Contents

Introduction

This document describes how to configure and deploy a two-node service graph within the Cisco Application Centric Infrastructure (ACI) platform. The two devices that are used in the service graph are a physical Cisco Adaptive Security Appliance (ASA) that runs in *Transparent* mode, and a Citrix NetScaler 1000V Virtual Appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt the configuration that is described in this document:

- Cisco ACI fabrics that consist of two spine switches and two leaf switches
- Cisco Virtual Machine Managed (VMM) domains
- Cisco ASAs

- NetScaler 1000V Virtual Appliances

Components Used

The information in this document is based on these hardware and software versions:

- An ACI fabric that consists of two spine switches and two leaf switches that run code Version 1.1(4e) or later, and device package Version 1.2 or later
- A VMM domain that is configured within the ACI for VMWare
- A physical ASA with two connections (one connection to each leaf switch)
- A NetScaler 1000V Virtual Appliance that is deployed in the VMWare vCenter
- A Cisco Application Policy Infrastructure Controller (APIC)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This section describes how to configure the various components that are involved in this deployment.

Configure the ASA

This section describes how to complete the configuration on the ASA.

Enable Multi-Context Support on the ASA

In order to create multiple contexts on the ASA, you must enable the feature. Log in to the ASA and enter this command in *Configuration* mode:

```
ciscoasa(config)# mode multiple
```

You are then prompted to reload. Once the device reloads, you can continue to create the *User* context.

> **Note**: An *Admin* context must be created before the User contexts. This document does not describe how to create the Admin context, but rather the User context. For more information about how to create the Admin context, refer to the Configuring Multiple Contexts section of the *Cisco ASA Series CLI Configuration Guide, 9.0*.

Configure the User Context on the ASA

In order to create the User context on the ASA, enter these command from the *System* context:

```
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
```

This configuration creates the context, allocates the management interface for use in this context, and specifies a location for the configuration file. You must now enter this context in order to configure the minimal bootstrap that is required so that the APIC can connect.

Configure the Management IP Address for the User Context

Once the User context is created, you can change to that context and configure the management IP address on the interface that is allocated. Enter these commands:

```
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
```

> **Note**: The *nameif* entry must be *management* because this is the expectation of the device package. If the *nameif* entry contains any additional characters, you will see faults in the deployment of the L4-L7 device in the APIC.

Configure the Required Bootstrap for the APIC

In order to connect the APIC to the ASA, some minimal configuration is required. This includes the HTTP server and a user account for the APIC. Use this configuration in the User context:

```
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
```

> **Note**: Enter your desired username and password into the **<username>** and **<password>** areas.

Configure the APIC

This section describes how to complete the configuration on the APIC.

Configure the Required Bridge Domains

There are three Bridge Domains (BDs) that are required in order to deploy a two-node service graph.

Use this information in order to configure the BD for the external ASA interface (consumer):

- *L2 Unknown Unicast* – **Flood**
- *ARP Flooding* – **Enabled**
- The subnet can be configured in order to act as the default gateway for the NetScaler external interface with *Unicast Routing* **Enabled**

Use this information in order to configure the BD that is used in order to connect the two devices:

- *L2 Unknown Unicast* – **Flood**
- *ARP Flooding* – **Enabled**
- *Unicast Routing* – **Disabled**

Configure the Required Endpoint Groups

The service graph requires that two Endpoint Groups (EPGs) be configured: one consumer and one provider. The consumer EPG should use the BD that connects to the external ASA interface. The provider EPG should use a BD that connects to the end-servers.

