在兩個SWA之間遷移配置

目錄

簡介

本檔案介紹將組態從安全網路裝置(SWA)還原到另一個的過程。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)
- 對SWA的管理訪問
- 安全管理裝置(SMA)的管理訪問許可權
- 訪問思科軟體許可門戶或SWA許可證檔案
- Active Directory具有將SWA加入域和建立DNS記錄的特權使用者訪問許可權

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

開始之前

在本文中，我們概述了從源SWA遷移到目標SWA的步驟。此表列出了每個系統的規格。

	源SWA	目標SWA
型號	S396	S100v
版本	15.5.0-710	15.5.0-710
授權	智慧許可證	智慧許可證
Active Directory	已加入	已加入
與身份服務引擎(ISE)整合	是	是
網路介面卡(NIC)數量	5	5
HTTPS解密	已啟用自簽名證書	已啟用自簽名證書

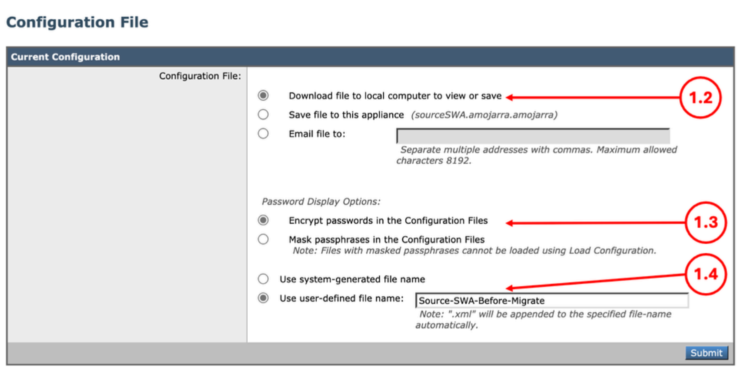
透通重新導向	WCCP	WCCP
由SMA管理	是	是
外部日誌伺服器	SCP推送	SCP推送
高可用性	已啟用	已啟用

附註：安裝新的虛擬SWA時，請務必確保Cisco推薦的所有網路介面都存在於虛擬機器(VM)上並已在虛擬機器上配置。 介面可以保持斷開連線，但是它們必須在VM中可用。

將SWA從一台裝置遷移到另一台裝置時，有兩種可能情況：
[案例1]更換現有SWA:原始SWA已停用，並且目標SWA的IP地址與源SWA相同。
[案例2]新增新的SWA:當配置新的SWA時，原始SWA仍然處於服務狀態。

準備和備份源SWA

使用以下步驟從源SWA收集必要的檔案和配置：

步驟1.匯出配置檔案	步驟1.1.從GUI導航到System Administration並選擇Configuration File。 步驟1.2.確保選中「Download file to local computer to view or save（將檔案下載到本地電腦檢視或儲存）」。 步驟1.3.在組態檔中選擇Encrypt passwords 步驟1.4.（可選）選擇配置檔案的名稱。 步驟1.5.按一下Submit。  映像 — 匯出配置檔案

