使用ASA多情景和NetScaler 1000V配置和部署双节点服务图

目录

简介

本文档介绍如何在思科以应用为中心的基础设施(ACI)平台中配置和部署双节点服务图。服务图中使用的两台设备是以透明模式运行的物理思科自适应安全设备(ASA)和Citrix NetScaler 1000V虚拟设备。

先决条件

要求

思科建议您在尝试本文档中描述的配置之前先了解这些主题：

- 思科ACI交换矩阵，由两台主干交换机和两台枝叶交换机组成
- 思科虚拟机托管(VMM)域

- 思科ASA
- NetScaler 1000V虚拟设备

使用的组件

本文档中的信息基于下列硬件和软件版本：

- ACI交换矩阵，由运行代码版本1.1(4e)或更高版本的两个主干交换机和两个枝叶交换机以及设备软件包版本1.2或更高版本组成
- 在ACI中为VMWare配置的VMM域
- 具有两个连接的物理ASA（每个枝叶交换机连接一个）
- 部署在VMWare vCenter中的NetScaler 1000V虚拟设备
- 思科应用策略基础设施控制器(APIC)

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本节介绍如何配置此部署中涉及的各种组件。

配置 ASA

本节介绍如何在ASA上完成配置。

在ASA上启用多情景支持

要在ASA上创建多个情景，必须启用该功能。登录到ASA并在配置模式下输入*此*命令：

```
ciscoasa(config)#
```

mode multiple

然后系统将提示您重新加载。设备重新加载后，您可以继续创建用*户上*下文。

> **注意**：必须*在用*户上下文之前创建管理上下文。本文档不介绍如何创建管理情景，而是描述用户情景。有关如何创建管理情景的详细信息，请参阅Cisco ASA系列CLI配置指南9.0的*配置多情景部分*。

在ASA上配置用户情景

要在ASA上创建用户上下文，请从系统上下文中输入以*下命*令：

```
ciscoasa/admin# changeto context sys
ciscoasa(config)# context

jristain    <--- This is the name of the desired context


Creating context 'jristain'... Done. (5)
ciscoasa(config-ctx)# allocate-interface Management0/1

ciscoasa(config-ctx)# config-url disk0:/

jristain

.cfg

<--- "context-name.cfg"


WARNING: Could not fetch the URL disk0:/jristain.cfg
INFO: Creating context with default config
```

此配置创建情景，分配管理接口以在此情景中使用，并指定配置文件的位置。您现在必须输入此情景，以配置所需的最小引导程序，以便APIC可以连接。

配置用户情景的管理IP地址

创建用户情景后，您可以更改该情景并在已分配接口上配置管理IP地址。输入这些命令：

```
ciscoasa(config-ctx)# changeto context jristain   <----

Drops into the user context


ciscoasa/jristain(config)# interface Management0/1
ciscoasa/jristain(config-if)# ip address 192.168.20.10 255.255.255.128
ciscoasa/jristain(config-if)# nameif management
INFO: Security level for "management" set to 0 by default.
ciscoasa/jristain(config-if)# security-level 100
ciscoasa/jristain(config-if)# exit
ciscoasa/jristain(config)# route management 0.0.0.0 0.0.0.0 192.168.20.1
ciscoasa/jristain(config)# exit
ciscoasa/jristain# copy running-config startup-config
```

> **注意**：*nameif* 条目必须是*管理*，因为这是设备包的预期。如果*nameif* 条目包含任何其他字符，则在APIC中部署L4-L7设备时会出现故障。

配置APIC所需的引导程序

要将APIC连接到ASA，需要进行一些最少的配置。这包括HTTP服务器和APIC的用户帐户。在用户情景中使用此配置：

```
ciscoasa/jristain(config)#username

<username>
```

```
 password

<password>


ciscoasa/jristain(config)#http server enable
ciscoasa/jristain(config)#http 0.0.0.0 0.0.0.0 management
```

注意：在<username>和<password>区域中输入所需的用户名和口令。

配置APIC

本节介绍如何在APIC上完成配置。

配置所需的网桥域

部署双节点服务图需要三个网桥域(BD)。

使用以下信息为外部ASA接口（消费者）配置BD:

- *L2未知单播* — 泛洪
- *ARP泛洪* — 启用
- 可以配置子网，以充当启用单播路由的NetScaler外部接口的*默认网关*

使用此信息配置用于连接两台设备的BD:

- *L2未知单播* — 泛洪
- *ARP泛洪* — 启用
- *单播路由* — 已禁用

配置所需的终端组

服务图要求配置两个终端组(EPG):一个消费者和一个提供商。消费者EPG应使用连接到外部ASA接口的BD。提供商EPG应使用连接到终端服务器的BD。

将管理情景添加为L4-L7设备

您必须将ASA管理情景和用户情景添加到APIC。要完成此操作，请导航至**Tenant > L4-L7 Services > L4-L7 Devices**，右键单击并选择**Create an L4-L7 Device**，然后完成以下步骤：

