Verifizierung des Authentifizierungsobjekts im FireSIGHT-System für Microsoft AD-Authentifizierung über SSL/TLS

Inhalt

Einführung

Sie können ein FireSIGHT Management Center so konfigurieren, dass externe Active Directory-LDAP-Benutzer den Zugriff auf die Webbenutzeroberfläche und die CLI authentifizieren können. In diesem Artikel wird erläutert, wie das Authentifizierungsobjekt für Microsoft AD Authentication Over SSL/TLS konfiguriert, getestet und Fehler behoben werden.

Voraussetzung

Cisco empfiehlt, dass Sie über Kenntnisse in den Bereichen Benutzerverwaltung und externes Authentifizierungssystem im FireSIGHT Management Center verfügen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Vorgehensweise

Schritt 1: Konfigurieren des Authentifizierungsobjekts ohne SSL/TLS-Verschlüsselung.

1. Konfigurieren Sie das Authentifizierungsobjekt wie gewohnt. Die grundlegenden Konfigurationsschritte für die verschlüsselte und unverschlüsselte Authentifizierung sind identisch.
2. Vergewissern Sie sich, dass das Authentifizierungsobjekt funktioniert, und AD-LDAP-Benutzer können sich unverschlüsselt authentifizieren.

Schritt 2: Testen des Authentifizierungsobjekts über SSL und TLS ohne Zertifizierungsstellenzertifikat.

Testen Sie das Authentifizierungsobjekt über SSL und TLS ohne CA-Zertifikat. Falls ein Problem auftritt, wenden Sie sich an Ihren Systemadministrator, um dieses Problem auf dem AD LDS-Server zu beheben. Wenn zuvor ein Zertifikat in das Authentifizierungsobjekt hochgeladen wurde, wählen Sie "**Zertifikat wurde geladen (Wählen Sie zum Löschen des geladenen Zertifikats aus)**", um das Zertifikat zu löschen und AO erneut zu testen.

Wenn das Authentifizierungsobjekt fehlschlägt, bitten Sie Ihren Systemadministrator, die AD LDS SSL/TLS-Konfiguration zu überprüfen, bevor Sie mit dem nächsten Schritt fortfahren. Sie können jedoch die folgenden Schritte ausführen, um das Authentifizierungsobjekt mit dem Zertifizierungsstellenzertifikat weiter zu testen.

Schritt 3: Laden Sie **Base64** CA Cert herunter.

1. Melden Sie sich beim AD LDS an.
2. Öffnen Sie einen Webbrowser, und stellen Sie eine Verbindung mit http://localhost/certsrv her.
3. Klicken Sie auf "**Zertifizierungsstellenzertifikat, Zertifikatskette oder CRL herunterladen**".
4. Wählen Sie das CA-Zertifikat aus der Liste "**CA Certificate**" und **Base64** aus der Liste "**Encoding Method**" aus.
5. Klicken Sie auf den Link **Zertifikat herunterladen**, um die certnew.cer-Datei herunterzuladen.

Schritt 4: Überprüfen Sie den **Betreff-**Wert im Zertifikat.

1. Klicken Sie mit der rechten Maustaste auf certnew.cer und wählen Sie **Öffnen** aus.
2. Klicken Sie auf die Registerkarte **Details** und wählen Sie **<Alle>** aus den Dropdown-Optionen Anzeigen aus.
3. Überprüfen Sie den Wert für jedes Feld. Überprüfen Sie insbesondere, ob der **Subject-**Wert mit dem **primären Server-Hostnamen** des Authentifizierungsobjekts übereinstimmt.

Schritt 5: Testen Sie das Zertifikat auf einem Microsoft Windows-Computer. Sie können diesen Test auf einer Arbeitsgruppe oder Domäne ausführen, die einem Windows-Computer beigetreten ist.

> **Tipp:** Dieser Schritt kann verwendet werden, um das CA-Zertifikat auf einem Windows-System zu testen, bevor ein Authentifizierungsobjekt in einem FireSIGHT Management Center erstellt wird.

1. Kopieren Sie das CA-Zertifikat in C:\Certficate oder ein beliebiges Verzeichnis.
2. Führen Sie die Windows-Befehlszeile cmd.exe aus. als Administrator
3. Testen Sie das CA-Zertifikat mit dem Befehl Certutil

```
cd c:\Certificate

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

Wenn der Windows-Computer bereits der Domäne beigetreten ist, sollte sich das Zertifizierungsstellenzertifikat im Zertifikatsspeicher befinden, und es sollte kein Fehler in cacert.test.txt auftreten. Wenn sich der Windows-Computer jedoch in einer Arbeitsgruppe befindet, wird möglicherweise eine der beiden Meldungen angezeigt, je nachdem, ob CA-Zertifikate in der Liste der vertrauenswürdigen Zertifizierungsstellen vorhanden sind.

a) Die CA ist vertrauenswürdig, aber keine CRL für die CA gefunden:

```
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) Die CA ist nicht vertrauenswürdig:

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

Wenn Sie wie unten beschrieben weitere FEHLER-Meldungen erhalten, wenden Sie sich an Ihren Systemadministrator, um das Problem mit der AD LDS- und der Zwischenzeitanzeige zu beheben. Diese Fehlermeldungen weisen auf eine falsche Zertifizierung, auf das Thema im Zertifizierungsstellenzertifikat, auf fehlende Zertifikatsketten usw. hin.

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

Schritt 6: Nachdem Sie bestätigt haben, dass das CA-Zertifikat gültig ist und den Test in Schritt 5 bestanden hat, laden Sie das Zertifikat in das Authentifizierungsobjekt hoch, und führen Sie den Test aus.

Schritt 7: Speichern Sie das Authentifizierungsobjekt, und wenden Sie die Systemrichtlinie erneut an.