使用Ldp.exe驗證通過SSL/TLS的 LDAP(LDAPS)和CA證書

目錄

<u>簡介</u> <u>如何驗證</u> <u>開始之前</u> <u>驗證步驟</u> <u>測試結果</u> 相關檔案

簡介

在FireSIGHT管理中心上為Active Directory LDAP Over SSL/TLS(LDAPS)建立身份驗證對象時,有時可能需要測試CA證書和SSL/TLS連線,並驗證身份驗證對象是否未通過測試。本文檔介紹如何使用Microsoft Ldp.exe運行測試。

如何驗證

開始之前

使用具有本地管理許可權的使用者帳戶登入到Microsoft Windows本地電腦,以執行本文檔上的步驟 。

附註:如果您的系統目前沒有ldp.exe,您必須首先下載**Windows支援工具**。可從Microsoft網 站獲得此功能。下載並安裝**Windows支援工具**後,請執行以下步驟。

在不是域成員的本地Windows電腦上執行此測試,因為如果根或企業CA加入域,它將信任它。如果 本地電腦不再位於域中,則在執行此測試之前,應從本地電腦**受信任的根證書頒發機構**儲存中刪除 根或企業CA證書。

驗證步驟

第1步:啟動ldp.exe應用程式。轉到「**Start**」選單,然後按一下「**Run**」。鍵入**ldp.exe**並按OK按鈕 。

第2步:使用域控制器FQDN連線到域控制器。若要連線,請轉到**連線>連線**,然後輸入域控制器 FQDN。然後選擇SSL,指定埠636(如下所示),然後按一下OK。

| Server: pdc1.virt | uallab local |
|-------------------|----------------|
| Port: 636 | Connectionless |
| OK | Cancel |

步驟3:如果在本地電腦上根或企業CA不受信任,則結果如下所示。錯誤消息表示從遠端伺服器收到 的證書是由不受信任的證書頒發機構頒發的。

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

第4步:使用以下條件過濾本地Windows電腦上的事件消息可提供特定結果:

- 事件源=機構
- •事件ID = 36882

| The certificate | received from the remo | te server was issued by an | untrusted certificate authority. Because of this, none of the data contained in |
|----------------------|-------------------------|----------------------------|---|
| the certificate | can be randated. The 35 | e connection request has t | |
| | | | |
| Log Name: | System | | |
| Log Name: Source: | System Schannel | Logged: | 11/24/2012 8:22:30 PM |

第5步:將CA證書匯入到本地Windows電腦證書儲存區。

i.運行Microsoft管理控制檯(MMC)。 轉到「Start」選單,然後按一下「Run」。鍵入mmc,然後按 一下OK按鈕。

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

二。新增本地電腦證書管理單元。在「檔案」(File)選單上導航至以下選項:

Add/Remote Snap-in > Certificates > Add >Choose "Computer Account" > Local Computer:(運行 此控制檯的電腦) > Finish>OK。

三。匯入CA證書。

Console Root > Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates > 按一下右鍵>All Tasks > Import。

| 🚡 Console1 | | | | |
|---|------------------|--------------|--------------|----------|
| ∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp |) 🖻 🖬 💷 | | | |
| 🚡 Console Root | | | | |
| Action <u>V</u> iew <u>F</u> avorites | ← → 🛍 💽 | 🖪 😫 | | |
| Tree Favorites | | Name | | |
| Console Root | | 🗐 Certificat | es (Local Co | omputer) |
| 🖻 👹 Certificates (Local Computer |) | | | |
| ⊕ | n Authorities | | | |
| | Find Certificate | s | | |
| | All Tasks | • | Find Cert | ificates |
| | New Window fr | om Here | Import | |
| | Refresh | | | |
| | Help | | | |
| | | | | |
| | | <u> </u> | | |
| Add a certificate to a store | | | | 11. |

• 按一下「**Next**」,然後瀏覽至「Base64 Encoded X.509 Certificate(*.cer, *.crt)CA certificate file。然後選擇檔案。

 按一下Open > Next,然後選擇Place all certificates in the following store:受信任的根憑證授權 單位。

• 按一下**下一步>完成**匯入檔案。

| Certificate Import Wizard | | |
|--|-------------------------|-----------------------|
| Certificate Store Certificate stores are system areas where | certificates are kept. | |
| Windows can automatically select a certific the certificate. | ate store, or you can s | pecify a location for |
| C Automatically select the certificate : | store based on the type | e of certificate |
| Place all certificates in the following | store | |
| Certificate store: | | |
| Trusted Root Certification Authori | ties\Local Computer | Browse |
| Learn more about <u>certificate stores</u> | | |
| | < Back Ne | ext > Cancel |

四。確認該CA與其他受信任的根CA一起列出。

第6步:按照步驟1和2操作,通過SSL連線到AD LDAP伺服器。如果CA證書正確,ldp.exe右窗格中 的前10行應如下所示:

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:

測試結果

如果證書和LDAP連線通過此測試,則可以成功配置通過SSL/TLS的LDAP身份驗證對象。但是,如 果由於LDAP伺服器配置或證書問題導致測試失敗,請解決AD伺服器上的問題或下載正確的CA證書 ,然後在FireSIGHT管理中心上配置身份驗證對象。

相關檔案

- 確定身份驗證對象配置的Active Directory LDAP對象屬性
- 在FireSIGHT系統上配置LDAP身份驗證對象