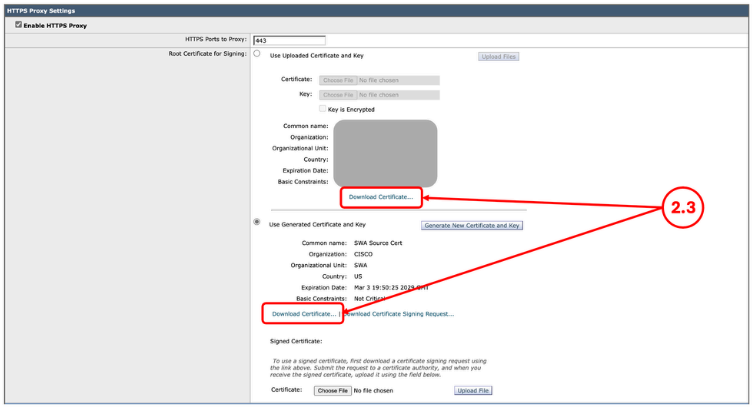
步驟2.匯出解密證書

附註：如果已停用HTTPS解密，請跳至步驟3。

步驟2.1.在GUI中，導覽至Security Services，然後按一下HTTPS Proxy。

步驟2.2.按一下Edit Settings。

步驟2.3.通過按一下Download Certificate...下載HTTPS解密證書 連結。



映像 — HTTPS解密證書

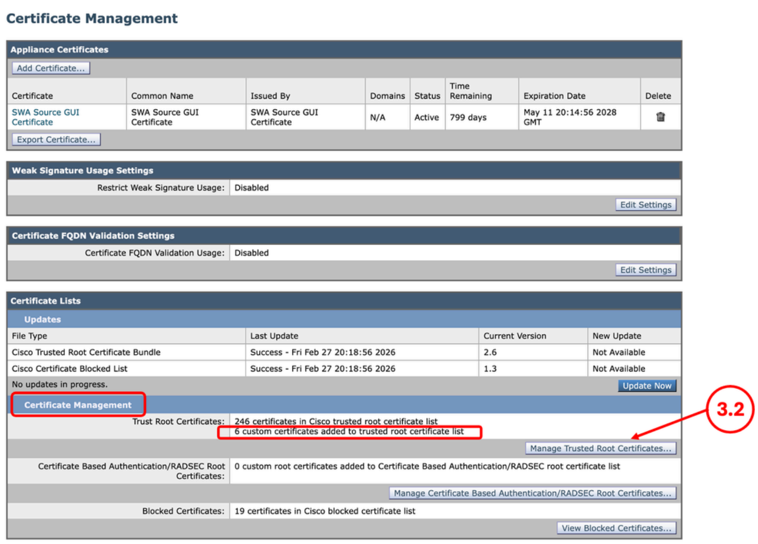
附註：在此範例中，說明兩種型別的HTTPS解密憑證；但是，在您的網路中，只能部署一種型別。

步驟3.匯出自定義信任根證書

附註：如果在SWA上沒有新增自定義受信任的根證書，請跳至步驟4。

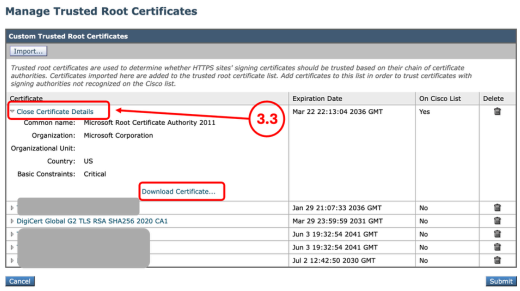
步驟3.1.在GUI中，導覽至Network，然後按一下Certificate Management。

步驟3.2.在Certificate Management部分，點選Manage Trusted Root Certificates。



映像 — 管理受信任的根證書

步驟3.3.按一下每個自定義受信任的根證書，然後按一下下載證書......