1. 如果尚未启用，请单击*General区域中的Managed复选框。*
2. 输入设备*名称*。
3. 从下拉*菜单中*选择服务类型。

4. 选择设备类型(**物理**或**虚拟**)。

5. 从下拉菜单中选择物理域。

6. 选择*Mode*。

7. 从**Device Package下拉菜**单中选择CISCO-ASA-1.2。

8. 从下拉菜单中选择ASA模型。

9. 选择功能类型(**GoThrough**为*透明*模式，**GoTo** 为路由模式)。

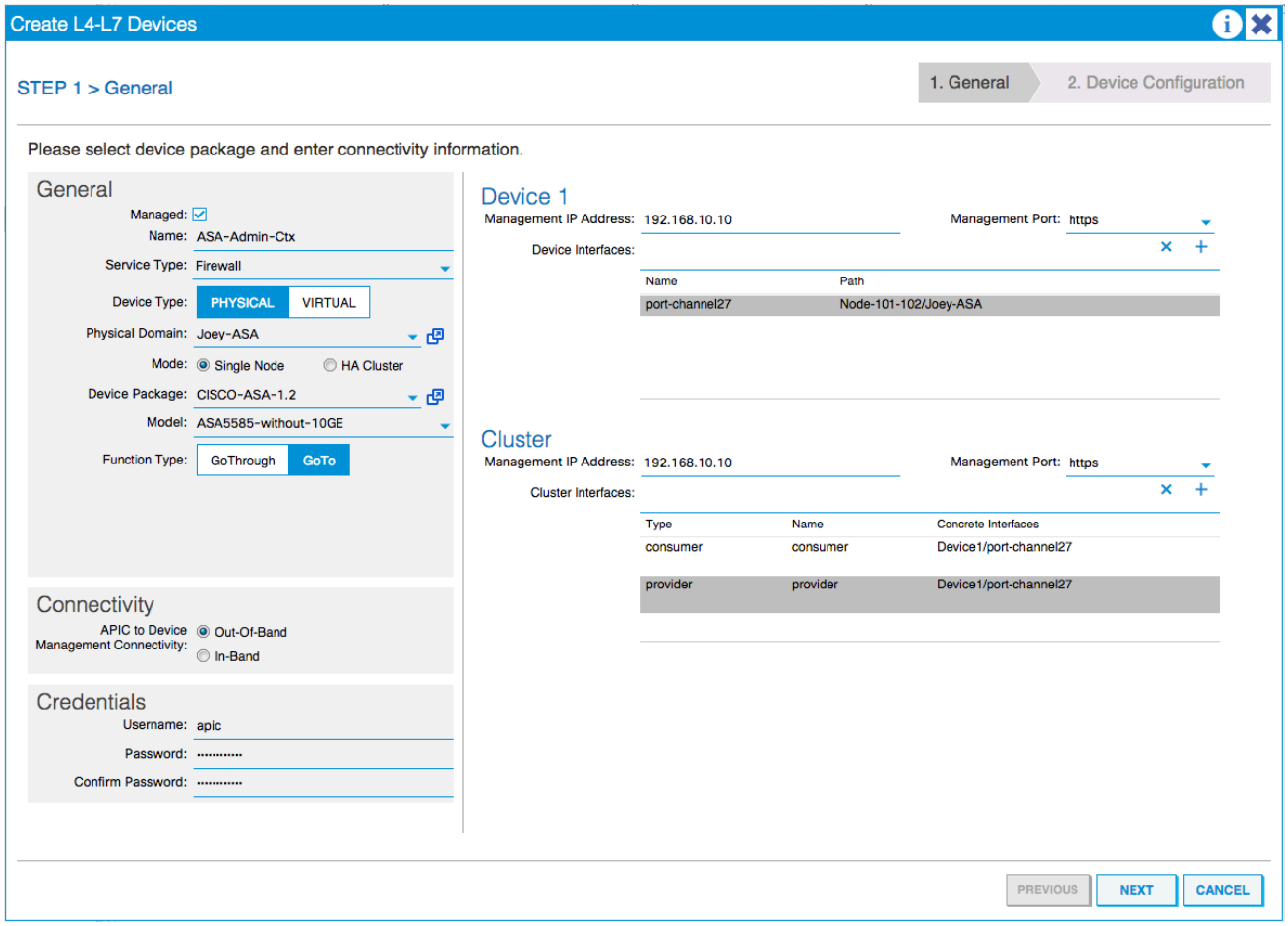
10. 在“连接”**区域中选择APIC到设**备管理连接选项。

11. 在“凭**证**”区**域输**入您的*用户名*和密码。

12. 在Device 1区域的Management IP Address字段(连同Port)中输入Admin上下文的IP地址。

13. 创建物理接口，为其命名，选择ASA使用的接口策略组，然后选择提供**商和消费者**。

14. 在集群区域中输入您用于设备1区域的相同信息。创建两个指向同一端口通道的集群接口(一个使用者和一个提供程序)。



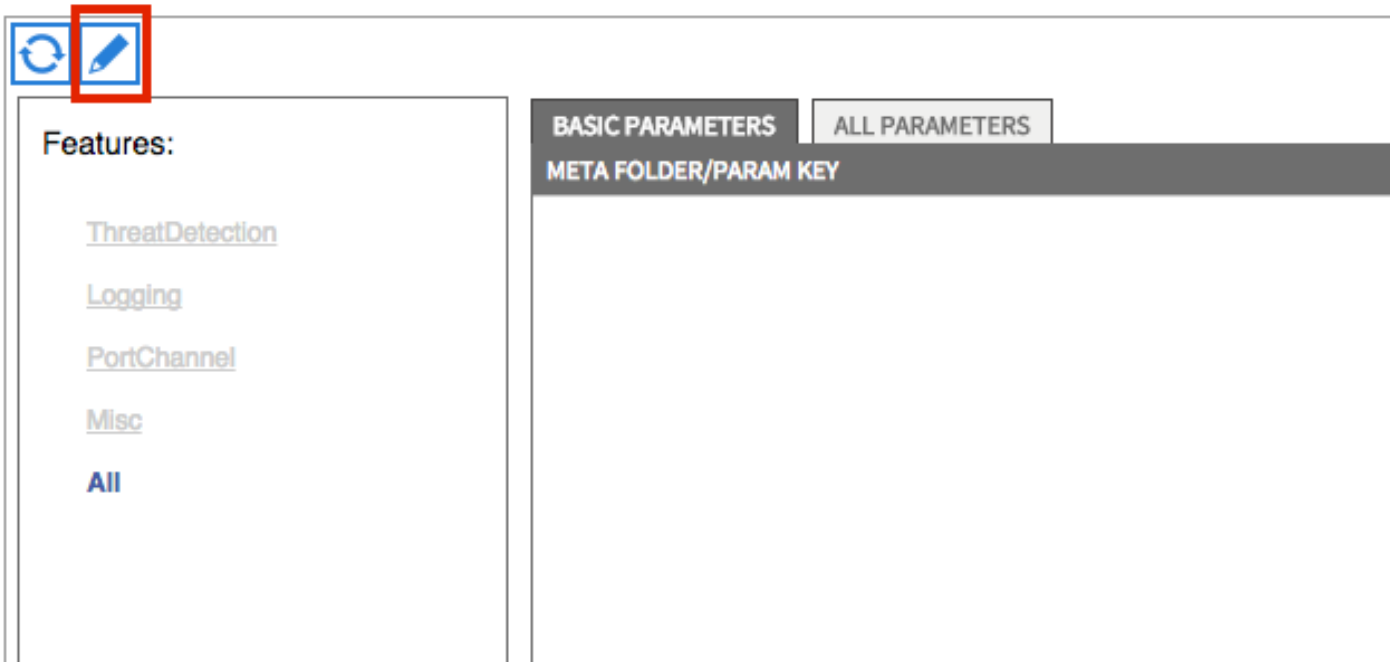
注意：此时可以完成向导的使用。您无需配置任何故障切换信息。

15. 验证设备是否稳定且没有故障：

配置端口通道参数

在向交换矩阵注册设备后，APIC可以通过设备参数推送配置。注册后，必须首先在虚拟端口通道(vPC)中配置将ASA连接到枝叶交换机的端口通道。

要配置端口通道，请导航至您创建的设备，然后单击工作窗格上角的**Parameters**选项卡。单击*铅笔*图标以修改参数：

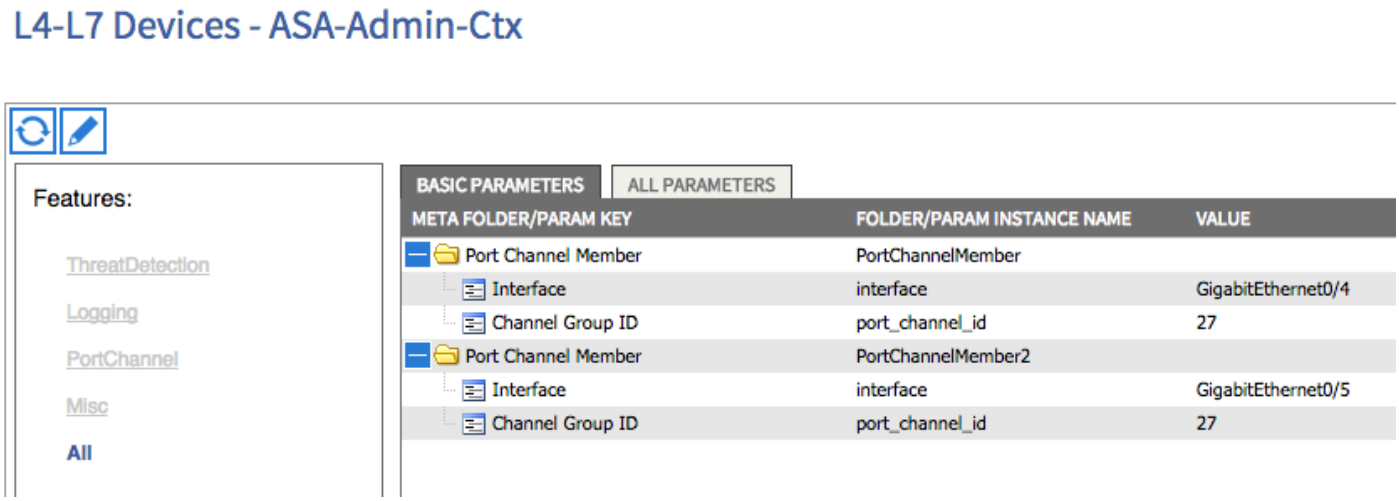


系统将*显示Edit Cluster Parameters*窗口。单击**PortChannel**以限制选项的范围。展开“Port Channel Member”**文件夹并**填写“配置*选项*”。以下是每个选项的说明：

