9.5及更新的AsyncOS for Email Security升級，使用較舊的證書(MD5)通訊TLSv1.2失敗

目錄

簡介

本文檔介紹在思科郵件安全裝置(ESA)上升級到AsyncOS for Email Security 9.5版或更高版本後，如果遇到TLS通訊問題或訪問Web介面，需要應用的必要步驟。

舊證書(MD5)導致9.5 AsyncOS上的TLSv1.2通訊失敗，以便進行郵件安全升級和更新版本

> **附註**：下面列出了適用於裝置上當前演示證書的解決方法。但是，以下步驟可能也適用於任何MD5簽名證書。

升級到AsyncOS for Email Security 9.5及更新版本後，任何仍在使用並申請交付、接收或LDAP的舊版IronPort演示證書在嘗試通過TLSv1/TLSv1.2與某些域通訊時可能會遇到錯誤。 TLS錯誤將導致所有入站或出站會話失敗。

如果證書應用到HTTPS介面，則現代Web瀏覽器將無法訪問裝置的網路介面。

郵件日誌應類似於以下示例：

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

此錯誤是由應用於舊證書（即MD5）的簽名演算法引起的；但是，與連線裝置/瀏覽器關聯的證書僅支援基於SHA簽名的演算法。雖然具有MD5簽名的較舊演示證書在裝置上與新的基於SHA的演示證書同時存在，但上述錯誤僅在基於MD5簽名的證書應用於指定部分（如接收、交付等）時才顯現

以下是從裝置的cli提取的示例，該裝置除具有新的演示證書外，還同時具有舊的MD5證書(注意：較新的憑證(Demo)應該是SHA演演算法的較新版本，且到期日期比較舊的演示憑證更長):

```
List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
delivery_  IronPort Appliance D  IronPort Appliance D  Active          303 days
```

```
https_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
ldaps_cer  IronPort Appliance D  IronPort Appliance D  Active          303 days
receiving  IronPort Appliance D  IronPort Appliance D  Valid           303 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         3218 days
```

糾正措施

1. 導航到Web(UI):**Network > Certificates**
2. 確認您目前已安裝舊證書以及新的SHA演示證書。
3. 根據較舊的演示證書的應用位置，將其替換為新的演示證書。

通常，在以下部分可以找到應用了這些證書：

- **網路>監聽程式>監聽程式名稱>證書**
- **郵件策略>目標控制>編輯全域性設定>證書**
- **Network > IP Interface > Choose interface associated with GUI access > HTTPS Certificate**
- **系統管理> LDAP >編輯設定>證書**

4.替換所有證書後，從命令列驗證TLS通訊現在是否成功。

使用TLSv1.2協商的工作中TLS通訊的示例：

```
Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1)
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

CLI糾正操作（如果無法訪問GUI）

可能需要在為HTTPS服務啟用證書的每個IP介面上修改證書。 要修改介面使用的證書，請在CLI上運行以下命令：

1. 鍵入**interfaceconfig**。
2. 選擇**edit**。
3. 輸入要編輯的介面的編號。
4. 使用return鍵接受所提出每個問題的當前設定。 當顯示要應用的證書選項時，選擇演示證書：
    1.
    ```
    1. Ironport Demo Certificate
    2. Demo
    Please choose the certificate to apply:
    [1]> 2

    You may use "Demo", but this will not be secure.
    Do you really wish to use the "Demo" certificate? [N]> Y
    ```
5. 完成設定提示步驟，直到所有配置問題都完成。
6. 使用return鍵退出到主CLI提示符。
7. **使用**commit儲存對配置的更改。

注意：請記住，在更改介面上正在使用的證書後，提交更改。

相關資訊

- ESA上的TLS綜合設定指南

- Cisco Email Security Appliance — 最終使用手冊
- 思科安全管理裝置 — 最終使用手冊
- 技術支援與文件 - Cisco Systems