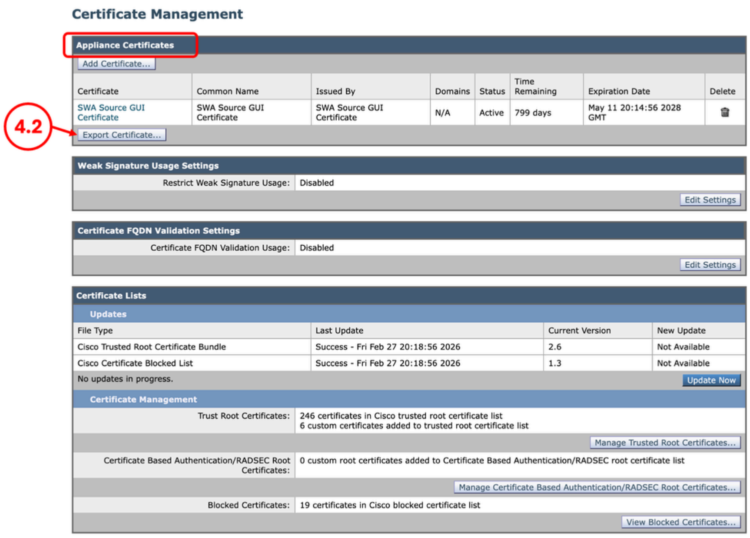
映像 — 下載受信任的根證書

步驟4.匯出GUI證書

附註：如果使用的是內建GUI證書，請跳至步驟5。

步驟4.1.在GUI中導覽至Network，然後按一下Certificate Management。

步驟4.2.在Appliance Certificates部分，點選Export Certificate。



映像 — 匯出GUI證書

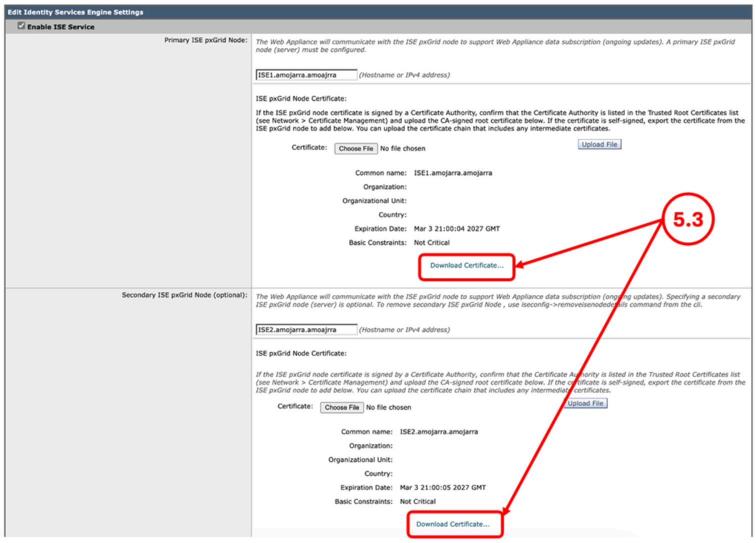
步驟5.匯出ISE證書

附註：如果沒有SWA、ISE整合，請跳至步驟6。

步驟5.1.在GUI中，導覽至Network，然後按一下Identity Services Engine。

步驟5.2.按一下「Edit Settings」。

步驟5.3.下載所有可用的證書。

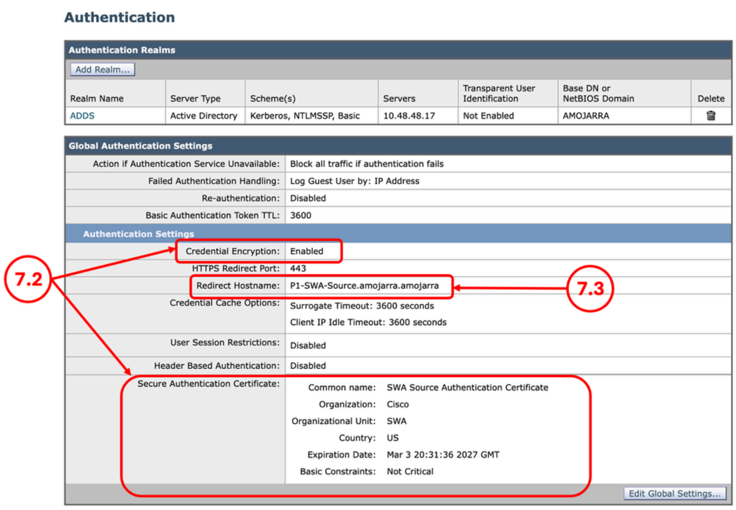
<table>
<tr>
<td></td>
<td>


映像 — 下載ISE證書
</td>
</tr>
<tr>
<td>步驟6.許可證/功能</td>
<td>
步驟6.1.在GUI中，導覽至System Administration，然後按一下Licenses或Features，具體取決於您使用的許可證型別。

步驟6.2.擷取許可證/功能的截圖。
</td>
</tr>
<tr>
<td>步驟7.驗證重新導向憑證</td>
<td>
步驟7.1.在GUI中，導覽至Network，然後按一下Authentication。

