Verificare LDAP su SSL/TLS (LDAPS) e certificato CA utilizzando Ldp.exe

Sommario

Introduzione Verifica Operazioni preliminari Fasi di verifica Risultato test Documenti correlati

Introduzione

Quando si crea un oggetto di autenticazione in un centro di gestione FireSIGHT per Active Directory LDAP over SSL/TLS (LDAPS), a volte può essere necessario verificare il certificato CA e la connessione SSL/TLS e verificare se l'oggetto di autenticazione non supera il test. In questo documento viene illustrato come eseguire il test utilizzando Microsoft Ldp.exe.

Verifica

Operazioni preliminari

Accedere a un computer locale di Microsoft Windows con un account utente con privilegi amministrativi locali per eseguire le operazioni descritte in questo documento.

Nota: Se sul sistema non è attualmente disponibile ldp.exe, è innanzitutto necessario scaricare gli **Strumenti di supporto di Windows**. È disponibile sul sito Web Microsoft. Dopo aver scaricato e installato gli **Strumenti di supporto di Windows**, eseguire la procedura seguente.

Eseguire questo test su un computer Windows locale che non è stato membro di un dominio, in quanto considererebbe attendibile la CA radice o l'autorità di certificazione dell'organizzazione (enterprise) se fosse aggiunta a un dominio. Se un computer locale non è più incluso in un dominio, è necessario rimuovere il certificato CA radice o dell'organizzazione dall'archivio Autorità di certificazione radice attendibili del computer locale prima di eseguire il test.

Fasi di verifica

Passaggio 1: Avviare l'applicazione ldp.exe. Andare al menu **Start** e fare clic su **Esegui**. Digitare **ldp.exe** e fare clic sul pulsante **OK**.

Passaggio 2: Connettersi al controller di dominio utilizzando l'FQDN del controller di dominio. Per connettersi, selezionare **Connessione > Connetti** e immettere il nome di dominio completo del controller di dominio. Quindi selezionare **SSL**, specificare la porta **636** come mostrato di seguito e fare clic su **OK**.

Server:	pdc1.virtuall	ab local
Port:	636	Connectionless
OK		Cancel

Passaggio 3: Se la CA radice o l'autorità di certificazione dell'organizzazione (enterprise) non è considerata attendibile in un computer locale, il risultato sarà il seguente. Il messaggio di errore indica che il certificato ricevuto dal server remoto è stato emesso da un'autorità di certificazione non attendibile.

```
View Options Utilities

Id = Idap_sslinit("pdc1.virtuallab.local", 636, 1);

Error <0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);

Error <0x51> = Idap_connect(hLdap, NULL);

Server error: <empty>

Error <0x51>: Fail to connect to pdc1.virtuallab.local.
```

Passaggio 4: L'applicazione di un filtro ai messaggi di evento nel computer Windows locale in base ai criteri seguenti restituisce un risultato specifico:

- Origine evento = Schannel
- ID evento = 36882

General Detail	s		
The certificate the certificate	received from the remo can be validated. The SS	ote server was issued by an SL connection request has f	untrusted certificate authority. Because of this, none of the data contained in ailed. The attached data contains the server certificate.
Log Name:	System		
Source	Schannel	Logged:	11/24/2012 8:22:30 PM
Event ID:	36882	Task Category:	None

Passaggio 5: Importare il certificato CA nell'archivio certificati del computer Windows locale.

i. Eseguire Microsoft Management Console (MMC). Andare al menu **Start** e fare clic su **Esegui**. Digitare **mmc** e premere il pulsante **OK**.

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

ii. Aggiungere lo snap-in certificato del computer locale. Passare alle opzioni seguenti del menu **File**:

Add/Remote Snap-in > Certificati > Add > Choose "Computer Account" > Computer locale: (il computer su cui è in esecuzione questa console) > Fine > OK.

iii. Importare il certificato CA.

Radice console > Certificati (computer locale) > Autorità di certificazione radice attendibili > Certificati > Clic con il pulsante destro del mouse > Tutte le attività > Importa.

🚡 Console1				
∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp) 🖻 🖬 💷			
🚡 Console Root				
Action View Eavorites	← → 🛍 💽	j 🖪 😫		
Tree Favorites		Name		
Console Root		🗐 Certifical	tes (Local Co	omputer)
🖻 👹 Certificates (Local Computer)			
Horizonal Horizonal Trusted Root Certificatio	on Authorities			
	Find Certificate	s		
	All Tasks	•	Find Cert	ificates
	New Window fr	om Here	Import	
	Refresh			
	Help			
Add a certificate to a store				

- Fare clic su **Avanti** e selezionare il file del certificato CA X.509 con codifica Base64 (*.cer, *.crt). Selezionare quindi il file.
- Fare clic su Apri > Avanti e selezionare Metti tutti i certificati nel seguente archivio: Autorità di certificazione radice attendibili.
- Fare clic su **Avanti > Fine** per importare il file.

Certificat	e Import Wizard
Certificate	e Store
Certifi	cate stores are system areas where certificates are kept.
Windo the ce	ws can automatically select a certificate store, or you can specify a location for rtificate.
С	Automatically select the certificate store based on the type of certificate
¢	Place all certificates in the following store
	Certificate store:
	Trusted Root Certification Authorities\Local Computer Browse
Learn more	e about <u>certificate stores</u>

iv. Verificare che la CA sia elencata con altre CA radice attendibili.

Passaggio 6: Seguire i passaggi 1 e 2 per connettersi al server LDAP AD tramite SSL. Se il certificato CA è corretto, le prime 10 righe sul riquadro destro di Idp.exe devono essere le seguenti:

```
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:
```

Se un certificato e una connessione LDAP superano questo test, è possibile configurare correttamente l'oggetto di autenticazione per LDAP su SSL/TLS. Tuttavia, se il test non riesce a causa di un problema di configurazione del server LDAP o di certificato, risolvere il problema sul server AD o scaricare il certificato CA corretto prima di configurare l'oggetto di autenticazione sul centro di gestione FireSIGHT.

Documenti correlati

- Identificare gli attributi dell'oggetto LDAP di Active Directory per la configurazione dell'oggetto di autenticazione
- <u>Configurazione dell'oggetto di autenticazione LDAP sul sistema FireSIGHT</u>