- *Channel Group ID* — 在*Value*字段中，输入要分配给ASA接口的PC ID（支持1到48）。

- *Interface* — 在*Value*字段中，输入要分配给信道组的ASA上的接口。

对要分配的每个接口重复此过程：



完成后，您应在系统情景中看到在ASA上创建端口通道。要验证此情况，请访问系统上下文并输入**show port-channel summary**命令：

```
ciscoasa#

show port-channel summary


Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
U - in use N - not in use, no aggregation/nameif
M - not in use, no aggregation due to minimum links not met
w - waiting to be aggregated
Number of channel-groups in use: 2
Group Port-channel Protocol Span-cluster Ports
------+-------------+---------+------------+----------------------


27      Po27(N)             LACP           No      Gi0/4(P)    Gi0/5(P)
```

将用户情景添加为L4-L7设备

您必须将用户情景注册为交换矩阵中的L4-L7设备。导航到**Tenant > L4-L7 Services > L4-L7 Devices**，右键单击并选择**Create an L4-L7 Device，然后完成以下步骤：**

1. 如果尚未启**用**，请单击*General区域中的Managed复选框。*
2. 输入设备*名称*。
3. 从下拉*菜单中*选择服务类型。
4. 选择设*备类型*。
5. 从下拉菜*单中选*择物理域。
6. 选择*Mode*。
7. 从**Device Package下拉菜**单中*选择*CISCO-ASA-1.2。

