# لنم ققحتال LDAP ربع LDAP نم ققحتال LDP.exe مادختساب CA ةداەشو

# المحتويات

<u>المقدمة</u> كيفية التحقق <u>قبل البدء</u> خطوات التحقق نتيجة الاختبار المستندات ذات الصلة

## المقدمة

عندما تقوم بإنشاء كائن مصادقة على FireSIGHT Management Center ل Active Directory LDAP عبر SSL/TLS (LDAPs)، قد يكون من الضروري في بعض الأحيان إختبار شهادة CA واتصال SSL/TLS، والتحقق مما إذا فشل كائن المصادقة في الاختبار. يشرح هذا المستند كيفية تشغيل الاختبار باستخدام Microsoft LDP.exe.

# كيفية التحقق

### قبل البدء

قم بتسجيل الدخول إلى كمبيوتر محلي في Microsoft Windows باستخدام حساب مستخدم له امتياز إداري محلي لتنفيذ الخطوات على هذا المستند.

**ملاحظة**: إذا لم يكن لديك حاليا LDP.exe متوفر على نظامك، فيجب عليك أولا تنزيل **أدوات دعم Windows**. يتوفر هذا على موقع Microsoft على الويب. بمجرد تنزيل **أدوات دعم Windows** وتثبيتها، اتبع الخطوات التالية.

قم بإجراء هذا الاختبار على كمبيوتر محلي يعمل بنظام التشغيل Windows لم يكن عضوا في مجال، حيث إنه سيضمن الجذر أو مرجع مصدق للمؤسسة إذا انضم إلى مجال. إذا لم يعد الكمبيوتر المحلي موجودا في مجال ما، فيجب إزالة شهادة المرجع المصدق الجذر أو شهادة المؤسسة من مخزن **مراجع التصديق الجذر الموثوق به** للكمبيوتر المحلي قبل إجراء هذا الاختبار.

#### خطوات التحقق

الخطوة 1: بدء تطبيق ldp.exe. انتقل إلى القائمة **ابدأ** وانقر فوق **تشغيل**. اكتب ldp.exe واضغط الزر **موافق**.

**الخطوة 2:** الاتصال بوحدة التحكم بالمجال باستخدام FQDN لوحدة التحكم بالمجال. للاتصال، انتقل إلى **الاتصال > الاتصال** وأدخل FQDN لوحدة التحكم بالمجال. ثم حدد SSL، حدد المنفذ 636 كما هو موضح أدناه وانقر فوق

| فق. | مواذ |
|-----|------|
|-----|------|

| rt: 636 Connectionles | Server: | pdc1.virtual | lab local      |
|-----------------------|---------|--------------|----------------|
| I♥ SSL                | Port:   | 636          | Connectionless |

**الخطوة 3:** إذا لم يكن المرجع المصدق للمؤسسة أو الجذر موثوقا به على كمبيوتر محلي، فإن النتيجة تبدو كما يلي. تشير رسالة الخطأ إلى أن الشهادة التي تم تلقيها من الخادم البعيد تم إصدارها من قبل مرجع مصدق غير موثوق به.

| View   | Options Utilities   |
|--------|---|
| ld = 1 | ap_sslinit("pdc1.virtuallab.local", 636, 1);                            |
| Error  | 0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3) |
| Error  | (0x51> = Idap_connect(hLdap, NULL);                                     |
| Serv   | error: <empty></empty>  |
| Frron  | (0x51): Fail to connect to ndc1.virtuallab.local.                       |

**الخطوة 4:** تؤدي تصفية رسائل الحدث على كمبيوتر Windows المحلي مع المعايير التالية إلى توفير نتيجة محددة:

- مصدر الحدث = قناة
- معرف الحدث = 36882

| The certificate the certificate | received from the remo<br>can be validated. The SS | te server was issued by an<br>L connection request has f | untrusted certificate authority. Because of this, none of the data contained in<br>ailed. The attached data contains the server certificate. |
|---------------------------------|--|--|--|
|                                 |  |  |  |
| Log Name:                       | System   |  |  |
| Log Name:<br>Source:            | System<br>Schannel                                 | Logged:  | 11/24/2012 8:22:30 PM  |

**الخطوة 5:** إستيراد شهادة المرجع المصدق إلى مخزن شهادات كمبيوتر Windows المحلي.

i. تشغيل Microsoft Management Console (MMC). انتقل إلى القائمة **ابدأ** وانقر فوق **تشغيل**. اكتب **mmc** واضغط على الزر **موافق**.

| Run   | <u>?</u> ×   |
|-------|--|
|       | Type the name of a program, folder, document, or<br>Internet resource, and Windows will open it for you. |
| Open: | mmc  |
|       | OK Cancel <u>B</u> rowse   |

2. إضافة الأداة الإضافية لشهادة الكمبيوتر المحلي. انتقل إلى الخيارات التالية في قائمة **الملف**:

إضافة/أداة إضافية عن بعد > شهادات > إضافة > أختر "حساب الكمبيوتر" > الكمبيوتر المحلي: (الكمبيوتر الذي تعمل عليه وحدة التحكم هذه) > إنهاء موافق.

