驗證通過SSL/TLS進行Microsoft AD身份驗證的FireSIGHT系統上的身份驗證對象

目錄

簡介

您可以配置FireSIGHT管理中心，以允許外部Active Directory LDAP使用者驗證對Web使用者介面和CLI的訪問。本文討論如何配置、測試和排除Microsoft AD Authentication Over SSL/TLS的身份驗證對象故障。

必備條件

思科建議您瞭解FireSIGHT管理中心的使用者管理和外部身份驗證系統。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

程式

步驟1.配置不帶SSL/TLS加密的身份驗證對象。

1. 按照正常方式配置身份驗證對象。加密和非加密身份驗證的基本配置步驟相同。
2. 確認身份驗證對象正在工作，並且AD LDAP使用者可以進行未加密的身份驗證。

步驟2.在不使用CA證書的情況下通過SSL和TLS測試身份驗證對象。

在不使用CA證書的情況下，通過SSL和TLS測試身份驗證對象。如果您遇到問題，請諮詢您的系統管理員，在AD LDS伺服器上解決此問題。如果之前已將證書上傳到身份驗證對象，請選擇「證書已載入（選擇以清除載入的證書）」以清除證書並再次測試AO。

如果身份驗證對象失敗，請諮詢您的系統管理員以驗證AD LDS SSL/TLS配置，然後再繼續下一步。但是，請隨意繼續執行以下步驟，以便使用CA證書進一步測試身份驗證對象。

步驟3.下**載Base**64 CA證書。

1. 登入AD LDS。

2. 開啟Web瀏覽器並連線到http://localhost/certsrv
3. 按一下「**Download a CA certificate， certificate chain， or CRL**」
4. 從「**CA Certificate**」列**表中選擇CA**憑證，從「**Encoding Method**」中選擇「**Base64**」
5. 按一下「**Download CA certificate**」連結，下載certnew.cer檔案。

步驟4.驗證cert中的**Subject**值。

1. 按一下右鍵certnew.cer，然後選擇**open**。
2. 按一下**Details**頁籤，然後從**Show**下拉選項中選擇**<All>**
3. 驗證每個欄位的值。具體來說，驗證**Subject**值是否與身份驗證對象的**Primary Server Host** name匹配。

步驟5.在Microsoft Windows電腦上測試證書。可以在加入工作組或域的Windows電腦上執行此測試。

提示：在FireSIGHT管理中心上建立身份驗證對象之前，此步驟可用於在Windows系統上測試CA證書。

1. 將CA憑證複製到C:\Certficate或任何首選目錄。
2. 運行Windows命令列cmd.exe。作為管理員
3. 使用Certutil指令測試CA憑證

```
cd c:\Certificate

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

如果Windows電腦已加入域，則CA證書應位於證書儲存中，並且cacert.test.txt中應該沒有錯誤。但是，如果Windows電腦在工作組中，您可能會看到這兩種消息之一，具體取決於受信任CA清單中是否存在CA證書。

a.CA受信任，但找不到CA的CRL:

```
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不受信任：

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

如果您收到以下任何其它錯誤消息，請諮詢您的系統管理員，解決AD LDS和中繼CA上的問題。這些錯誤消息表示Cert不正確、CA證書中的主題、缺少證書鏈等。

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

步驟6.確認CA證書有效並已通過步驟5中的測試後，將證書上傳到身份驗證對象並運行測試。

步驟7.儲存身份驗證對象並重新應用系統策略。