8. 从下拉菜单中选择ASA模型。

9. 在“连接”区域中选择APIC到设备管理连接选项。

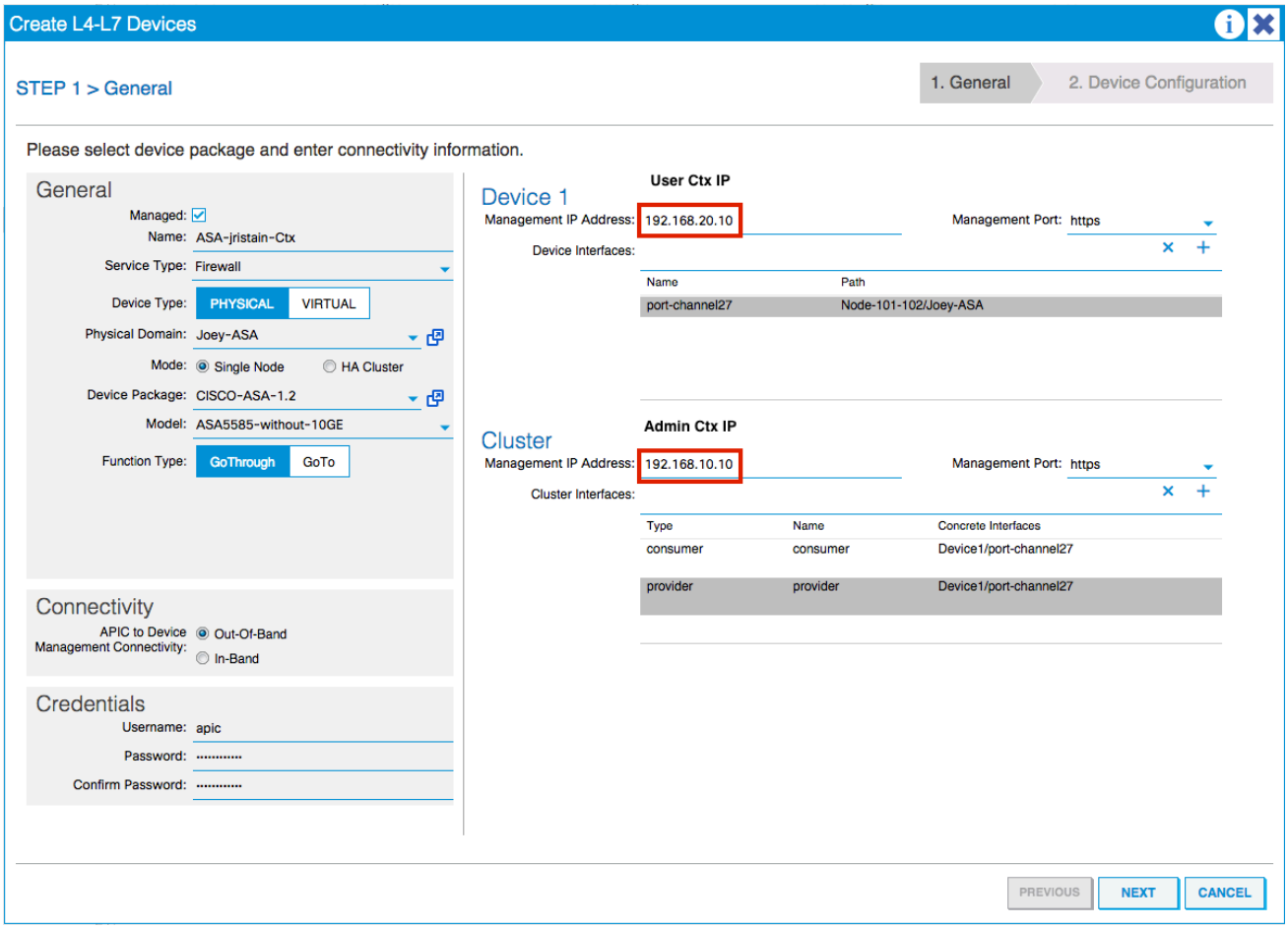
10. 选择功能类型(GoThrough为透明模式，GoTo 为路由模式)。

11. 在“凭证”区域输入您的用户名和密码。

12. 在Device 1区域的Management IP Address字段(连同Port)中输入User上下文的IP地址。

13. 创建物理接口，为其命名，选择ASA使用的接口策略组，然后选择提供商和消费者。

14. 在“集群”区域中输入管理情景的管理IP地址（以及端口）。创建两个指向同一端口通道的集群接口(一个使用者和一个提供程序)。



注意：此时可以完成向导的使用。您无需配置任何故障切换信息。

15. 验证设备是否稳定且没有故障：

将NetScaler 1000V添加为L4-L7设备

本配置示例中的第二个节点是NetScaler 1000V。NetScaler为连接的服务器提供负载均衡功能。您还必须向APIC注册此设备。导航**到Tenant > L4-L7 Services > L4-L7 Devices**，右键单击并选择**Create an L4-L7 Device，然后完成以下步骤：**

1. 如果尚未启**用**，请单击*General*区*域中的Managed复选框。*

2. 输入设备*名称*。

3. 从下拉*菜单中选择*服务类型(NetScaler是*ADC*或应用*交付控制*器)。

4. 选择设*备类型*。

5. 从下拉菜*单中选*择VMM域（如果为虚拟）。

6. 选择*Mode*。

7. 从**Device Package下拉菜单**中选*择Cisco-NetScaler1KV*-1.0。

8. 从下拉菜单中选择*Model*(Virtual Appliance是*NetScaler-VPX*)

