在两个SWA之间迁移配置

目录

简介

先决条件

- 要求
- 使用的组件

开始使用前

准备和备份源SWA

- 步骤1.导出配置文件
- 步骤2.导出解密证书
- 步骤3.导出自定义信任根证书
- 步骤4.导出GUI证书
- 步骤5.导出ISE证书
- 步骤6.许可证/功能
- 步骤7.身份验证重定向证书
- 步骤8.导出静态路由
- 步骤9. DNS设置

准备目标SWA

- 步骤10.安装虚拟SWA
- 步骤11.初始SWA设置
- 步骤12.清理配置文件

将配置文件导入目标SWA

- 步骤13.导入自定义受信任根证书
- 步骤14.导入配置文件
- 步骤15.更改管理员密码
- 步骤16.提交
- 步骤17.导入路由
- 步骤18.配置DNS设置
- 步骤19.将SWA加入/重新加入Active Directory
- 步骤20.重新加入SMA

修复错误

- 元素port_name的解析错误
- 元素ise_service的解析错误
- 故障转移未在新虚拟SWA上工作

相关信息

简介

本文档介绍将配置从安全Web设备(SWA)恢复到另一个的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的图形用户界面(GUI)
- 对SWA的管理访问
- 安全管理设备(SMA)的管理访问权限
- 访问思科软件许可门户或SWA许可证文件
- Active Directory具有将SWA加入域和创建DNS记录的特权用户访问权限

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

在本文中，我们概述了从源SWA迁移到目标SWA的步骤。此表列出了每个系统的规格。

	源SWA	目标SWA
型号	S396	S100v
version	15.5.0-710	15.5.0-710
许可证	智能许可证	智能许可证
Active Directory	已加入	已加入
与身份服务引擎(ISE)集成	Yes	Yes
网络接口卡(NIC)数量	5	5
HTTPS解密	使用自签名证书启用	使用自签名证书启用

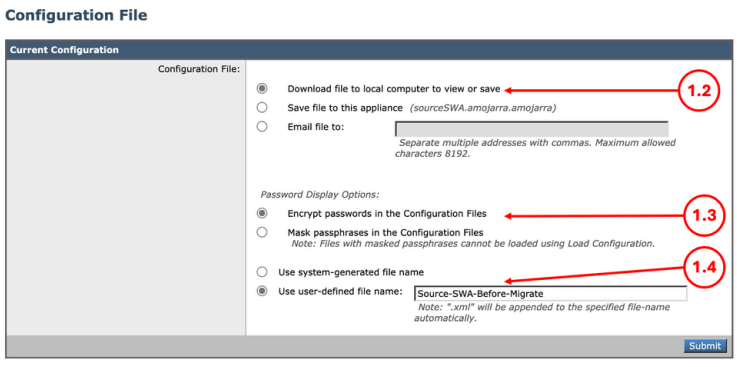
透明重定向	WCCP	WCCP
由SMA管理	Yes	Yes
外部日志服务器	SCP推送	SCP推送
高可用性	启用	启用

注意：请务必确保在安装新的虚拟SWA时，思科推荐的所有网络接口都存在于虚拟机(VM)上，并在虚拟机上进行配置。 接口可以保持断开连接，但它们必须在VM中可用。

将SWA从一台设备迁移到另一台设备时，可能会出现两种情况：
[场景–1]更换现有SWA:原始SWA已停用，目标SWA的IP地址与源SWA相同。
[场景–2]添加新的SWA:配置新的SWA时，原始SWA仍然处于服务状态。

准备和备份源SWA

使用以下步骤从源SWA收集必要的文件和配置：

步骤1.导出配置文件	第1.1步：从GUI中，导航到System Administration并选择Configuration File。 第1.2步：确保已选择将文件下载到本地计算机以查看或保存。 步骤1.3.在配置文件中选择Encrypt password 第1.4步(可选)选择配置文件的名称。 第1.5步。单击提交。  映像 — 导出配置文件

