SSL または TLS 経由で Microsoft AD 認証を行うための FireSIGHT システム上の認証オブジェクトの検証

内容

概要

外部 Active Directory LDAP ユーザによる Web ユーザ インターフェイスと CLI に対するアクセス認証を許可するように FireSIGHT Management Center を設定することができます。この記事では、SSL/TLS を使用した Microsoft AD 認証のための認証オブジェクトを設定、テスト、トラブルシューティングする方法を説明します。

前提条件

FireSIGHT Management Center でのユーザ管理および外部認証システムに関する知識があることが推奨されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

手順

ステップ 1：SSL/TLS 暗号化を使用せずに認証オブジェクトを設定します。

1. 通常と同じように認証オブジェクトを設定します。暗号化認証と非暗号化認証の基本的な設定手順は同じです。
2. 認証オブジェクトが機能していて、AD LDAP ユーザが非暗号化認証を行えることを確認します。

ステップ 2：CA 証明書を使用せずに SSL および TLS を使用して認証オブジェクトをテストします。

CA 証明書を使用せずに SSL および TLS を使用して認証オブジェクトをテストします。問題が発

生した場合は、システム管理者に問い合わせて AD LDS サーバに関する問題を解決してください。認証オブジェクトに証明書がアップロード済みの場合は、[Certificate has been loaded (Select to clear loaded certificate)] を選択し、証明書をクリアしてから認証オブジェクトを再テストします。

認証オブジェクトが失敗した場合は、次のステップに進む前に、システム管理者に問い合わせて AD LDS SSL/TLS 設定を確認してください。ただし、次のステップに進んで、CA 証明書を使用した認証オブジェクトのテストを行うこともできます。

ステップ 3：**Base64 CA 証明書をダウンロードします。**

1. AD LDS にログインします。
2. Web ブラウザを開き、http://localhost/certsrv にアクセスします。
3. [Download a CA certificate, certificate chain, or CRL] をクリックします。
4. [CA Certificate] リストから CA 証明書を選択し、[Encoding Method] から [Base64] を選択します。
5. [Download CA certificate] リンクをクリックして certnew.cer ファイルをダウンロードします。

ステップ 4：証明書の [Subject] フィールドの値を確認します。

1. certnew.cer を右クリックして [open] を選択します。.
2. [Details] タブをクリックし、[Show] ドロップダウン オプションから [<All>] を選択します。
3. 各フィールドの値を確認します。特に、[Subject] フィールドの値が認証オブジェクトの [Primary Server Host] の名前と一致していることを確認します。

ステップ 5：Microsoft Windows マシン上で証明書をテストします。このテストは、ワークグループまたはドメインに参加している Windows マシン上で実行できます。

> **ヒント**：FireSIGHT Management Center で認証オブジェクトを作成する前に、このステップを使用して Windows システム上で CA 証明書をテストできます。

1. CA 証明書を C:\Certficate または任意のディレクトリにコピーします。
2. Windowsコマンドラインcmd.exeを実行します。管理者として
3. Certutil コマンドを使用して CA 証明書をテストします。

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

Windows マシンがすでにドメインに参加している場合、CA 証明書は証明書ストアに保管されているため、cacert.test.txt にエラーは記録されていないはずです。一方、Windows マシンがワークグループに属している場合、信頼された CA リストに CA 証明書があるかどうかによって、次の 2 つのメッセージのうちのいずれかが表示されることがあります。

a.CA は信頼されている一方、CA の CRL が見つからない場合：

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b.CA が信頼されていない場合：

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

次に示すようなエラー メッセージが表示された場合は、システム管理者に問い合わせて AD LDS および中間 CA に関する問題を解決してください。これらのエラー メッセージは、証明書が誤っていること、CA 証明書内のサブジェクトが誤っていること、あるいは証明書チェーンが欠落していることなどを示唆します。

```
Failed "AIA" Time: 0
Failed "CDP" Time: 0
Error retrieving URL: The specified network resource or d evice is no longer available
```

ステップ6:CA証明書が有効であり、ステップ5でテストに合格したことを確認したら、証明書を認証オブジェクトにアップロードし、テストを実行します。

ステップ 7：認証オブジェクトを保存し、システム ポリシーを再適用します。