Add the Admin Context as an L4-L7 Device

You must add the ASA Admin and User contexts to the APIC. In order to complete this, navigate to **Tenant > L4-L7 Services > L4-L7 Devices**, right-click and select **Create an L4-L7 Device**, and then complete these steps:

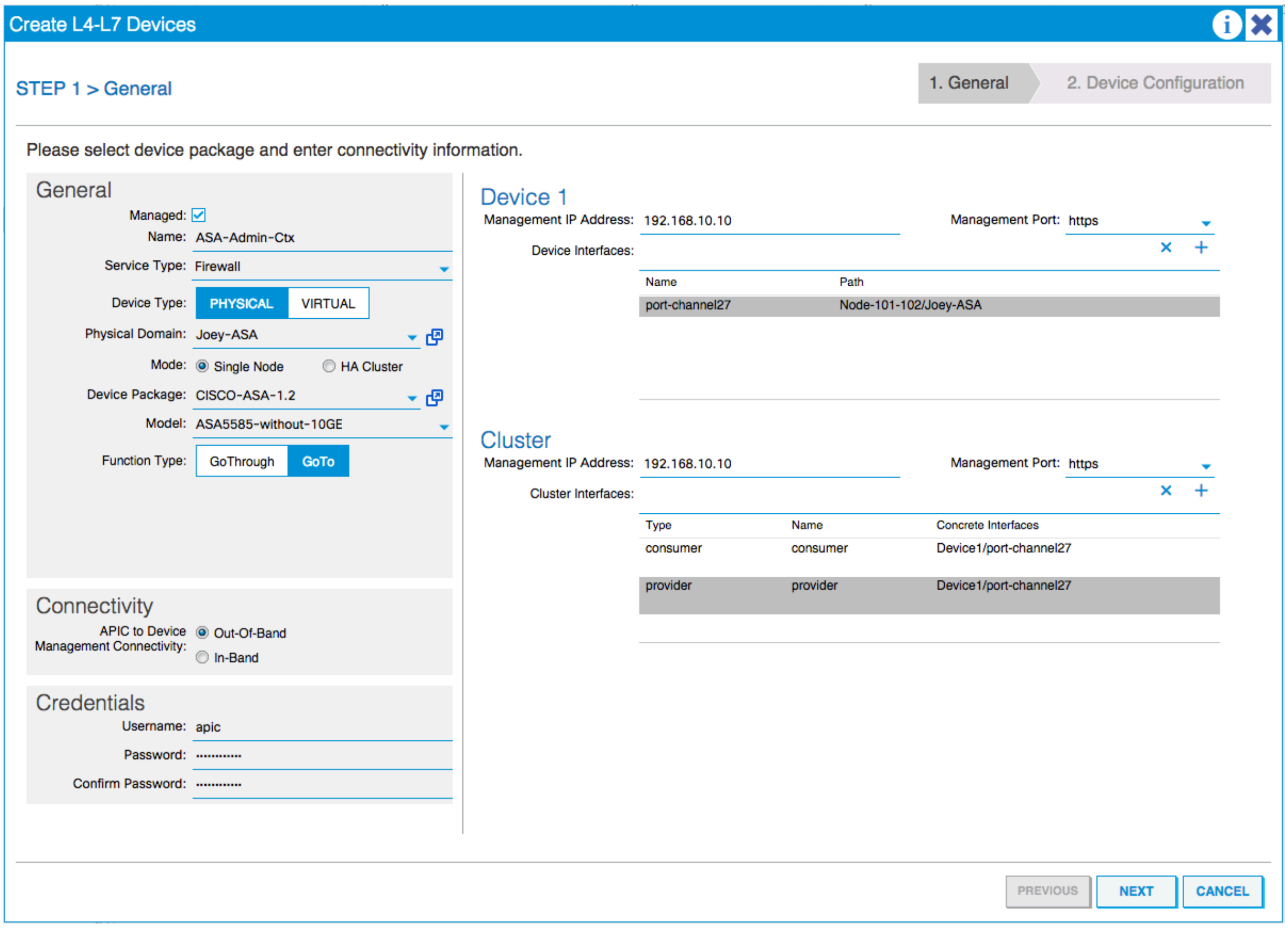
1. Click the **Managed** check box in the *General* area, if it is not already enabled.
2. Enter the device *Name*.
3. Select the *Service Type* from the drop-down menu.
4. Choose the *Device Type* (**PHYSICAL** or **VIRTUAL**).
5. Select the *Physical Domain* from the drop-down menu.
6. Choose the *Mode*.
7. Select **CISCO-ASA-1.2** from the *Device Package* drop-down menu.
8. Select the ASA *Model* from the drop-down menu.
9. Choose the *Function Type* (**GoThrough** is *Transparent* mode and **GoTo** is *Routed* mode).
10. Choose an **APIC to Device Management Connectivity** option in the *Connectivity* area.

