# Ldp.exe を使用して SSL/TLS(LDAPS)および CA 証明書で LDAP を検証する

### 内容

<u>概要</u> <u>の検証方法</u> <u>はじめに</u> 確認手順 <u>テスト結果</u> 関連資料

## 概要

FireSIGHT Management Center で、Active Directory LDAP Over SSL/TLS(LDAP)用の認証オ ブジェクトを作成する場合、CA 証明書と SSL/TLS 接続をテストし、認証オブジェクトがテスト に失敗しないか確認することが必要になることがあります。このドキュメントでは、Microsoft Ldp.exe を使用してテストを実行する方法について説明します。

# の検証方法

#### はじめに

このドキュメントの手順を実行するには、ローカルの管理権限を持つユーザアカウントを使用して Microsoft Windows ローカルコンピュータにログインします。

**注**:現在システムでldp.exeを使用できない場合は、まず**Windowsサポートツール**をダウン ロードする必要があります。このツールは、Microsoft 社の Web サイトで入手できます。 **Windowsサポートツール**をダウンロードしてインストールしたら、次の手順に従います。

ローカル Windows コンピュータは、ドメインに参加すると、ルート CA またはエンタープライズ CA を信頼します。そのため、このテストは、ドメインのメンバーではないローカル Windows コ ンピュータで実行します。ローカルコンピュータがドメインに参加していない場合、このテスト を実行する前に、コンピュータの [信頼されたルート証明機関(Trusted Root Certification Authorities)] ストアからルート証明書またはエンタープライズ CA 証明書を削除する必要があり ます。

#### 確認手順

**ステップ1:**Idp.exeアプリケーションを起動します。[スタートメニュー(Start)] メニューから [実行(Run)] を選択します。Idp.exeと入力し、OKボタンを押します。

ステップ2:ドメインコントローラの FQDN を使用して、ドメインコントローラに接続します。 接続するには、[接続(Connection)] > [接続(Connect)] の順に移動して、ドメインコントロー ラの FQDN を入力します。次に、[SSL] を選択し、次に示すようにポート 636 を指定して、[OK] をクリックします。

Server:	pdc1.virtual	lab.local
Port:	636	Connectionless
0	K I	Cancel

**ステップ 3**: ルート CA またはエンタープライズ CA が、ローカルコンピュータで信頼されてい ない場合、次のような結果が表示されます。このエラーメッセージは、リモートサーバから受信 した証明書が信頼できない認証局によって発行されたことを示しています。

View	Options Utilities
ld =	ldap_sslinit("pdc1.virtuallab.local", 636, 1);
Erro	r <0x0> = Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Erro	r <0x51> = Idap_connect(hLdap, NULL);
Serv	/er error: <empty></empty>
Erro	r <0x51>: Fail to connect to pdc1.virtuallab.local.

**ステップ 4**: ローカル Windows コンピュータのイベントメッセージを次の条件でフィルタリング すると、結果を具体的に確認できます。

- イベントソース = Schannel
- イベント ID = 36882

General Details

The certificate received from the remote server was issued by an untrusted certificate authority. Because of this, none of the data contained in the certificate can be validated. The SSL connection request has failed. 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

i.Microsoft Management Console(MMC)を起動します。 [スタートメニュー(Start)] メニュー から [実行(Run)] を選択します。mmc と入力して、[OK] ボタンをクリックします。

Run		<u>?×</u>
	Type the name of a program, I Internet resource, and Window	folder, document, or ws will open it for you.
Open:	mmc	<b></b>
	ОК	Cancel <u>B</u> rowse

ii.ローカルコンピューター証明書スナップインを追加します。[ファイル(File)] メニューで、次のオプションに移動します。

[スナップインの追加と削除(Add/Remove Snap-in)] > [証明書(Certificates)] > [追加(Add)] > [コンピューターアカウント(Computer Account)] を選択 > [ローカルコンピューター: (こ のコンソールを実行しているコンピューター)(Local Computer (the computer this console is running on))] > [完了(Finish)] > [OK]

iii.CA証明書をインポートします。

0

[コンソールルート(Console Root)] > [証明書(ローカルコンピューター)(Certificates (Local Computer))] > [信頼されたルート証明機関(Trusted Root Certification Authorities)] > [証明書 (Certificates)] > 右クリックする > [すべてのタスク(All Tasks)] > [インポート(Import)]

🚡 Console1			
∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp	) 🖻 🖬 💷		
🚡 Console Root			<u> </u>
<u>Action</u> <u>V</u> iew <u>E</u> avorites	← →   🛍 💽	j   🖪   😫	
Tree Favorites		Name	
Console Root		🗐 Certifica	tes (Local Computer)
🖻 👹 Certificates (Local Computer	)		
⊕	on Authorities		
	Find Certificate	s	
	All Tasks	•	Find Certificates
	New Window fr	om Here	Import
	Refresh		
	Help		
Add a certificate to a store			1.

- [次へ(Next)] をクリックして、Base64 でエンコードされた X.509 証明書(\*.cer、\* .crt)の CA 証明書ファイルを参照し、ファイルを選択します。
- [開く (Open)] > [次へ (Next)] の順にクリックして、[証明書をすべて次のストアに配置す る (Place all certificates in the following store)] : **[信頼されたルート証明機関 (Trusted Root Certification Authorities)] を選択します。**
- •[次へ(Next)]>[完了(Finish)]の順にクリックして、ファイルをインポートします。

Pertificate Store         Certificate stores are system areas where certificates are kept.         Windows can automatically select a certificate store, or you can specify a location for the certificate.         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		tificate Import Wizard
Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. 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		tificate Store
<ul> <li>Windows can automatically select a certificate store, or you can specify a location for the certificate.</li> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:</li> <li>Trusted Root Certification Authorities\Local Computer</li> <li>Browse</li> </ul>	ertificates are kept.	Certificate stores are system area
<ul> <li>Automatically select the certificate store based on the type of certificate</li> <li>Place all certificates in the following store</li> <li>Certificate store:         <ul> <li>Trusted Root Certification Authorities\Local Computer</li> <li>Browse</li> </ul> </li> </ul>	te store, or you can specify a location for	Windows can automatically select the certificate.
<ul> <li>Place all certificates in the following store</li> <li>Certificate store:         <ul> <li>Trusted Root Certification Authorities\Local Computer</li> <li>Browse</li> </ul> </li> </ul>	ore based on the type of certificate	C Automatically select the ce
Certificate store: Trusted Root Certification Authorities\Local Computer Browse	tore	Place all certificates in the
Trusted Root Certification Authorities\Local Computer Browse		Certificate store:
	s\Local Computer Browse	Trusted Root Certification
arn more about <u>certificate stores</u>		n more about <u>certificate stores</u>
< Back   Next >   Car	< Back   Next >   Cance	

iv.CAが他の信頼されたルートCAと共にリストされていることを確認します。

**ステップ 6**: ステップ 1 と 2 を実行し、SSL を介して AD LDAP サーバに接続します。CA 証明 書が正しい場合、ldp.exe の右側のペインに表示される最初の 10 行は、次のようになります。

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:

## テスト結果

このテストで、証明書と LDAP 接続に問題がないことを確認できれば、SSL/TLS を介した LDAP

の認証オブジェクトを正常に設定できます。ただし、LDAP サーバの設定、または証明書の問題 が原因でテストに失敗した場合は、FireSIGHT Management Center で認証オブジェクトを設定す る前に、AD サーバの問題を解決するか、正しい CA 証明書をダウンロードしてください。

# 関連資料

- 認証オブジェクトに関する Active Directory LDAP オブジェクト属性の識別の設定
- <u>FireSIGHT システムでの LDAP 認証オブジェクトの設定</u>