ثالثا - إستيراد شهادة المرجع المصدق.

**جذر وحدة التحكم > الشهادات** (كمبيوتر محلي) > **مراجع التصديق الجذر الموثوق بها > الشهادات**>انقر بزر الماوس الأيمن > **جميع المهام>إستيراد**.

| 🚡 Console1  |
|---|
| 📙 🤆 Console 💆 Window Help 🗍 🎦 🚅 🔚 💷   |
| Console Root  |
| Action View Eavorites $\downarrow \leftarrow \Rightarrow \mid \blacksquare \blacksquare \blacksquare$ |
| Tree Favorites Name   |
| Console Root 🐻 Certificates (Local Computer)  |
| 🖻 👹 Certificates (Local Computer)   |
| Personal     Trusted Boot Certification Authorities   |
| Find Certificates   |
| All Tasks Find Certificates   |
| New Window from Here Import   |
| Refresh   |
| Help  |
|   |
| Add a certificate to a store  |

• طقطقت **بعد ذلك** واستعرض إلى Base64 يرمز X.509 شهادة (\*.crt) CA شهادة مبرد. ثم حدد الملف. • انقرعات فتح كالتالي محدد وضع كار الشمادات في المخنين التالي في احد التمريية الحذر المعثمة. فيما

• انقر على **فتح > التالي** وحدد **وضع كل الشهادات في المخزن التالي: مراجع التصديق الجذر الموثوق فيها.** 

|            | ate Import Wizard   |
|------------|---|
| Certifica  | ate Store   |
| Cert       | ificate stores are system areas where certificates are kept.                                      |
| Win<br>the | dows can automatically select a certificate store, or you can specify a location for certificate. |
| 1          | C Automatically select the certificate store based on the type of certificate                     |
| 1          | Place all certificates in the following store   |
|            | Certificate store:  |
|            | Trusted Root Certification Authorities\Local Computer Browse                                      |
|            |   |
|            |   |
|            |   |
|            |   |
|            |   |
|            |   |
| .earn mo   | re about <u>certificate stores</u>  |
| .earn mo   | re about <u>certificate stores</u>  |
| .earn mo   | pre about <u>certificate stores</u>   |
| earn mo    | ore about <u>certificate stores</u>   |

iv. تأكد من أن CA مدرج مع CA الجذر الآخر الموثوق به.

**الخطوة 6:** اتبع الخطوة 1 و 2 للاتصال بخادم AD LDAP عبر SSL. إذا كانت شهادة المرجع المصدق صحيحة، فيجب أن تكون الأسطر العشرة الأولى في الجزء الأيمن من ldp.exe كما يلي:

```
Id = Idap_sslinit("pdc1.virtuallab.local", 636, 1);
Error <0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Error <0x0> = Idap_connect(hLdap, NULL);
Error <0x0> = Idap_get_option(hLdap,LDAP_OPT_SSL,[void*]&Iv);
Host supports SSL, SSL cipher strength = 128 bits
Established connection to pdc1.virtuallab.local.
Retrieving base DSA information...
Result <0>: [null]
Matched DNs:
Getting 1 entries:
>> Dn:
```

إذا نجحت شهادة واتصال LDAP في هذا الاختبار، فيمكنك تكوين كائن المصادقة ل LDAP عبر SSL/TLS بنجاح. ومع ذلك، إذا فشل الاختبار بسبب تكوين خادم LDAP أو مشكلة في الشهادة، فيرجى حل المشكلة على خادم AD أو تنزيل شهادة CA الصحيحة قبل تكوين كائن المصادقة على مركز إدارة FireSIGHT.

# المستندات ذات الصلة

- تعريف سمات كائن LDAP لخدمة Active Directory لتكوين كائن المصادقة
  - تكوين كائن مصادقة LDAP على نظام FireSIGHT

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما