目次

概要

外部アクティブ ディレクトリ LDAP ユーザが Web ユーザ ユーザー・ インターフェースおよび CLI にアクセスを認証することを可能にするように FireSIGHT Management Center を設定できます。 この技術情報は、テストするために設定する方法を、解決します SSL/TLS 上の Microsoft AD 認証のための認証 オブジェクトを論議します。

前提条件

Cisco は FireSIGHT Management Center のユーザマネージメントおよび外部認証認証システムのナレッジがあることを推奨します。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

手順

ステップ 1. SSL/TLS 暗号化なしで認証 オブジェクトを設定して下さい。

1. 普通ように認証 オブジェクトを設定して下さい。 暗号化されるのための基本構成ステップは非暗号化認証同じであり。
2. 認証 オブジェクトがはたらき、AD LDAP がユーザ非暗号化を認証できることを確認して下さい。

ステップ 2. CA 認証なしで SSL および TLS 上の認証 オブジェクトをテストして下さい。

CA 証明書なしで SSL および TLS 上の認証 オブジェクトをテストして下さい。 問題に出会う場合、AD LDS サーバのこの問題を解決するために System Admin と相談して下さい。 認証が認証オブジェクトに以前にアップロードされる場合、「**認証**証明書をクリアし、AO を再度テストするために**ロードされました（選り抜きロードされた認証をクリアするため）**」を選択して下さい。

認証 オブジェクトが失敗した場合、次 の ステップに進む前に AD LDS SSL/TLS 設定を確認するために System Admin を参照して下さい。 ただし、次のステップに CA 認証の認証 オブジェクトを更にテストし続けること自由に感じて下さい。

ステップ 3.ダウンロード **Base64** CA 証明書。

1. AD LDS へのログイン。
2. Webブラウザを開き、`http://localhost/certsrv` に接続して下さい
3. クリックして下さい「**ダウンロード CA 認証、証明書 チェーン、または CRL**」を
4. 選択して下さい「**符号化 方式**」からの「**CA 認証**」リストおよび「**Base64"** から CA 証明書を
5. `certnew.cer` ファイルをダウンロードするために「**ダウンロード CA 認証**」リンクをクリックして下さい。

ステップ 4.証明書の**認証対象**値を確認して下さい。

1. `certnew.cer` を右クリックし、『Open』 を選択 して下さい。
2. タブを『Details』 をクリック し、**提示**ドロップダウン オプションから **<All> を**選択して下さい
3. 各フィールドの値を確認して下さい。 特に**サブジェクト**値が認証 オブジェクトの**プライマリ サーバ ホスト名と**一致することを、確認して下さい。

ステップ 5. Microsoft Windows マシンの CERT をテストして下さい。 ワークグループまたはドメインによって加入される Windows マシンのこのテストを行うことができます。

> **ヒント**： このステップが FireSIGHT Management Center の認証 オブジェクトを作成する前に Windows システムの CA 認証をテストするのに使用することができます。

1. `C:\Certficate` か優先 する ディレクトリに CA 証明書をコピーして下さい。
2. Run ウィンドウ コマンド・ライン、管理者 `cmd.exe`
3. Certutil コマンドで CA 認証をテストして下さい

```
cd c:\Certificate

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

Windows マシンが既にドメイン加入されている場合、CA 認証は認証 ストアにあり、`cacert.test.txt` に No エラーがあるはずです。 ただし、Windows マシンがワークグループにあれば、信頼された CA リストの CA 証明書のプロシージャによって 2 つのメッセージの 1 つが表示されるかもしれません。

a. CA は信頼されますが、CRL は CA のために見つけませんでした:

```
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 は信頼されません:

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

の下で、AD LDS および中間 CA の問題を解決するために System Admin と相談しなさいように他のどのエラーメッセージも得れば。 これらのエラーメッセージは不正確な証明書を表している、CA 証明書のサブジェクト、抜けた証明書 チェーン、先祖などです

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
```

```
CertUtil: -verify command completed successfully.
```
ステップ 6 確認すれば CA 証明書は有効で、ステップ 5 のテストに合格し、認証 オブジェクトに証明書をアップロードし、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て下さい。