Verificatie van verificatieobject via FireSIGHT System voor Microsoft AD-verificatie via SSL/TLS

Inhoud

Inleiding

U kunt een FireSIGHT Management Center configureren om externe gebruikers van de Active Directory LDAP toegang tot de web user interface en CLI te authenticeren. Dit artikel schrijft over het configureren, testen, probleemoplossing van verificatieobject voor Microsoft AD-verificatie via SSL/TLS.

Voorwaarden

Cisco raadt u aan kennis te hebben over gebruikersbeheer en extern verificatiesysteem via FireSIGHT Management Center.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Procedure

Stap 1. Configureer de verificatieobject zonder SSL/TLS-encryptie.

1. Configureer de verificatieobject zoals u dat normaal zou doen. De basisconfiguratiestappen voor gecodeerde en niet gecodeerde authenticatie zijn hetzelfde.
2. Bevestig dat het verificatieobject werkt en dat gebruikers van de ADSL niet-versleuteld kunnen authenticeren.

Stap 2. Test het verificatieobject via SSL en TLS zonder CA-certificaat.

Test het authenticatieobject via SSL en TLS zonder CA cert. Als u een probleem tegenkomt, raadpleegt u uw systeembeheerder om dit probleem op de AD LDS-server op te lossen. Indien

een certificaat eerder naar het authenticatieobject is geüpload, selecteert u "**certificaatnummer is geladen (selecteer dit om het geladen certificaat vrij te geven)**" om het certificaat te verwijderen en nogmaals te testen.

Als de verificatieobject niet werkt, raadpleeg dan uw systeembeheerder om de AD LDS SSL/TLS-configuratie te controleren voordat u naar de volgende stap gaat. U kunt echter de volgende stappen blijven uitvoeren om de verificatieobject verder te testen met CA-certificaat.

Stap 3. Download **Base64** CA Cert.

1. Aanmelden bij de AD LDS.
2. Open een webbrowser en sluit deze aan op http://localhost/certsrv
3. Klik op "**Een CA-certificaat, certificeringsketen of CRL downloaden**"
4. Kies de CA-cert in de lijst "**CA-certificaat**" en "**Base64**" van "**coderingsmethode**"
5. Klik op de link "**CA-certificaat downloaden**" om het bestand certnew.cer te downloaden.

Stap 4. Controleer de **Onderwerp**-waarde in de cert.

1. Klik met de rechtermuisknop op certnew.cer en selecteer **Openen**.
2. Klik op het tabblad **Details** en selecteer **<All>** in de vervolgkeuzemogelijkheden **tonen**
3. Controleer de waarde voor elk veld. Controleer in het bijzonder of de **Onderwerp**-waarde overeenkomt met de naam van de **primaire server** van het verificatieobject.

Stap 5. Test de machine van Microsoft Windows. U kunt deze test uitvoeren op een werkgroep of een domein dat aangesloten is op Windows machine.

> **Tip**: Deze stap kan worden gebruikt om CA Certificate op een Windows systeem te testen voordat u Verificatieobject maakt op een FireSIGHT Management Center.

1. Kopieer de CA cert naar C:\Certficate of een voorkeursmap.
2. Start Windows-opdrachtregel, cmd.exe. als beheerder
3. Test het CA-certificaat met Certutil opdracht

```
cd c:\Certificate

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

Als de Windows machine al is aangesloten bij het domein, zou het CA certificaat in de certificaatopslag moeten zijn en er zou geen fout in cacert.test.txt moeten zijn. Als de Windows machine echter op een werkgroep is, kunt u een van de twee berichten zien, afhankelijk van het bestaan van een CA-cert in de vertrouwde CA-lijst.

a. De CA is betrouwbaar maar geen CRL gevonden voor de CA:

```
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 is niet vertrouwd:

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

Als u andere FOUTmeldingen zoals hieronder krijgt, raadpleegt u uw System Admin om het probleem op te lossen via AD LDS en Intermediate CA. Deze foutmeldingen zijn een indicatie van onjuist Cert, onderwerp van de CA-cert, ontbrekende certificatenketen, enz.

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

Stap 6. Zodra u het CA-certificaat bevestigt is geldig en de test in Stap 5 hebt doorlopen, uploadt u de cert naar het verificatieobject en voert u de test uit.

Stap 7. Sla de verificatieobject op en pas het systeembeleid opnieuw toe.