11. Enter your **Username** and **Password** in the *Credentials* area.

12. Enter the IP address of the Admin context into the *Management IP Address* field (along with the *Port*) in the *Device 1* area.

13. Create a physical interface, give it a name, choose the *Interface Policy Group* that the ASA uses, and then select **Provider and consumer**.

14. Enter the same information that you used for the *Device 1* area into the *Cluster* area. Create two cluster interfaces (one *consumer* and one *provider*) that point to the same port-channel.



Create L4-L7 Devices

STEP 1 > General

1. General | 2. Device Configuration

Please select device package and enter connectivity information.

General

Managed: ☑

Name: ASA-Admin-Ctx

Service Type: Firewall

Device Type: PHYSICAL | VIRTUAL

Physical Domain: Joey-ASA

Mode: ● Single Node ○ HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASA5585-without-10GE

Function Type: GoThrough | GoTo

Connectivity

APIC to Device Management Connectivity: ● Out-Of-Band ○ In-Band

Credentials

Username: apic

Password: ············

Confirm Password: ············

Device 1

Management IP Address: 192.168.10.10 Management Port: https

Device Interfaces:

Name	Path
port-channel27	Node-101-102/Joey-ASA

Cluster

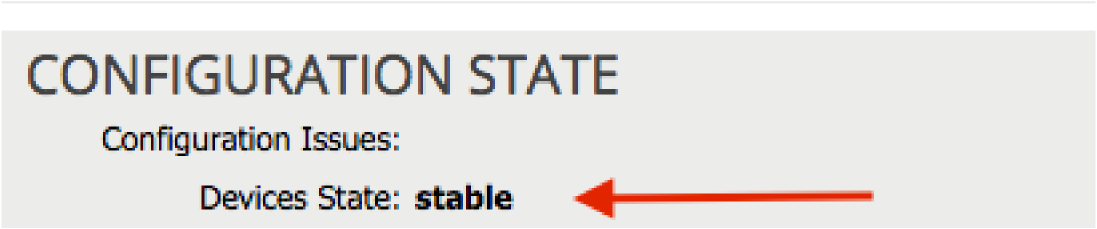
Management IP Address: 192.168.10.10 Management Port: https

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	consumer	Device1/port-channel27
provider	provider	Device1/port-channel27

Note: You can finish you use of the wizard at this time. You do not need to configure any of the failover information.