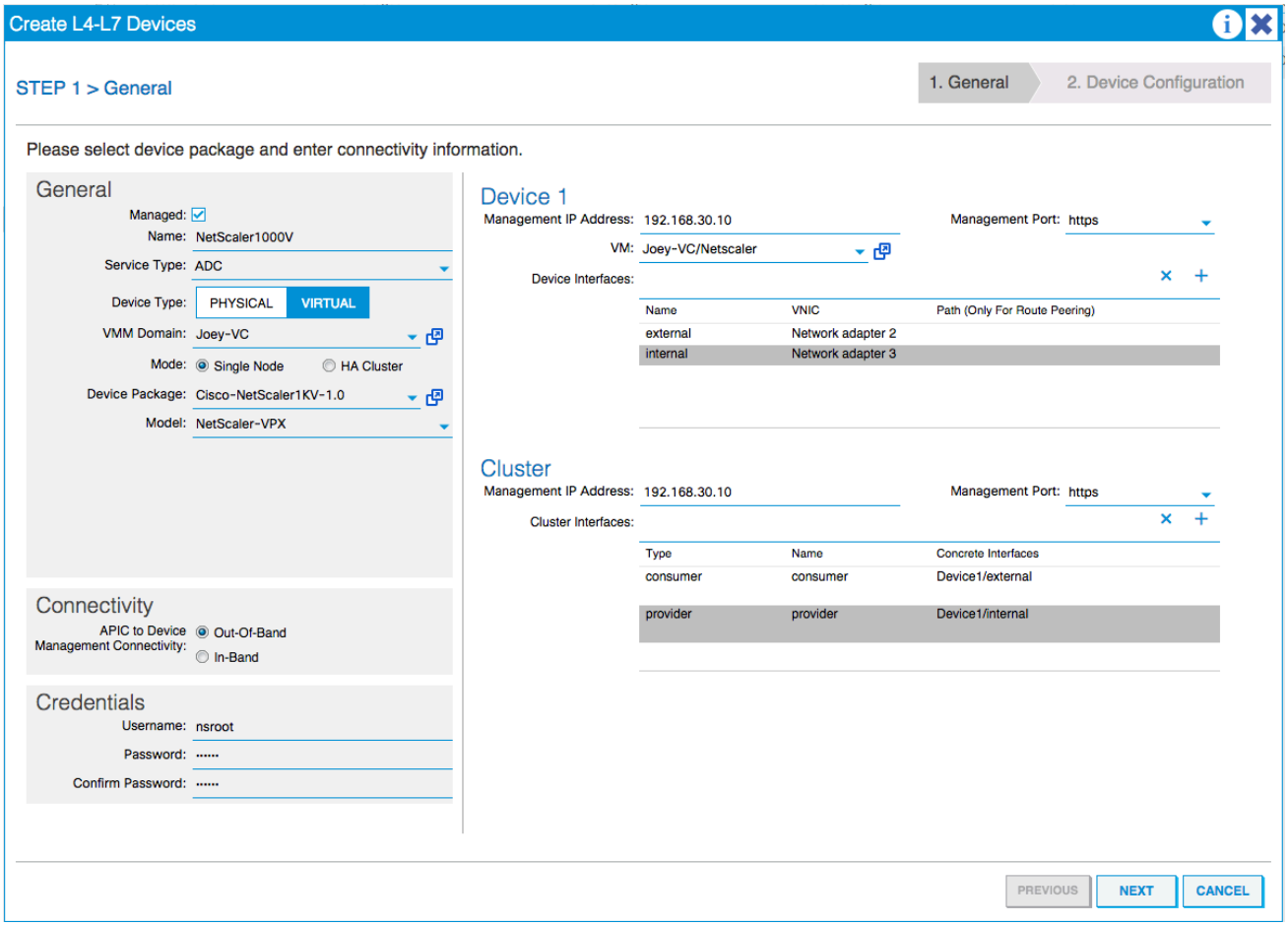
9. 在“连接**”区域中选择APIC到设**备管理连*接选*项。

10. 在“凭**证”**区**域输**入您的*用户名*和密码。

11. 在Device 1区域的Management IP Address字*段(*连同Port)中输*入Admin*上下文*的IP地*址。选择VM（如果为虚拟）。

12. 在Device Interfaces*区*域创建外*部接*口，并选择未使用的网络适配器。 **注意：***网络适配器*1用于管理目的，因此请勿使用它。
13. 在“设备*接口*”区域*创建内*部接口，并选择未使用的网络适配器。