步驟7.2.如果Credential Encryption已啟用，請確保您擁有憑證和金鑰。

步驟7.3.獲取當前配置的截圖。



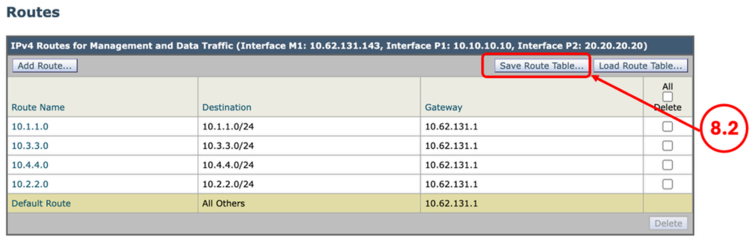
映像 — 身份驗證證書

附註：無法從GUI下載身份驗證證書。
</td>
</tr>
</table>

<table>
<tr>
<td>步驟8.匯出靜態路由

附註：如果計畫對目標SWA使用相同的網路配置和IP地址，請跳至步驟10。</td>
<td>步驟8.1.在GUI中導覽至Network，然後按一下Routes。

步驟8.2.對於每個路由表，按一下Save Route Table。



影象 — 匯出路由表</td>
</tr>
<tr>
<td>步驟9. DNS設定

附註：如果計畫對目標SWA使用相同的網路配置和IP地址，請跳至步驟10。</td>
<td>步驟9.1.在GUI中，導覽至Network，然後按一下DNS。

步驟9.2.擷取DNS配置的截圖。</td>
</tr>
</table>

準備目標SWA

<table>
<tr>
<td>步驟10.安裝虛擬SWA

附註：如果目標SWA是物理的，則可以跳至步驟11。</td>
<td>步驟10.1.使用以下指南安裝虛擬SWA:

• 在Vmware ESXi上安裝安全Web裝置
• 在Microsoft Hyper-V上安裝安全網路裝置

步驟10.2.確保新SWA具有推薦的網路訪問許可權：

• 為安全Web裝置配置防火牆</td>
</tr>
<tr>
<td>步驟11.初始SWA設定</td>
<td>步驟11.1.配置IP地址。

步驟11.2.配置預設網關。

步驟11.3.配置DNS伺服器。

步驟11.4.許可裝置。

步驟11.5.啟用功能。

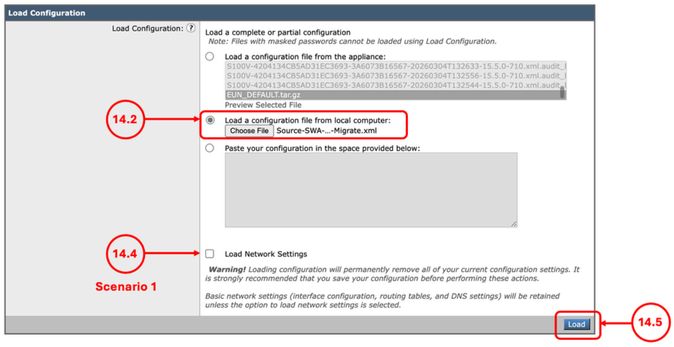
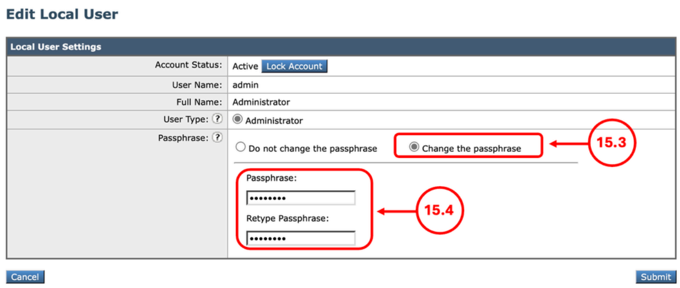
步驟11.6.運行系統設定嚮導。

您可以在本文中找到詳細步驟：Secure Web Appliance Initial Setup</td>
</tr>
</table>

步驟12.清理配置檔案 附註：如果您未將ISE與SWA整合，則可以跳至步驟13。	步驟12.1.查看本文的修復錯誤(Fixing Errors)部分，從XML備份檔案中刪除ISE證書配置。

