Vérification de l'objet d'authentification sur FireSIGHT System pour l'authentification Microsoft AD sur SSL/TLS

Contenu

Introduction

Vous pouvez configurer FireSIGHT Management Center pour permettre aux utilisateurs LDAP Active Directory externes d'authentifier l'accès à l'interface utilisateur Web et à l'interface de ligne de commande. Cet article explique comment configurer, tester et dépanner l'objet d'authentification pour l'authentification Microsoft AD sur SSL/TLS.

Prérequis

Cisco recommande que vous ayez des connaissances sur la gestion des utilisateurs et le système d'authentification externe sur FireSIGHT Management Center.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Procédure

Étape 1. Configurer l'objet d'authentification sans chiffrement SSL/TLS.

1. Configurez l'objet d'authentification comme vous le feriez normalement. Les étapes de configuration de base pour l'authentification chiffrée et non chiffrée sont les mêmes.
2. Confirmez que l'objet d'authentification fonctionne et que les utilisateurs LDAP AD peuvent authentifier des données non chiffrées.

Étape 2. Testez l'objet d'authentification sur SSL et TLS sans certificat CA.

Testez l'objet d'authentification sur SSL et TLS sans certificat CA. Si vous rencontrez un problème, consultez votre administrateur système pour résoudre ce problème sur le serveur AD LDS. Si un certificat a déjà été téléchargé vers l'objet d'authentification, sélectionnez "**Certificat a**

été chargé (Sélectionner pour effacer le certificat chargé)" pour effacer le certificat et tester à nouveau l'AO.

Si l'objet d'authentification échoue, consultez votre administrateur système pour vérifier la configuration SSL/TLS d'AD LDS avant de passer à l'étape suivante. Cependant, n'hésitez pas à poursuivre les étapes suivantes pour tester l'objet d'authentification avec le certificat CA.

Étape 3. Télécharger **Base64** CA Cert.

1. Connectez-vous à AD LDS.
2. Ouvrez un navigateur Web et connectez-vous à http://localhost/certsrv
3. Cliquez sur "**Télécharger un certificat CA, une chaîne de certificats ou une liste de révocation de certificats**"
4. Choisissez le certificat CA dans la liste "**Certificat CA**" et "**Base64**" dans "**Méthode de codage**"
5. Cliquez sur le lien "**Télécharger le certificat d'autorité de certification**" pour télécharger le fichier certnew.cer.

Étape 4. Vérifiez la valeur **Objet** dans le certificat.

1. Cliquez avec le bouton droit sur le certnew.cer et sélectionnez **ouvrir**.
2. Cliquez sur l'onglet **Détails** et sélectionnez **<Tout>** dans les options **Afficher**.
3. Vérifiez la valeur de chaque champ. En particulier, vérifiez que la valeur **Subject** correspond au nom **Hôte du serveur principal** de l'objet d'authentification.

Étape 5. Testez le certificat sur une machine Microsoft Windows. Vous pouvez effectuer ce test sur un ordinateur Windows joint à un groupe de travail ou à un domaine.

> **Astuce** : Cette étape peut être utilisée pour tester le certificat d'autorité de certification sur un système Windows avant de créer un objet d'authentification sur FireSIGHT Management Center.

1. Copiez le certificat de l'autorité de certification sur C:\Certficate ou tout répertoire préféré.
2. Exécutez la ligne de commande Windows, cmd.exe. en tant qu'administrateur
3. Tester le certificat CA avec la commande Certutil

```
cd c:\Certificate

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

Si l'ordinateur Windows est déjà joint au domaine, le certificat de l'autorité de certification doit se trouver dans le magasin de certificats et il ne doit pas y avoir d'erreur dans cacert.test.txt. Cependant, si l'ordinateur Windows se trouve sur un groupe de travail, vous pouvez voir l'un des deux messages selon l'existence d'un certificat d'autorité de certification dans la liste des autorités de certification approuvées.

a. L'autorité de certification est approuvée, mais aucune liste de révocation de certificats n'a été trouvée pour l'autorité de certification :

```
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. L'autorité de certification n'est pas fiable :

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

Si vous recevez d'autres messages d'ERREUR comme ci-dessous, veuillez consulter votre administrateur système pour résoudre le problème sur AD LDS et l'autorité de certification intermédiaire. Ces messages d'erreur indiquent un certificat incorrect, un sujet dans le certificat CA, une chaîne de certificats manquante, etc.

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

Étape 6. Une fois que vous avez confirmé la validité du certificat CA et que vous avez réussi le test à l'étape 5, téléchargez le certificat dans l'objet d'authentification et exécutez le test.

Étape 7. Enregistrez l'objet d'authentification et réappliquez la stratégie système.