14. 在集群区域中输入您用*于设备*1区域*的相*同信息。创建两个集群接口(一个*消费者*接口和一*个提供*商)。



15. 验证设备是否稳定且没有故障：

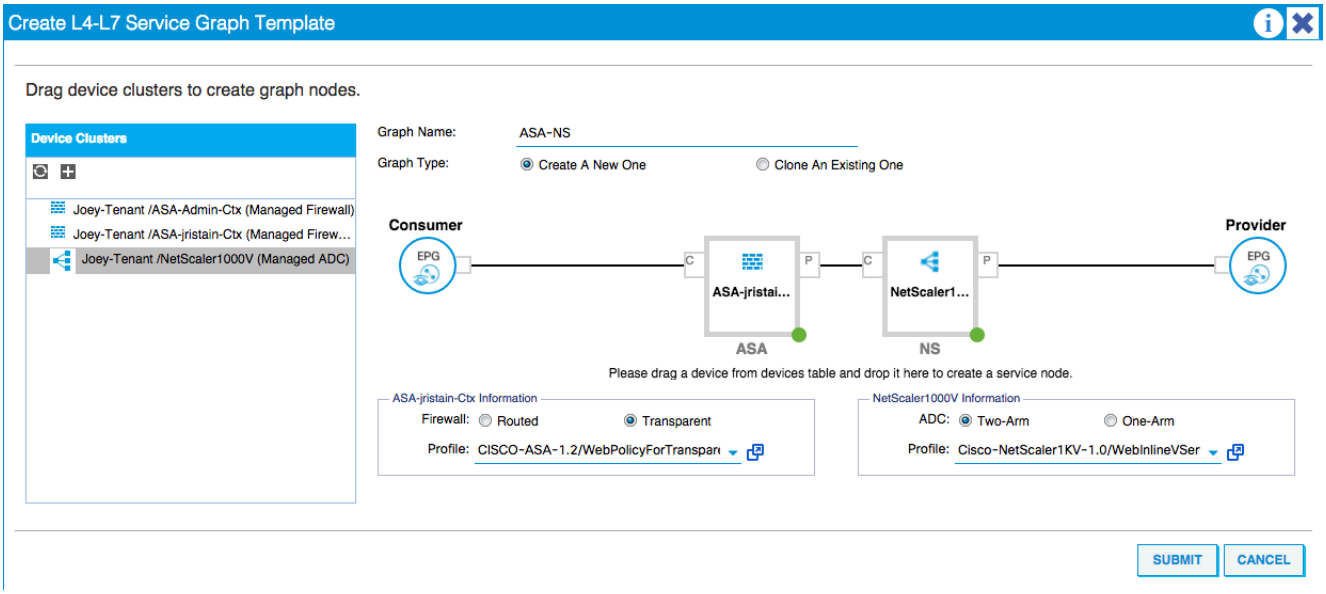
创建服务图模板

现在设备已注册，您可以创建服*务图模板*。导航至**租户> L4-L7服务> L4-L7服务图模板>创建L4-L7服务图模板**，并完成以下步骤：

1. 在图形名称字*段中输*入名称。

2. 按设备集群的部署顺序从*设备*集群区域拖放设备。输入每个名称。

3. 为每台设备选*择功*能配置文件。对于NetScaler，此示例使**用双臂**(或*内联*模式)。

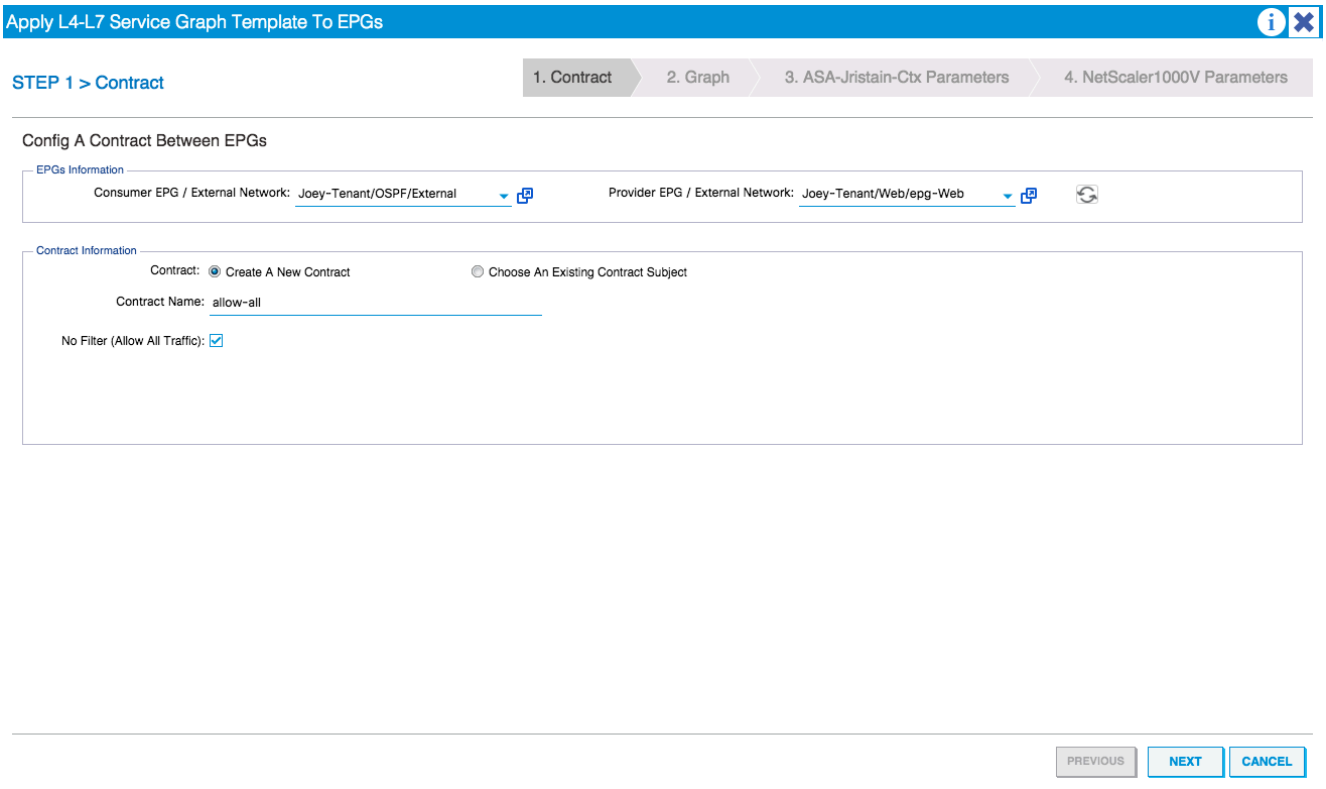


部署服务图模板

创建模板后，可将其部署到设备。导航至**租户> L4-L7服务> L4-L7服务图模板>服务图模板>应用服务图模板**。

在“合同*”(Contract)*选项卡上，完成以下步骤：

1. 从Consumer EPG/External Network下*拉菜单中选择*Consumer EPG。
2. 从Provider EPG/External Network下*拉菜单中选择*提供商EPG。
3. 在“合同信息”(Contract Information)区域创建新合同，或选择已*存在的*合同。