15. Verify that the device is stable and that there are no faults:



CONFIGURATION STATE

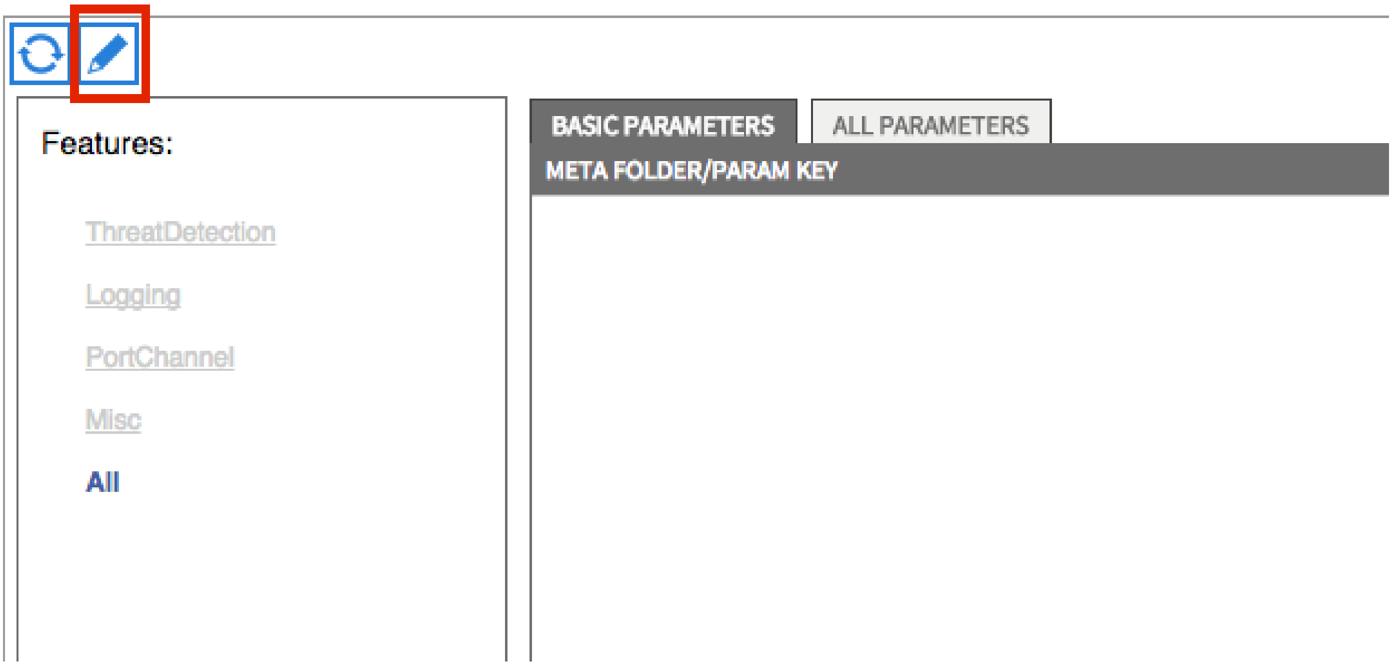
Configuration Issues:

Devices State: **stable**

Configure the Port-Channel Parameters

After the device is registered with the fabric, the APIC can push the configuration via the device parameters. After registration, you must first configure the port-channel that connects the ASA to the leaf switches in a Virtual Port Channel (vPC).

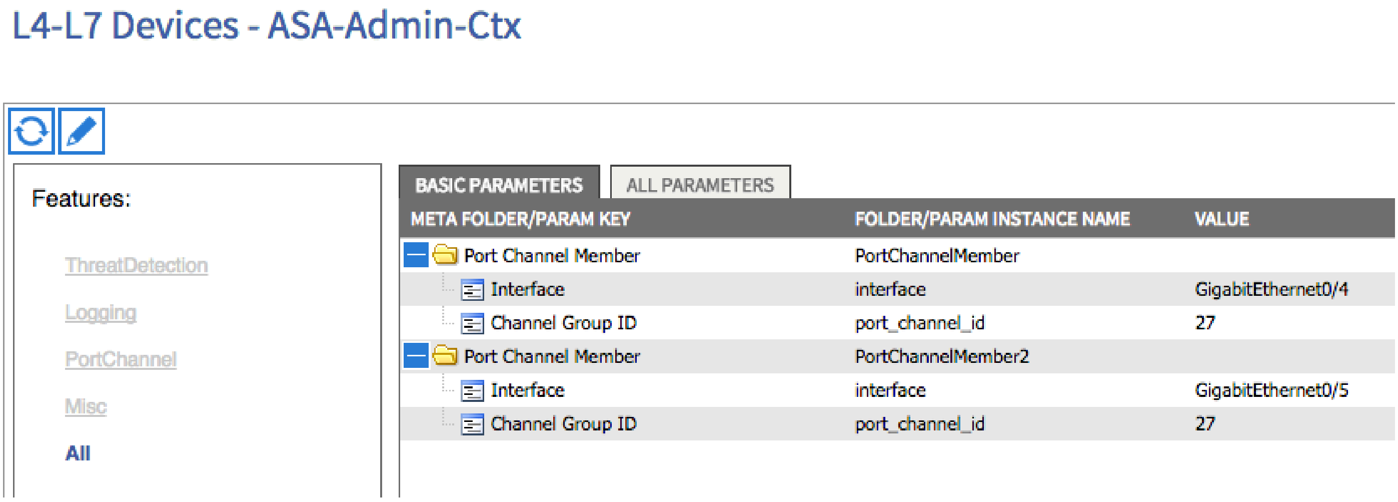
In order to configure the port-channel, navigate to the device that you created and click the **Parameters** tab in the upper corner of the work pane. Click the *pencil* icon in order to modify the parameters:



The *Edit Cluster Parameters* window appears. Click **PortChannel** in order to limit the scope of the option. Expand the **Port Channel Member** folder and complete the *Configuration Options*. Here is an explanation of each option:

- *Channel Group ID* – In the *Value* field, enter the PC ID that you wish to assign to the interfaces on the ASA (1 through 48 are supported).
- *Interface* – In the *Value* field, enter the interface on the ASA that you wish to assign to the channel group.

Repeat this process for each interface that you wish to assign:



META FOLDER/PARAM KEY	FOLDER/PARAM INSTANCE NAME	VALUE
Port Channel Member	PortChannelMember	
Interface	interface	GigabitEthernet0/4
Channel Group ID	port_channel_id	27
Port Channel Member	PortChannelMember2	
Interface	interface	GigabitEthernet0/5
Channel Group ID	port_channel_id	27

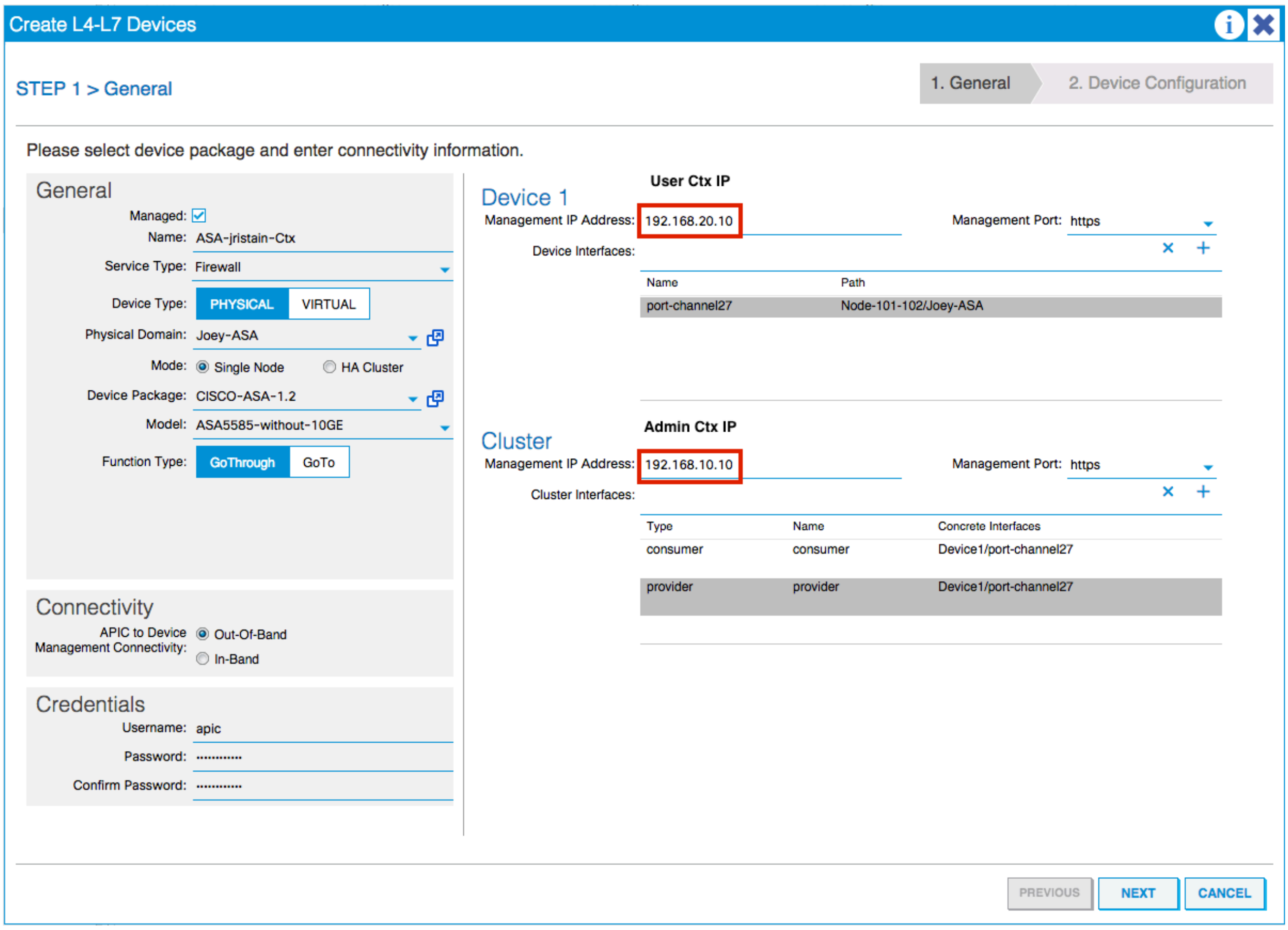
Once complete, you should see a port-channel creation on the ASA in the System context. In order to verify this, access the System context and enter the **show port-channel summary** command:

```
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)
```

Add the User Context as an L4-L7 Device

You must register the User context as an L4-L7 device in the fabric. Navigate to **Tenant > L4-L7 Services > L4-L7 Devices**, right-click and select **Create an L4-L7 Device**, and then complete these steps:

1. Click the **Managed** check box in the *General* area, if it is not already enabled.
2. Enter the device *Name*.
3. Select the *Service Type* from the drop-down menu.
4. Choose the *Device Type*.
5. Select the *Physical Domain* from the drop-down menu.
6. Choose the *Mode*.
7. Select **CISCO-ASA-1.2** from the *Device Package* drop-down menu.
8. Select the ASA *Model* from the drop-down menu.
9. Choose an **APIC to Device Management Connectivity** option in the *Connectivity* area.
10. Choose the *Function Type* (**GoThrough** is *Transparent* mode and **GoTo** is *Routed* mode).
11. Enter your **Username** and **Password** in the *Credentials* area.
12. Enter the IP address of the User context into the *Management IP Address* field (along with the *Port*) in the *Device 1* area.
13. Create a physical interface, give it a name, choose the *Interface Policy Group* that the ASA uses, and then select **Provider and consumer**.
14. Enter the *Management IP Address* of the Admin context (along with the Port) in the *Cluster* area. Create two cluster interfaces (one *consumer* and one *provider*) that point to the same port-channel.



Create L4-L7 Devices

STEP 1 > General

1. General | 2. Device Configuration

Please select device package and enter connectivity information.

General

Managed: ☑

Name: ASA-jristain-Ctx

Service Type: Firewall

Device Type: [✓ PHYSICAL] VIRTUAL

Physical Domain: Joey-ASA

Mode: ● Single Node ○ HA Cluster

Device Package: CISCO-ASA-1.2

Model: ASA5585-without-10GE

Function Type: [✓ GoThrough] GoTo

Connectivity

APIC to Device Management Connectivity: ● Out-Of-Band ○ In-Band

Credentials

Username: apic

Password: ············

Confirm Password: ············

User Ctx IP

Device 1

Management IP Address: 192.168.20.10

Management Port: https

Device Interfaces:

Name	Path
port-channel27	Node-101-102/Joey-ASA

Admin Ctx IP

Cluster

Management IP Address: 192.168.10.10

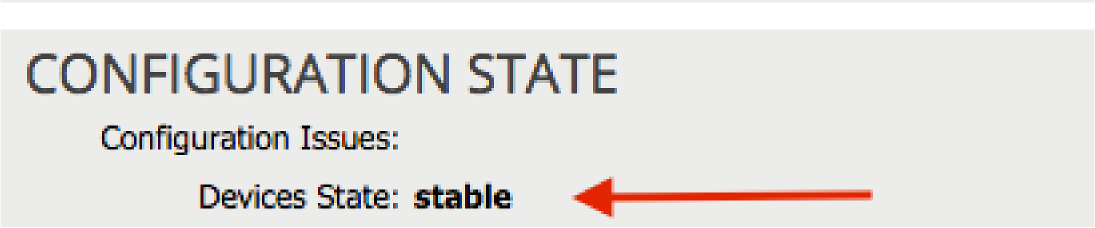
Management Port: https

Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	consumer	Device1/port-channel27
provider	provider	Device1/port-channel27

Note: You can finish you use of the wizard at this time. You do not need to configure any of the failover information.

15. Verify that the device is stable and that there are no faults:



CONFIGURATION STATE

Configuration Issues:

Devices State: **stable**

Add the NetScaler 1000V as an L4-L7 Device

The second node in this configuration example is a NetScaler 1000V. The NetScaler provides load balancing functionality to the connected servers. You must register this device with the APIC as well. Navigate to **Tenant > L4-L7 Services > L4-L7 Devices**, right-click and select **Create an L4-L7 Device**, and then complete these steps:

1. Click the **Managed** check box in the *General* area, if it is not already enabled.

2. Enter the device *Name*.

3. Select the *Service Type* from the drop-down menu (NetScaler is an *ADC*, or *Application Delivery Controller*).

4. Choose the *Device Type*.

5. Select the *VMM Domain* (if Virtual) from the drop-down menu.

6. Choose the *Mode*.

7. Select **Cisco-NetScaler1KV-1.0** from the *Device Package* drop-down menu.

8. Select the *Model* from the drop-down menu (Virtual Appliance is the *NetScaler-VPX*)

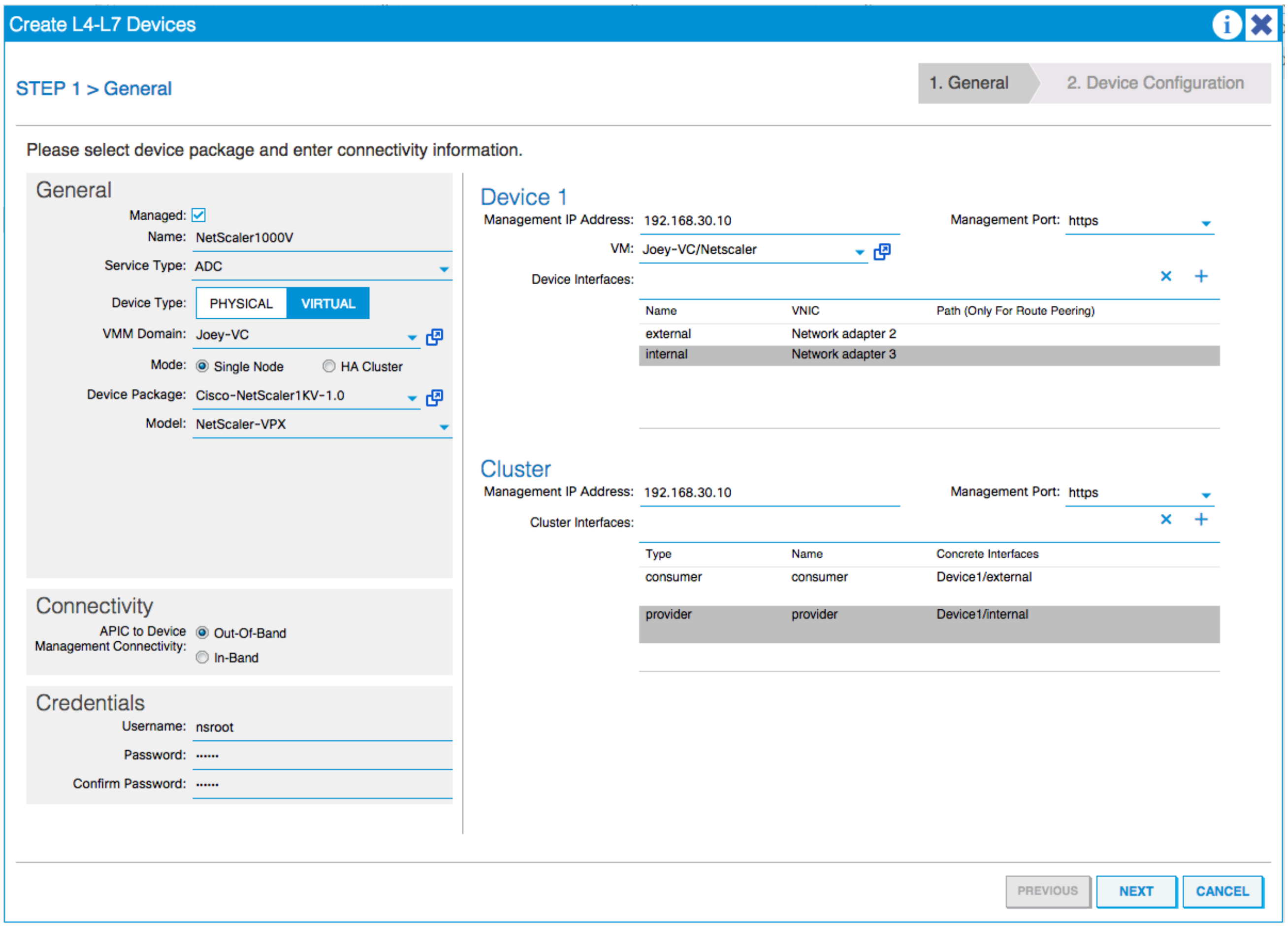
9. Choose an **APIC to Device Management Connectivity** option in the *Connectivity* area.