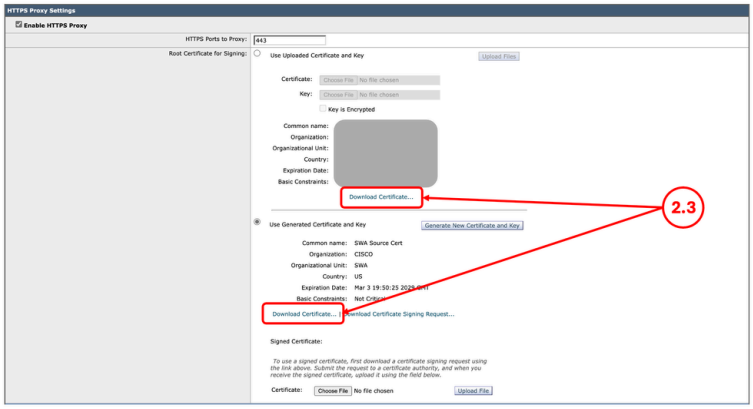
步骤2.导出解密证书

注意：如果HTTPS解密已禁用，请跳至步骤3。

第2.1步：在GUI中，导航到Security Services并点击HTTPS Proxy。

第2.2步。单击编辑设置。

第2.3步：通过点击Download Certificate...下载HTTPS解密证书 链接。



映像 — HTTPS解密证书

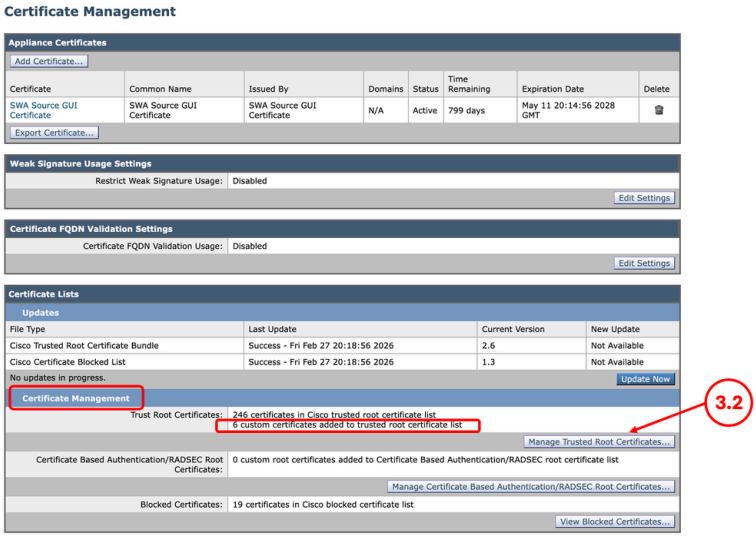
注意：在本例中，显示了两种类型的HTTPS解密证书；但是，在您的网络中，只能部署一种类型。

步骤3.导出自定义信任根证书

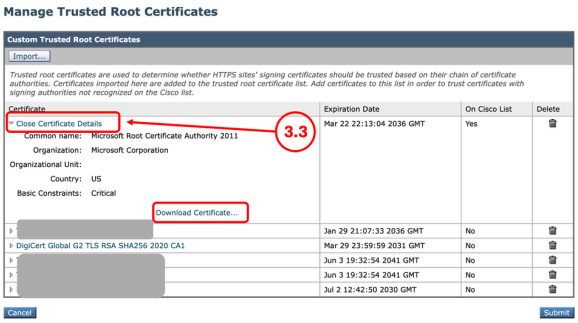
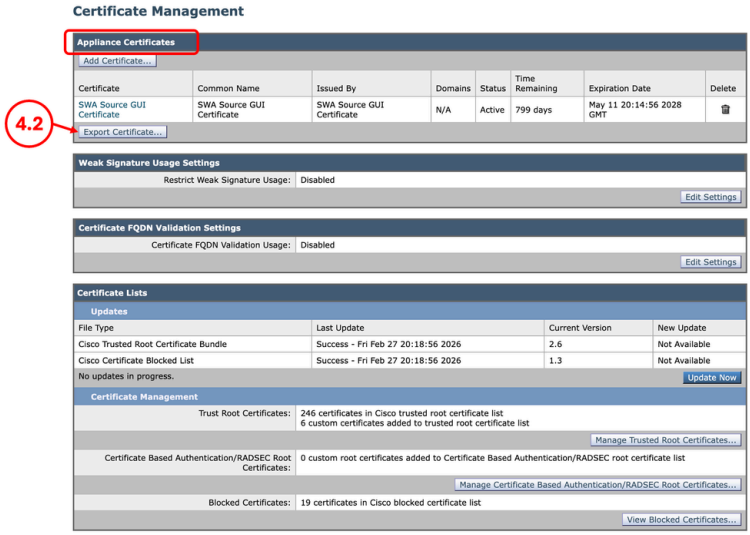
注意：如果SWA上没有添加自定义受信任根证书，请跳至步骤4。

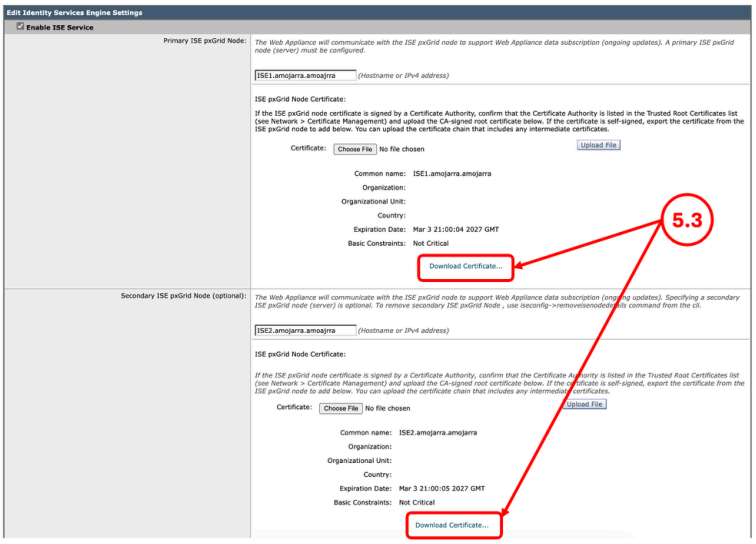
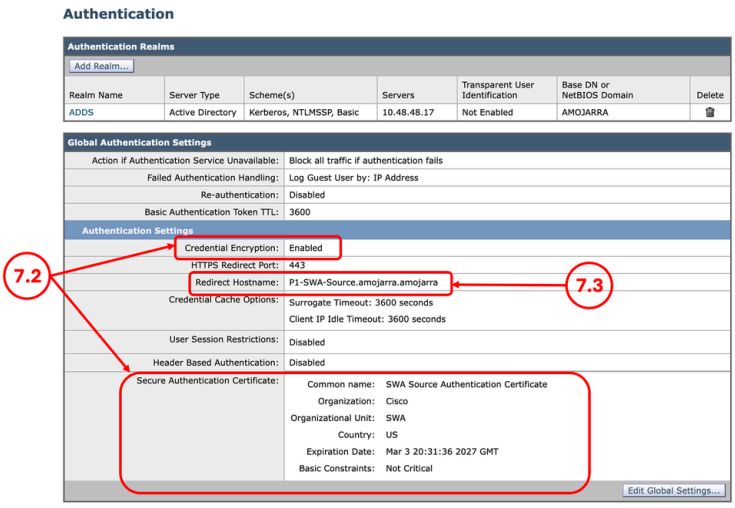
第3.1步：从GUI中，导航到Network，然后点击Certificate Management。

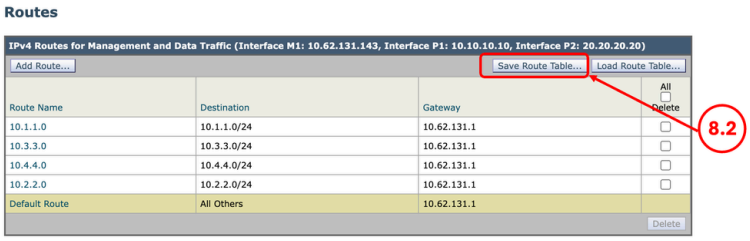
第3.2步：在Certificate Management部分，点击Manage Trusted Root Certificates。



映像 — 管理受信任的根证书

	第3.3步：通过点击每个自定义受信任根证书(Custom Trusted Root Certificates)的名称并点击Download Certificate..  映像 — 下载受信任的根证书
步骤4.导出GUI证书 注意：如果使用的是内置GUI证书，请跳至步骤5。	第4.1步：从GUI中，导航到Network，然后点击Certificate Management。 第4.2步：在Appliance Certificates部分，点击Export Certificate。  映像 — 导出GUI证书
步骤5.导出ISE证书 注意：如果没有SWA、ISE集成，请跳至步骤6。	第5.1步：从GUI中，导航到网络，然后点击Identity Services Engine。 第5.2步。单击Edit Settings。 第5.3步：下载所有可用的证书。

	 映像 — 下载ISE证书
步骤6.许可证/功能	第6.1步：在GUI中，导航到系统管理，然后点击许可证或功能，具体取决于您使用的许可证类型。 第6.2步：截取许可证/功能的截图。
步骤7.身份验证重定向证书	第7.1步：从GUI中，导航到Network，然后点击Authentication。 第7.2步：如果启用了Credential Encryption，请确保您拥有证书和密钥。 步骤7.3.截取当前配置的截图。  图像 — 身份验证证书 注意：无法从GUI下载身份验证证书。

步骤8.导出静态路由 注意：如果计划对目标SWA使用相同的网络配置和IP地址，请跳至步骤10。	第8.1步：在GUI中，导航到Network，然后点击Routes。 第8.2步：对于每个路由表，点击保存路由表。  图像 — 导出路由表
步骤9. DNS设置 注意：如果计划对目标SWA使用相同的网络配置和IP地址，请跳至步骤10。	第9.1步：在GUI中，导航到网络，然后点击DNS。 步骤9.2.截取DNS配置的截图。

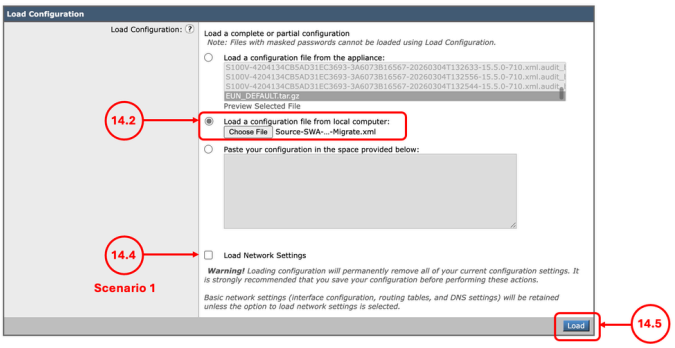
准备目标SWA

步骤10.安装虚拟SWA 注意：如果目标SWA是物理的，您可以跳至步骤11。	步骤10.1.使用以下指南安装虚拟SWA: • 在Vmware ESXi上安装安全Web设备 • 在Microsoft Hyper-V上安装安全Web设备 步骤10.2.确保新SWA具有推荐的网络访问权限： • 为安全Web设备配置防火墙
步骤11.初始SWA设置	步骤11.1.配置IP地址。 步骤11.2.配置默认网关。 步骤11.3.配置DNS服务器。 步骤11.4.许可设备。 步骤11.5.启用功能。 步骤11.6.运行系统设置向导。 您可以在本文中找到详细步骤：Secure Web Appliance Initial Setup

步骤12.清理配置文件 注意：如果未将ISE与SWA集成，您可以跳至步骤13。	第12.1步：查看本文中的Fixing Errors部分，从XML备份文件中删除ISE证书配置。

将配置文件导入目标SWA

步骤13.导入自定义受信任根证书 注意：如果未使用任何自定义受信任根证书，请跳至步骤14。	第13.1步：从GUI中，导航到Network，然后点击Certificate Management。 第13.2步：在Certificate Management部分，点击Manage Trusted Root Certificates。 步骤13.3.单击导入。 步骤13.4.上传之前在步骤3中下载的证书。 警告：当根证书和中间证书都可用时，首先上传根CA证书。提交并提交更改后，继续导入中间证书。
步骤14.导入配置文件	第14.1步：从GUI中，导航到System Administration并选择Configuration File。 步骤14.2.在Load Configuration部分，选择Load a configuration file from local computer。 第14.3步。点击选择文件并选择XML配置文件。 第14.4步：如果迁移与Scenario 1匹配，且必须在新SWA中使用之前的IP地址，请选中Load Network Settings复选框，否则不要选择此选项。 步骤14.5.单击加载。 步骤14.6.在Confirm Load Configuration弹出中点击Continue。

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

映像 — 导入配置</td></tr>
<tr><td>步骤15.更改管理员密码

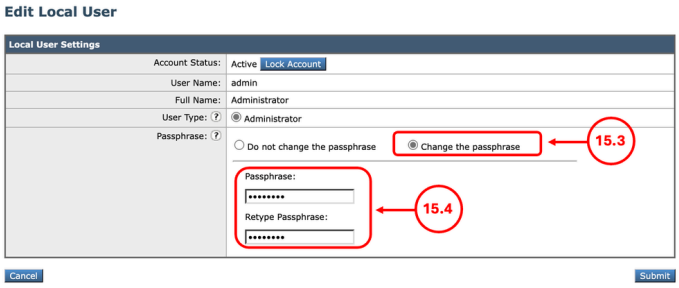
注意：如果您有源SWA管理密码，请跳至步骤16。</td><td>15.1.从GUI中，导航到System Administration并选择Users。

15.2.单击admin用户名。

15.3.选择更改口令。

15.4.输入密码。

15.5.单击提交。

图像 — 更改管理员密码</td></tr>
<tr><td>步骤16.提交</td><td>步骤16.1.现在您可以提交更改了。</td></tr>
<tr><td>步骤17.导入路由

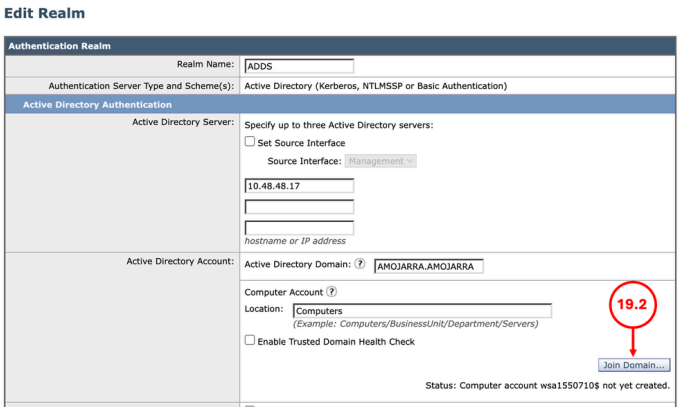
注意：如果导入配置时加载网络设置，请跳至步骤19。</td><td>第17.1步：在GUI中，导航到Network，然后点击Routes。

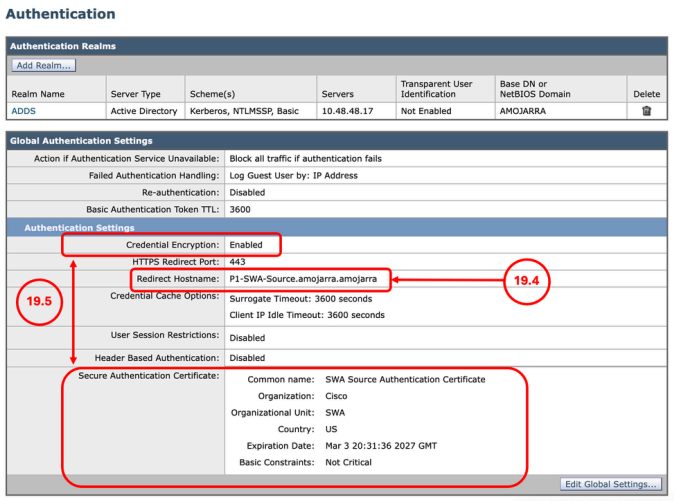
步骤17.2.对于每个路由表，单击Load Route Table。

第17.3步。选择您在第8步中导出的文件。

步骤17.4.点击提交。

步骤17.5.提交更改。</td></tr>
</table>

步骤18.配置DNS设置 注意：如果在导入配置时加载Network Settings，请跳至步骤19。	第18.1步：从GUI导航到Network，然后单击DNS。 步骤18.2.单击Edit Settings。 步骤18.3.使用步骤9中的截图 步骤18.4.单击提交。 步骤18.5.提交更改。
步骤19.将SWA加入/重新加入Active Directory	第19.1步：从GUI中，导航到Network，然后单击Authentication。 步骤19.2.点击身份验证领域名称的名称。 提示：如果为SWA分配了新的IP地址和主机名，请确保在Active Directory DNS服务中创建必要的DNS记录。 第19.2步：点击加入域并输入凭证：  映像 — 加入Active Directory域 第19.3步。单击提交。 步骤19.4.确保重定向主机名正确。 第19.5步：如果启用了凭证加密，请确保安全身份验证证书正确。



图像 — 身份验证设置

步骤19.6.提交更改。

步骤20.重新加入SMA

注意：如果SWA不由SMA管理，请跳过此步骤。

注意：如果没有替换现有的SWA（场景2），并且已迁移的SWA具有新的IP地址，请将SWA作为新设备添加到SMA并跳过步骤20。

步骤20.1.连接到SMA的CLI。

步骤20.2.运行logconfig。

步骤20.3.输入HOSTKEYCONFIG。

步骤20.4.键入DELETE并按Enter。

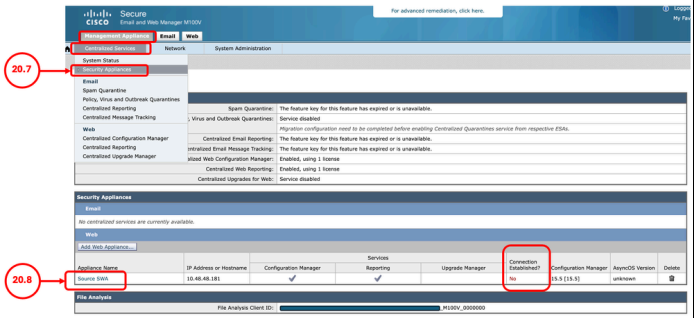
第20.5步：键入与最近迁移的SWA相关联的号码，然后按Enter键，直到向导完成。

步骤20.6.键入commit并按Enter保存更改。

第20.7步：从SMA GUI中，导航到Management Appliance。选择Centralized Services，然后点击Security Appliances。

步骤20.8.单击最近迁移的SWA的名称。

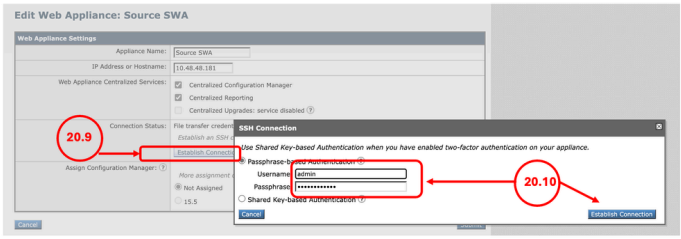
提示：您可以看到Connection Established列设置为No。



映像 — SMA安全设备状态

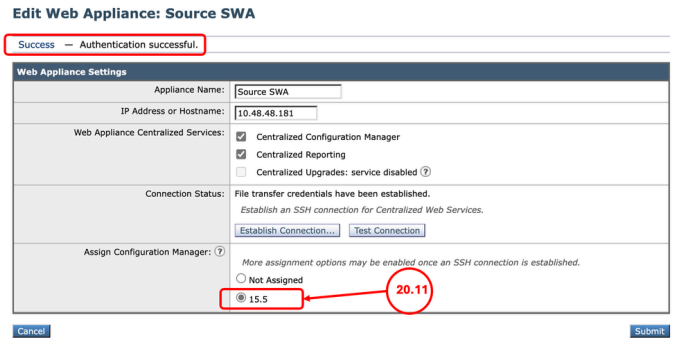
步骤20.9.单击Establish Connection。

第20.10步。输入Username和Passphrase，然后单击Establish Connection。



映像 — 建立与SWA的连接

步骤20.11.分配配置管理器。



映像 — 分配配置管理器

步骤20.12.提交并提交更改。

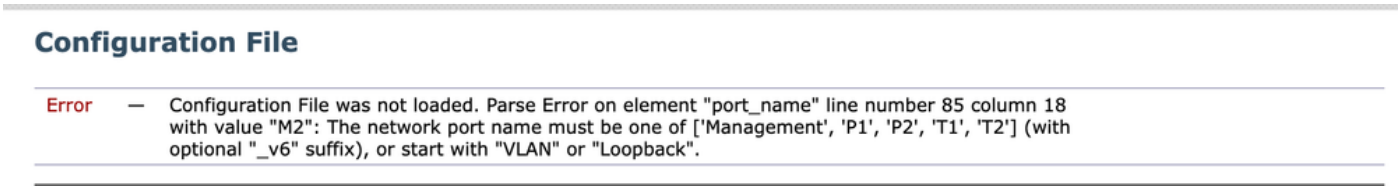
第20.13步(可选)：可以通过将配置发布到SWA进行测试。

提示：SMA保留以前的SWA中的所有报告和跟踪数据。

修复错误

元素port_name的解析错误

网络端口名称必须是['Management'、'P1'、'P2'、'T1'、'T2']之一:



映像 — 网络接口命名错误

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

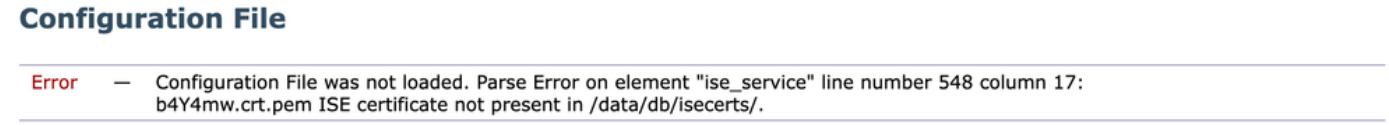
当您从物理SWA迁移到虚拟时，会发生此错误。虚拟SWA只有5个NIC，并且M2接口无效。要修复错误，请在文本编辑器中编辑XML配置文件并删除以下行：

```
        M2
```

```
         M2
```

```
M2



autoselect




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

元素ise_service的解析错误



映像 — ISE证书错误

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

由于ISE证书不包括在SWA配置导出中，并且直接上传到设备上，您需要从XML文件中删除证书配置，并在成功导入后，手动配置ISE。要解决此问题，请在文本编辑器中编辑XML配置文件，并在错误中搜索证书名称(在本例中，搜索AA11AA)，然后将其从配置文件中删除：

```
Before:
```

AA11AA

BB22BB

After:

除了证书名称，您还需要删除Web Appliance Client Certificate名称。

在本示例中，Web设备客户端证书是自签名证书：

Before:

1

xAcK6T

After:

0

故障转移未在新虚拟SWA上工作

如果高可用性（故障转移）未在目标虚拟SWA上运行，请确保正确配置虚拟机监控程序。有关详细信息，请访问：确保VMware环境中适当的虚拟WSA HA组功能

相关信息

- 思科安全Web设备AsyncOS 15.2用户指南
- 在Vmware ESXi上安装安全Web设备
- 在Microsoft Hyper-V上安装安全Web设备

- 安全Web设备初始设置

- 思科安全邮件和Web虚拟设备安装指南
- 在安全Web设备中配置自定义URL类别 — 思科

- 使用安全Web设备最佳实践

- 为安全Web设备配置防火墙

- 在安全Web设备中配置解密证书

- 安全网络设备DNS服务故障排除
- 确保VMware环境中适当的虚拟WSA HA组功能

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。