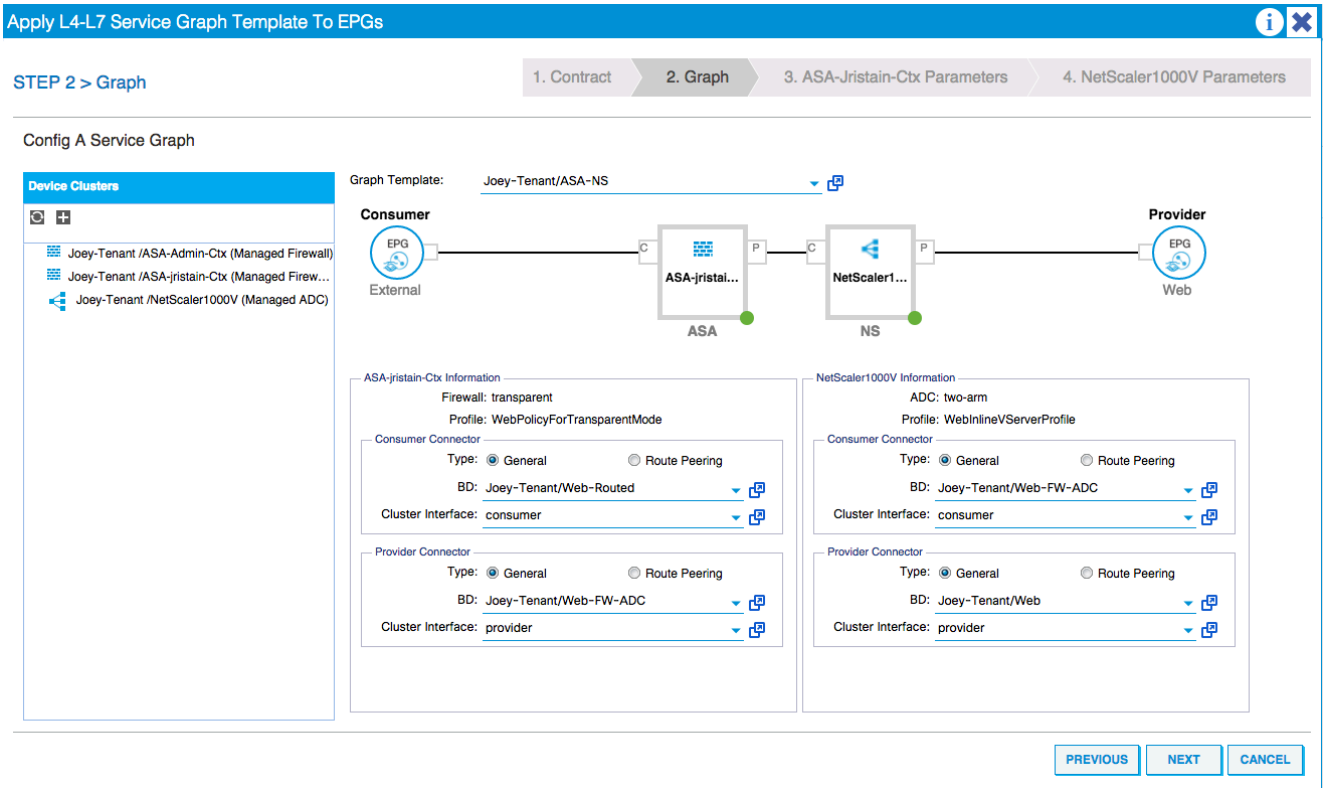
在“图形”选项卡上，完成以下步骤：

1. 从BD下拉菜单中选择ASA外部接口的BD。

2. 从BD下拉菜单中选择BD For the ASA内部接口。

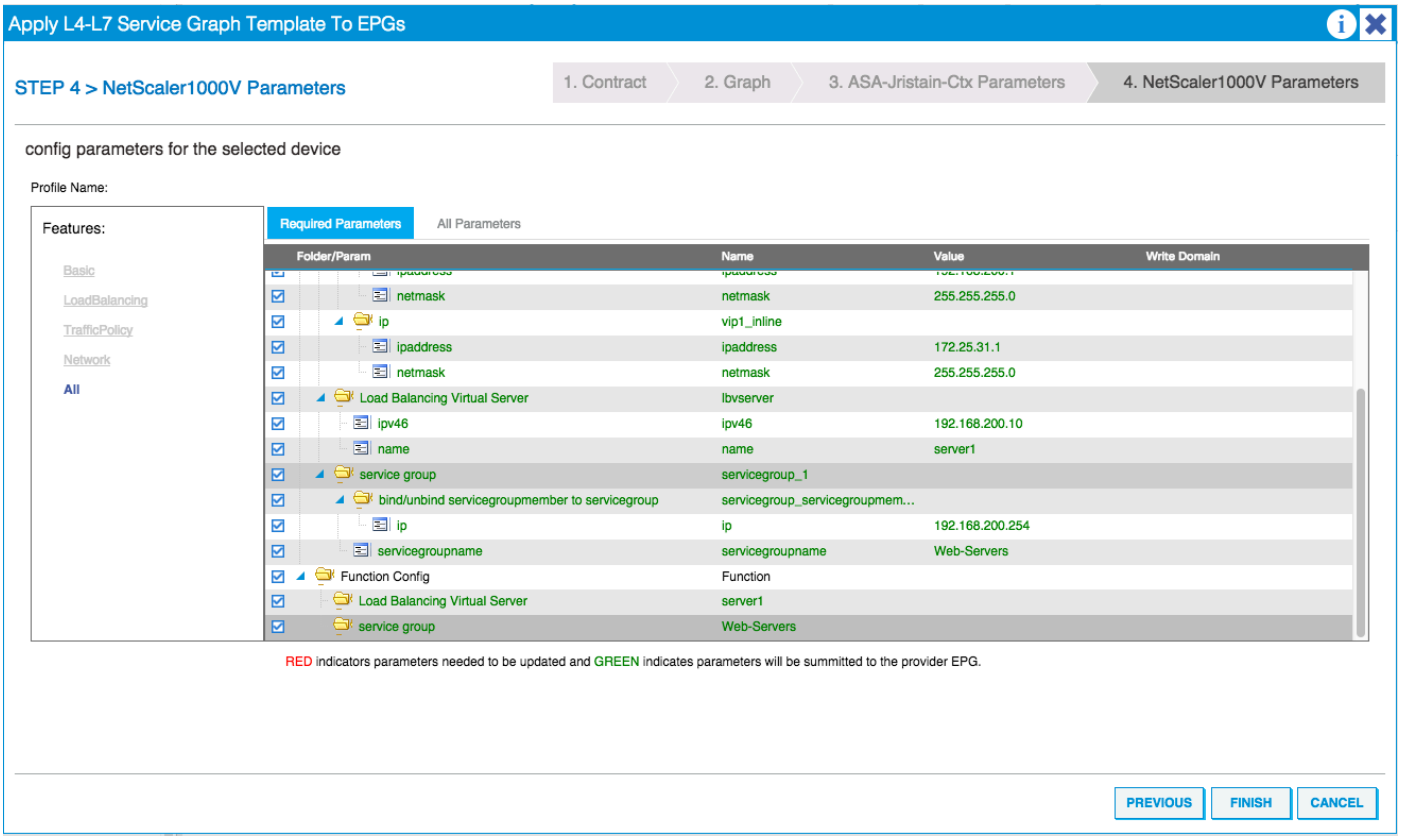
3. 从BD下拉菜单中选择NetScaler外部接口的BD。

4. 从BD下拉菜单中选择NetScaler内部接口的BD。



在“ASA参数”选项卡上，输入所需参数。不需要此选项卡上的任何参数。

在NetScaler参数选项卡上，通过向导输入NetScaler配置：



验证

当前没有可用于此配置的验证过程。

故障排除

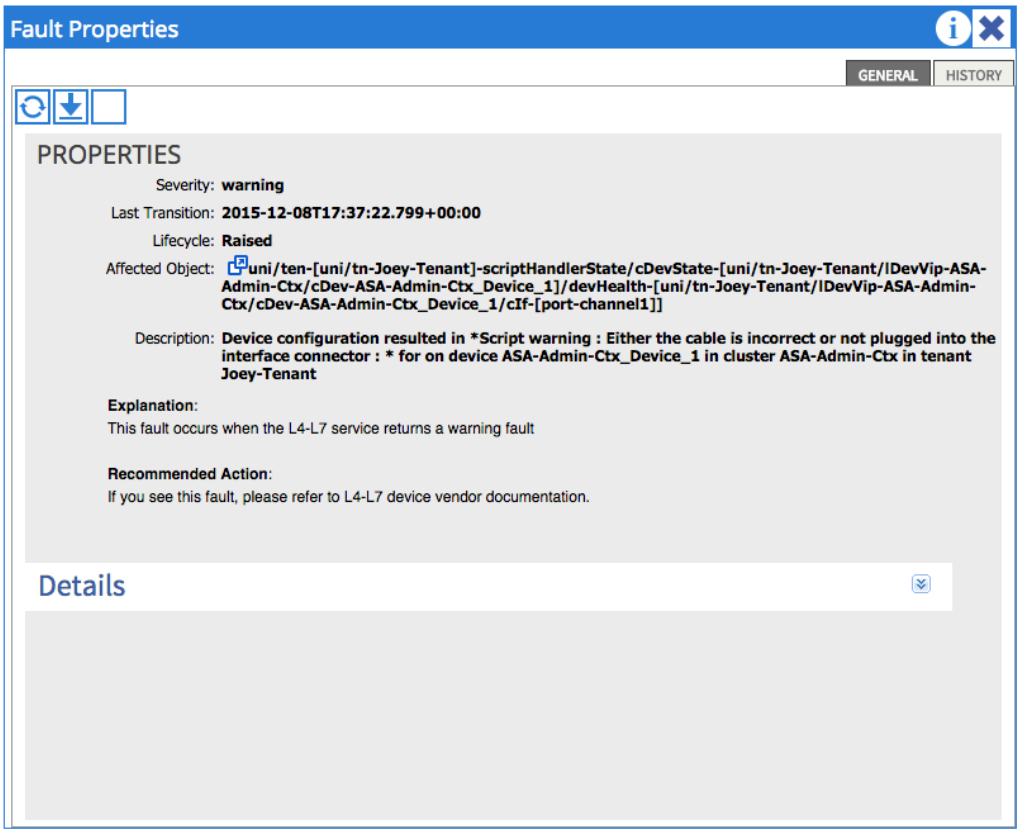
本节提供可用于排除配置故障的信息。

已知故障

以下是与本文档中所述配置相关的两个已知故障：

- **脚本警告：电缆不正确或未插入接口连接器**:

CREATION TIME	LAST TRANSITION	AFFECTED OBJECT	LIFECYCLE	DESCRIPTION
2015-12-08T17:35:01.557+00:00	2015-12-08T17:37:22.799+00:00	uni/ten-[uni/tn-Joey-Tenant]-scriptHandlerState/cDevState-[uni/tn-Joey-Tenant/lDevVip-ASA-Admin-Ctx/cDev-ASA-Admin-Ctx_Device_1]/devHealth-[uni/tn-Joey-Tenant/lDevVip-ASA-Admin-Ctx/cDev-ASA-Admin-Ctx_Device_1/cIf-[port-channel1]]	Raised	Device configuration resulted in *Script warning : Either the cable is incorrect or not plugged into the interface connector : * for on device ASA-Admin-Ctx_Device_1 in cluster ASA-Admin-Ctx in tenant Joey-Tenant

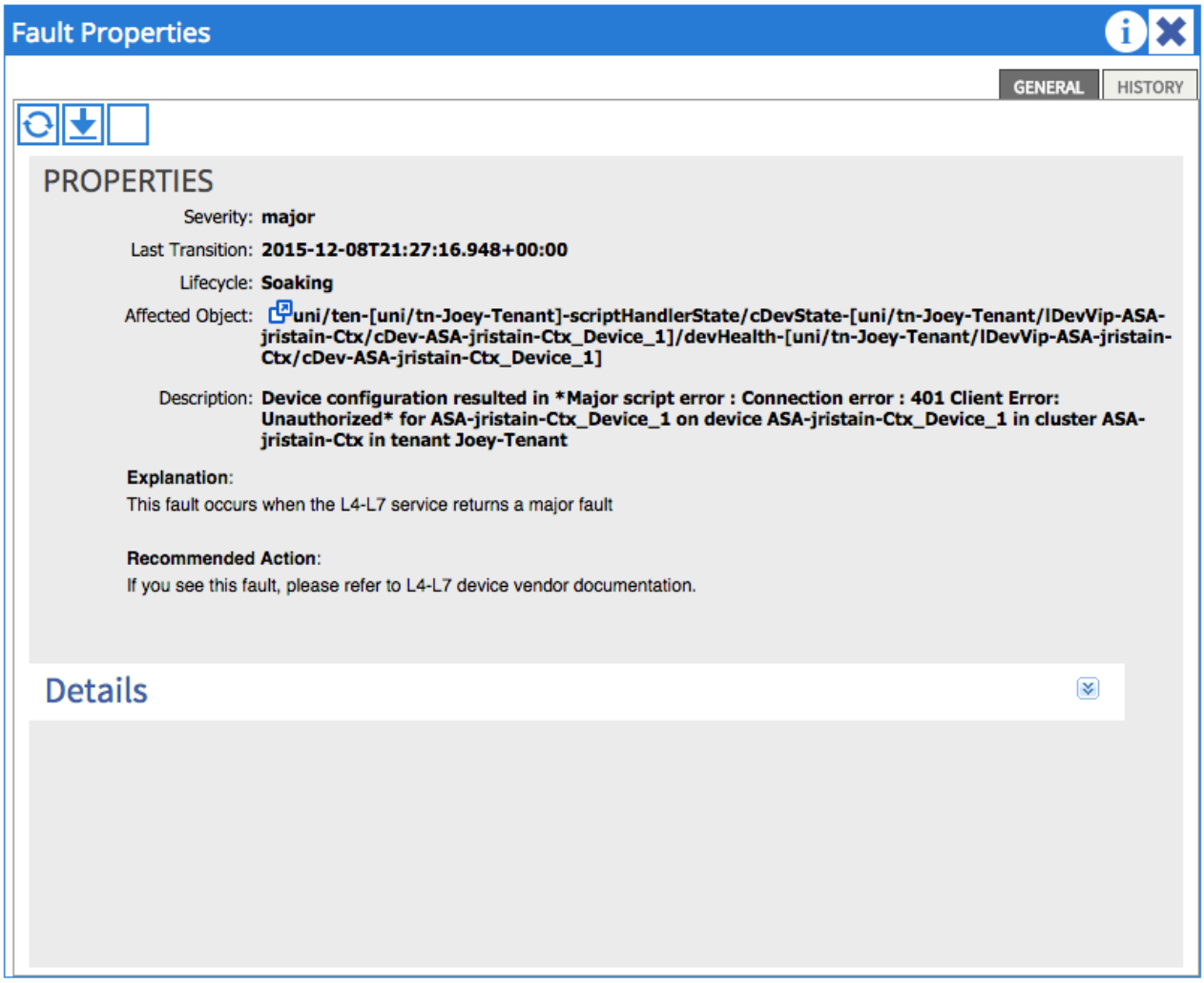


要解决此问题，请确保已配置端口通道参数，并且ASA上的端口通道已启用。有关如何验证此项的信息，请参阅本文档的配置端口通道参数部分。

如果接口已启用，但您仍然看到这些故障，则可能是由于Cisco Bug ID CSCuw56882。此Bug已在1.2.3 ACI软件版本的*1.2.3设备包*支持中修复。设备软件包可以在此下载。

- **主脚本错误：连接错误:401客户端错误：未授权:**

2015-12-08T21:27:16.948+00:00	uni/ten-[uni/tn-Joey-Tenant]-scriptHandlerState/cDevState-[uni/tn-Joey-Tenant/lDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1]/devHealth-[uni/tn-Joey-Tenant/lDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1]	Soaking	Device configuration resulted in *Major script error : Connection error : 401 Client Error: Unauthorized* for ASA-jristain-Ctx_Device_1 on device ASA-jristain-Ctx_Device_1 in cluster ASA-jristain-Ctx in tenant Joey-Tenant
2015-12-08T21:27:22.985+00:00	uni/ten-[uni/tn-Joey-Tenant]-scriptHandlerState/cDevState-[uni/tn-Joey-Tenant/lDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1]	Soaking	Device validate operation for device ASA-jristain-Ctx_Device_1 in cluster ASA-jristain-Ctx in tenant Joey-Tenant failed



要解决此问题，请确保在设备上调配适当的凭证并在APIC中正确配置。