Contenu

Introduction

Vous pouvez configurer un centre de Gestion de FireSIGHT pour permettre aux utilisateurs externes de LDAP de Répertoire actif pour authentifier l'accès à l'interface utilisateur d'utilisateur web et au CLI. Cet article discutent comment configurer, tester, dépannent l'objet d'authentification pour l'authentification d'AD de Microsoft au-dessus de SSL/TLS.

Condition préalable

Cisco recommande que vous ayez la connaissance sur le système de gestion des utilisateurs et d'authentification externe au centre de Gestion de FireSIGHT.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Procédure

Étape 1. Configurez l'objet d'authentification sans cryptage SSL/TLS.

1. Configurez l'objet d'authentification comme vous normalement. Les étapes de configuration de base pour l'authentification chiffrée et décryptée sont identiques.
2. Confirmez que l'objet d'authentification fonctionne et des utilisateurs de LDAP d'AD peut authentifier décrypté.

Étape 2. Testez l'objet d'authentification au-dessus du SSL et le TLS sans certificat de CA.

Testez l'objet d'authentification au-dessus du SSL et le TLS sans CERT CA. Si vous rencontrez une question, consultez s'il vous plaît avec votre admin de système pour résoudre ce problème sur le serveur de l'AD LDS. Si un certificat ont été précédemment téléchargés à l'objet d'authentification, sélectionnez s'il vous plaît le « **certificat a été chargé (choisi pour effacer le certificat chargé)** » pour effacer le CERT et pour tester l'ao de nouveau.

Si l'objet d'authentification échoue, veuillez consultent votre admin de système pour vérifier la configuration de l'AD LDS SSL/TLS avant que vous passiez à l'étape suivante. Cependant, sentez-vous s'il vous plaît libre de continuer aux étapes suivantes à tester l'objet d'authentification plus loin avec le certificat de CA.

Étape 3. CERT du téléchargement **Base64** CA.

1. Procédure de connexion à l'AD LDS.
2. Ouvrez un navigateur Web et connectez à `http://localhost/certsrv`
3. Cliquez sur en fonction le « **téléchargement un certificat de CA, une chaîne de certificat, ou un CRL** »
4. Choisissez le CERT CA du « **certificat de CA** » liste et « **Base64"** « de la **méthode de codage** »
5. Cliquez sur en fonction le lien « de **certificat de CA de téléchargement** » pour télécharger le fichier de `certnew.cer`.

Étape 4. Vérifiez la valeur **soumise** dans le CERT.

1. Le clic droit sur `certnew.cer` et sélectionnent **ouvert**.
2. Cliquez sur en fonction l'onglet de **détails** et sélectionnez le **<All> des** options de déroulant d'**exposition**
3. Vérifiez la valeur pour chaque champ. En particulier, vérifiez que la valeur de **sujet** apparie le nom **primaire d'hôte de serveur de l'**objet d'authentification.

Étape 5. Testez le CERT sur un ordinateur de Microsoft Windows. Vous pouvez réaliser cet essai sur un groupe de travail ou un ordinateur Windows joint par domaine.

> **Conseil** : Cette étape peut être utilisée pour tester le certificat de CA sur un système Windows avant de créer l'objet d'authentification à un centre de Gestion de FireSIGHT.

1. Copiez le CERT CA sur `C:\Certficate` ou n'importe quel répertoire préféré.
2. Exécutez la ligne de commande Windows, `cmd.exe en tant qu'`administrateur
3. Testez le certificat de CA avec la commande de Certutil

```
cd c:\Certificate

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

Si l'ordinateur Windows est déjà joint le domaine, le certificat de CA devrait être dans la mémoire de certificat et il ne devrait y avoir aucune erreur dans `cacert.test.txt`. Cependant, si l'ordinateur Windows est sur un groupe de travail, vous pouvez voir un des deux messages selon l'existence du CERT CA dans la liste de confiance CA.

a. Le CA est de confiance mais CRL ne fonde pas pour le 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. Le CA n'est pas fait confiance :

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

Si vous recevez n'importe quels autres messages d'erreur comme ci-dessous, consultez s'il vous plaît avec votre admin de système pour résoudre le problème sur l'AD LDS et l'intermédiaire CA. Ces messages d'erreur sont des indicatifs du CERT incorrect, du sujet dans le CERT CA, de la

chaîne de certificat manquante, etc.

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

Étape 6. Une fois que vous confirmez le CERT CA est valide et a passé le test dans l'étape 5, télécharge le CERT à l'objet d'authentification et exécute le test.

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