將配置檔案匯入目標SWA

步驟13.匯入自定義受信任的根證書 附註：如果未使用任何自定義受信任的根證書，請跳至步驟14。	步驟13.1。在GUI中，導覽至Network，然後按一下Certificate Management。 步驟13.2.在Certificate Management部分，點選Manage Trusted Root Certificates。 步驟13.3.單擊Import。 步驟13.4.上傳先前在步驟3中下載的憑證。 注意：如果根證書和中間證書都可用，則首先上傳根CA證書。提交並提交更改後，繼續匯入中間證書。
步驟14.匯入配置檔案	步驟14.1.在GUI中，導覽至System Administration，然後選擇Configuration File。 步驟14.2.在Load Configuration部分，選擇Load a configuration file from local computer。 步驟14.3.單擊Choose File並選擇XML配置檔案。 步驟14.4。如果遷移與場景1匹配，並且必須在新SWA中使用以前的IP地址，請選中Load Network Settings覈取方塊，否則不選擇此選項。 步驟14.5。單擊Load。 步驟14.6.在Confirm Load Configuration快出視窗中單擊Continue。

	 映像 — 匯入配置
步驟15.更改管理員密碼 注意：如果您有源SWA管理密碼，請跳至步驟16。	15.1.在GUI中，導航到System Administration並選擇Users。 15.2.單擊admin用戶名。 15.3.選擇「更改密碼」。 15.4.輸入密碼。 15.5.單擊Submit。  影象 — 更改管理員密碼
步驟16.提交	步驟16.1。現在可以提交更改了。
步驟17.匯入路由 注意：如果在導入配置時載入網路設定，請跳至步驟19。	步驟17.1.在GUI中，導覽至Network，然後按一下Routes。 步驟17.2.按一下每個路由表的載入路由表。 步驟17.3.選擇您在第8步中匯出的檔案。 步驟17.4.按一下Submit。 步驟17.5.提交更改。

<table>
<tr>
<td>步驟18.配置DNS設定

附註：如果在匯入配置時載入Network Settings，請跳至步驟19。</td>
<td>步驟18.1.在GUI中導覽至Network，然後按一下DNS。

步驟18.2。單擊Edit Settings。

步驟18.3.使用步驟9中的截圖

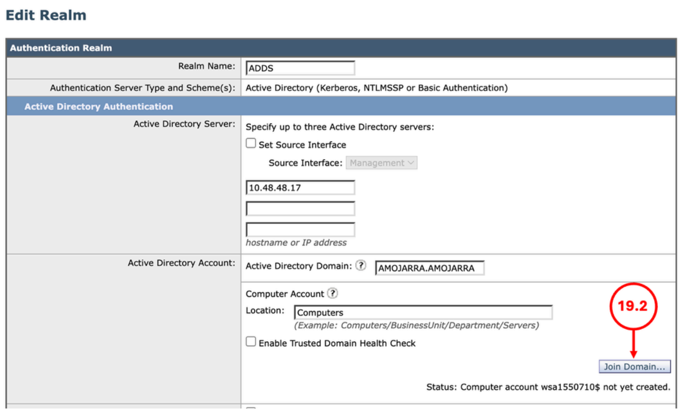
步驟18.4.按一下Submit。

步驟18.5.提交更改。</td>
</tr>
<tr>
<td>步驟19.將SWA加入/重新加入Active Directory</td>
<td>步驟19.1.在GUI中導覽至Network ，然後按一下Authentication。

