Verifica dell'oggetto di autenticazione sul sistema FireSIGHT per l'autenticazione AD Microsoft su SSL/TLS

Sommario

Introduzione

Èpossibile configurare un centro di gestione FireSIGHT per consentire agli utenti LDAP di Active Directory esterni di autenticare l'accesso all'interfaccia utente Web e alla CLI. In questo articolo viene descritto come configurare, verificare e risolvere i problemi relativi all'oggetto Autenticazione per l'autenticazione di Microsoft AD tramite SSL/TLS.

Prerequisito

Cisco raccomanda la conoscenza della gestione degli utenti e del sistema di autenticazione esterna su FireSIGHT Management Center.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura

Passaggio 1. Configurare l'oggetto di autenticazione senza crittografia SSL/TLS.

1. Configurare l'oggetto di autenticazione normalmente. La configurazione di base per l'autenticazione crittografata e non crittografata è la stessa.
2. Confermare che l'oggetto di autenticazione funziona e che gli utenti LDAP di Active Directory possano autenticare i messaggi non crittografati.

Passaggio 2. Eseguire il test dell'oggetto di autenticazione su SSL e TLS senza certificato CA.

Verificare l'oggetto di autenticazione tramite SSL e TLS senza certificato CA. Se si verifica un problema, rivolgersi all'amministratore di sistema per risolverlo nel server AD LDS. Se un

certificato è stato precedentemente caricato nell'oggetto di autenticazione, selezionare "**Certificato caricato (selezionare per cancellare il certificato caricato)**" per cancellare il certificato e provare di nuovo l'oggetto attivazione.

Se l'oggetto di autenticazione ha esito negativo, consultare l'amministratore di sistema per verificare la configurazione SSL/TLS di AD LDS prima di procedere con il passaggio successivo. È comunque possibile continuare con i passaggi seguenti per verificare ulteriormente l'oggetto di autenticazione con il certificato CA.

Passaggio 3. Scaricare il certificato CA **Base64**.

1. Accedere ad AD LDS.
2. Aprire un browser e connettersi a http://localhost/certsrv
3. Fare clic su "**Scarica un certificato CA, una catena di certificati o un CRL**"
4. Scegliere il certificato CA dall'elenco "**Certificato CA**" e "**Base64**" da "**Metodo di codifica**"
5. Fare clic sul collegamento "**Scarica certificato CA**" per scaricare il file certnew.cer.

Passaggio 4. Verificare il valore **Subject** nel certificato.

1. Fare clic con il pulsante destro del mouse su certnew.cer e selezionare **apri**.
2. Fare clic sulla scheda **Details** (Dettagli) e selezionare **<All>** (Tutto) dall'elenco a discesa **Show** (Mostra)
3. Verificare il valore di ogni campo. In particolare, verificare che il valore **Subject** corrisponda al nome dell'**host server primario** dell'oggetto Authentication.

Passaggio 5. Verificare il certificato su un computer con Microsoft Windows. È possibile eseguire questo test su un computer Windows aggiunto a un gruppo di lavoro o a un dominio.

> **Suggerimento**: Questo passaggio può essere utilizzato per verificare il certificato CA su un sistema Windows prima di creare un oggetto di autenticazione su un centro di gestione FireSIGHT.

1. Copiare il certificato CA in C:\Certficate o in qualsiasi directory preferita.
2. Eseguire la riga di comando di Windows, cmd.exe. come amministratore
3. Verificare il certificato CA con il comando Certutil

```
cd c:\Certificate

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

Se il computer Windows è già stato aggiunto al dominio, il certificato CA deve trovarsi nell'archivio certificati e non deve essere presente alcun errore in cacert.test.txt. Tuttavia, se il computer Windows si trova in un gruppo di lavoro, è possibile che uno dei due messaggi venga visualizzato a seconda dell'esistenza del certificato CA nell'elenco delle CA attendibili.

r. La CA è attendibile ma non è stato trovato alcun CRL per la 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 non attendibile:

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

Se vengono visualizzati altri messaggi di ERRORE come quelli riportati di seguito, rivolgersi all'amministratore di sistema per risolvere il problema in AD LDS e nella CA intermedia. Questi messaggi di errore sono indicativi di un certificato errato, di un oggetto nel certificato CA, di una catena di certificati mancante e così via.

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

Passaggio 6. Dopo aver confermato la validità del certificato CA e aver superato il test illustrato al passaggio 5, caricare il certificato nell'oggetto di autenticazione ed eseguire il test.

Passaggio 7. Salvare l'oggetto di autenticazione e riapplicare il criterio di sistema.