <[1]
                                          :Please enter the bind username
                                 cn=Anonymous]>cn=ESA,cn=Users,dc=example,dc=com]
                                          :Please enter the bind password
                                                        password <[]
                                                   Name: PublicLDAP
                                 Hostname: myldapserver.example.com Port 389
                                                Authentication Type: password
                                                    Base:dc=example,dc=com
```

2. ثانيا، تحتاج إلى تحديد الاستعلام لتنفيذه مقابل خادم LDAP الذي قمت بتكوينه للتو.

```
                                          :Choose the operation you want to perform
                                 .SERVER - Change the server for the query -
.LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped -
   .LDAPROUTING - Configure message routing. - MASQUERADE - Configure domain masquerading -
            .LDAPGROUP - Configure whether a sender or recipient is in a specified group -
                                                .SMTPAUTH - Configure SMTP authentication -
                                                        ldapaccept <[]
                                                :Please create a name for this query
                                      PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept]
                                                   :Enter the LDAP query string
                                 (({mailLocalAddress= {a})]>(|(mail={a})(proxyAddresses=smtp:{a)]
                                                :Please enter the cache TTL in seconds
                                                                        <[900]
                                :Please enter the maximum number of cache entries to retain
                                                                      <[10000]
                                                Do you want to test this query? [Y]> n
                                                           Name: PublicLDAP
                                 Hostname: myldapserver.example.com Port 389
                                                Authentication Type: password
                                                       Base:dc=example,dc=com
                                             LDAPACCEPT: PublicLDAP.ldapaccept
```

3. بمجرد تكوين استعلام LDAP، تحتاج إلى تطبيق نهج LDAP ACCEPT على موزع الرسائل الوارد الخاص بك.

```
                                                  example.com> listenerconfig
                                          :Currently configured listeners
                                Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public .1
                              Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private .2
                                          :Choose the operation you want to perform
                                                    .NEW - Create a new listener -
                                                       .EDIT - Modify a listener -
                                                    .DELETE - Remove a listener -
                                                 .SETUP - Change global settings -
                                                              edit <[]
                                .Enter the name or number of the listener you wish to edit
                                                                    1 <[]
                                                           Name: InboundMail
                                                                Type: Public
                                      Interface: PublicNet (192.168.2.1/24) TCP Port 25
                                                            Protocol: SMTP
                                                           :Default Domain
                                          (Max Concurrency: 1000 (TCP Queue: 50
                                                        Domain Map: Disabled
                                                                    TLS: No
                                                    SMTP Authentication: Disabled
                                                          Bounce Profile: Default
                              Use SenderBase For Reputation Filters and IP Profiling: Yes
                                                                Footer: None
                                                                   LDAP: Off
                                          :Choose the operation you want to perform
                                          .NAME - Change the name of the listener -
                                                .INTERFACE - Change the interface -
                                            .LIMITS - Change the injection limits -
```

```
                                                    .SETUP - Configure general options -
                                                .HOSTACCESS - Modify the Host Access Table -
                                            .RCPTACCESS >- Modify the Recipient Access Table -
.BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener -
                                        .MASQUERADE - Configure the Domain Masquerading Table -
                                                .DOMAINMAP - Configure domain mappings -
LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should be -
                                                                    .accepted or bounced/dropped
                                    .LDAPROUTING - Configure an LDAP query to reroute messages -
                                           ldapaccept Available Recipient Acceptance Queries <[]
                                                                                    None .1
                                                                  PublicLDAP.ldapaccept .2
                                                                                    2 <[1]
                        ?Should the recipient acceptance query drop recipients or bounce them
                         NOTE: Directory Harvest Attack Prevention may cause recipients to be
                                                                    .dropped regardless of this setting
                                                                                  bounce .1
                                                                                    drop .2
                                                                                    2 <[2]
                                                                        Name: InboundMail
                                                                             Type: Public
                                                  Interface: PublicNet (192.168.2.1/24) TCP Port 25
                                                                           Protocol: SMTP
                                                                          :Default Domain
                                                      (Max Concurrency: 1000 (TCP Queue: 50
                                                                      Domain Map: Disabled
                                                                                TLS: No
                                                                SMTP Authentication: Disabled
                                                                      Bounce Profile: Default
                                          Use SenderBase For Reputation Filters and IP Profiling: Yes
                                                                           Footer: None
                                                        (LDAP: ldapaccept (PublicLDAP.ldapaccept
```

4. لتنشيط التغييرات التي تم إجراؤها على المصغي، قم بتنفيذ التغييرات.

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).