步驟19.2.按一下身份驗證領域名稱的名稱。

提示：如果為SWA分配了新的IP地址和主機名，請確保在Active Directory DNS服務中建立必要的DNS記錄。

步驟19.2.單擊Join Domain並輸入憑據：

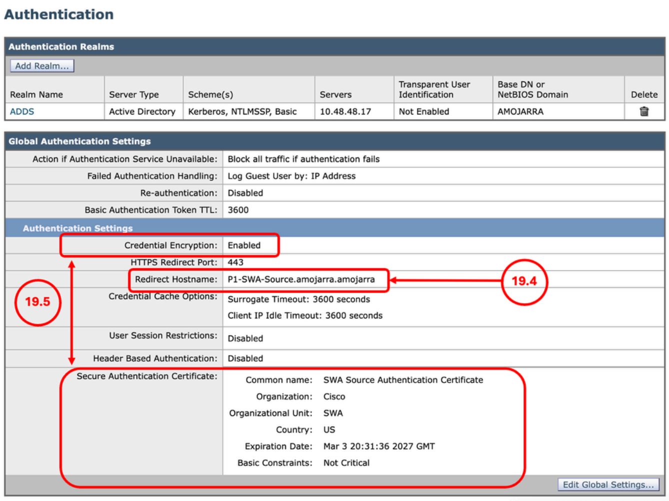


影象 — 加入Active Directory域

步驟19.3.按一下Submit。

步驟19.4.確保重定向主機名正確。

步驟19.5.如果啟用憑證加密，請確保安全驗證憑證正確。</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>


影象 — 身份驗證設定

步驟19.6.提交更改。
</td>
</tr>
<tr>
<td>
步驟20.重新加入SMA

附註：如果SWA不是由SMA管理的，請跳過此步驟。
</td>
<td>
附註：如果沒有替換現有的SWA（場景2），並且已遷移的SWA具有新的IP地址，請將SWA作為新裝置新增到SMA中，並跳過步驟20。

步驟20.1.連線到SMA的CLI。

步驟20.2.運行logconfig。

步驟20.3.輸入HOSTKEYCONFIG。

步驟20.4.鍵入DELETE並按Enter鍵。

步驟20.5.輸入與最近遷移的SWA相關聯的號碼，然後按Enter鍵直至嚮導完成。

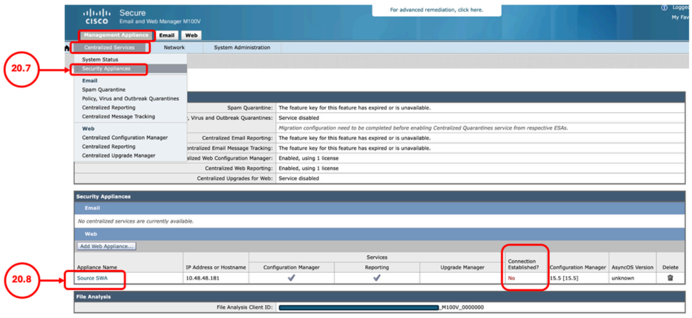
步驟20.6。鍵入commit，然後按Enter鍵儲存更改。

步驟20.7.從SMA GUI導航到Management Appliance。選擇Centralized Services，然後按一下Security Appliances。

步驟20.8.按一下最近遷移的SWA的名稱。

提示：您可以看到Connection
</td>
</tr>
</table>

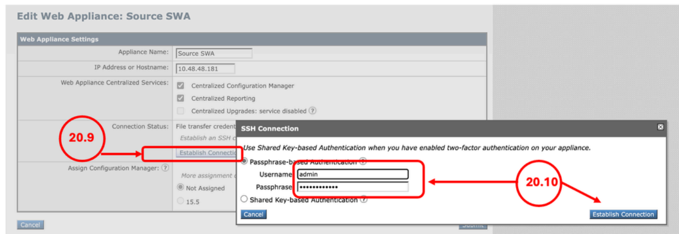
	Established列已設定為No。



映像 — SMA安全裝置狀態

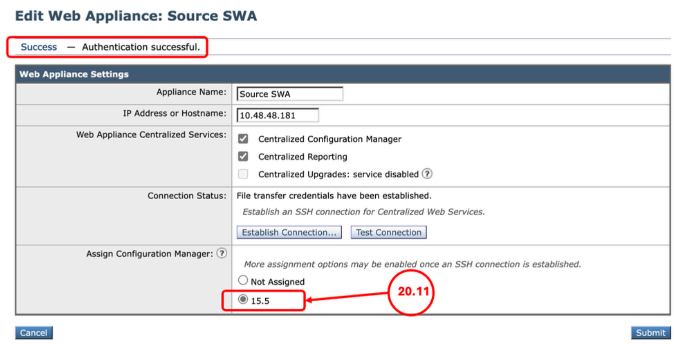
步驟20.9。單擊建立連線。

步驟20.10。輸入Username和Passphrase，然後按一下Establish Connection。



映像 — 建立與SWA的連線

步驟20.11.分配配置管理器。



映像 — 分配Configuration Manager

步驟20.12.提交並提交更改。

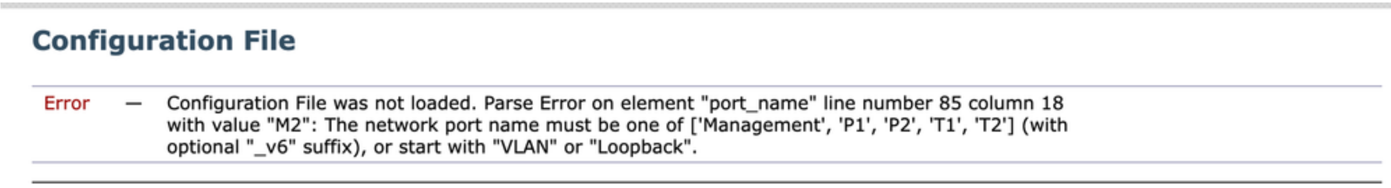
第20.13步(可選)您可以通過向SWA發佈配置進行測試。

提示：SMA保留以前的SWA中的所有報告和跟蹤資料。

修復錯誤

元素port_name上的分析錯誤

網路埠名稱必須是['Management'、'P1'、'P2'、'T1'、'T2']之一:



影象 — 網路介面命名錯誤

```
Error     –     Configuration File was not loaded. Parse Error on element "port_name" line number 85 colu
```

當您從物理SWA遷移到虛擬時，會發生此錯誤。虛擬SWA只有5個NIC，並且M2介面無效。要修復錯誤，請在文本編輯器中編輯XML配置檔案並刪除以下行：

```
M2
```

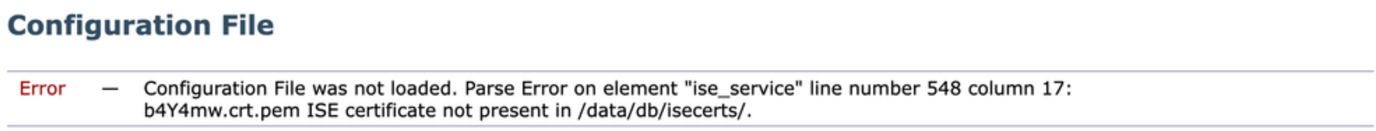
```
M2
```

```
M2
```

```
autoselect
```

```
aa:bb:cc:00:00:00
```

元素ise_service分析錯誤



影象 — ISE證書錯誤

```
Error - Configuration File was not loaded. Parse Error on element "ise_service" line number 548 column
```

由於ISE證書不包括在SWA配置匯出中，並且直接上傳到裝置上，您需要從XML檔案中刪除證書配置，並在成功匯入後，手動配置ISE。要解決此問題，請在文本編輯器中編輯XML配置檔案，並在出現錯誤時搜尋證書名稱(在本示例中，搜尋AA11AA)，然後從配置檔案將其刪除：

```
Before:
```

```
AA11AA
```

```
BB22BB
```

```
After:
```

除了證書名稱，您還需要刪除Web Appliance Client Certificate名稱。

在本示例中，Web Appliance Client Certificate是一個自簽名證書：

```
Before:
```

```
1
```

```
xAcK6T
```

```
After:
```

```
0
```

故障切換在新虛擬SWA上不起作用

如果高可用性（故障轉移）在目標虛擬SWA上無法正常工作，請確保虛擬機器監控程式配置正確。有關詳細資訊，請訪問：確保在VMware環境中具有正確的虛擬WSA HA組功能

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 在Vmware ESXi上安裝安全Web裝置
- 在Microsoft Hyper-V上安裝安全網路裝置
- 安全Web裝置初始設定
- 思科安全電子郵件和網路虛擬裝置安裝指南
- 在Secure Web Appliance中配置自定義URL類別 — Cisco
- 使用安全Web裝置最佳做法
- 為安全Web裝置配置防火牆
- 在安全Web裝置中配置解密證書
- 對安全Web裝置DNS服務進行故障排除
- 確保VMware環境中適當的虛擬WSA HA組功能

關於此翻譯