10. Enter your **Username** and **Password** in the *Credentials* area.

11. Enter the IP address of the Admin context into the *Management IP Address* field (along with the *Port*) in the *Device 1* area. Choose the VM (if Virtual).

12. Create an *external* interface in the *Device Interfaces* area, and choose an unused network adapter. **Note**: *Network Adapter 1* is used for management purposes, so do not use it.
13. Create an *internal* interface in the *Device Interfaces* area, and choose an unused network adapter.

14. Enter the same information that you used for the *Device 1* area into the *Cluster* area. Create two cluster interfaces (one *consumer* and one *provider*).



Please select device package and enter connectivity information.

General

Managed: ☑
Name: NetScaler1000V
Service Type: ADC
Device Type: PHYSICAL [✓ VIRTUAL]
VMM Domain: Joey-VC
Mode: ● Single Node ○ HA Cluster
Device Package: Cisco-NetScaler1KV-1.0
Model: NetScaler-VPX

Connectivity

APIC to Device Management Connectivity: ● Out-Of-Band ○ In-Band

Credentials

Username: nsroot
Password: ••••••
Confirm Password: ••••••

Device 1

Management IP Address: 192.168.30.10
Management Port: https
VM: Joey-VC/Netscaler
Device Interfaces:

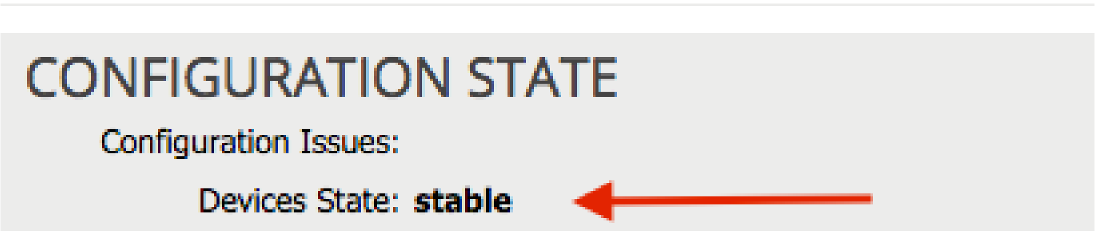
Name	VNIC	Path (Only For Route Peering)
external	Network adapter 2	
internal	Network adapter 3	

Cluster

Management IP Address: 192.168.30.10
Management Port: https
Cluster Interfaces:

Type	Name	Concrete Interfaces
consumer	consumer	Device1/external
provider	provider	Device1/internal

15. Verify that the device is stable and that there are no faults:



CONFIGURATION STATE

Configuration Issues:

Devices State: **stable**

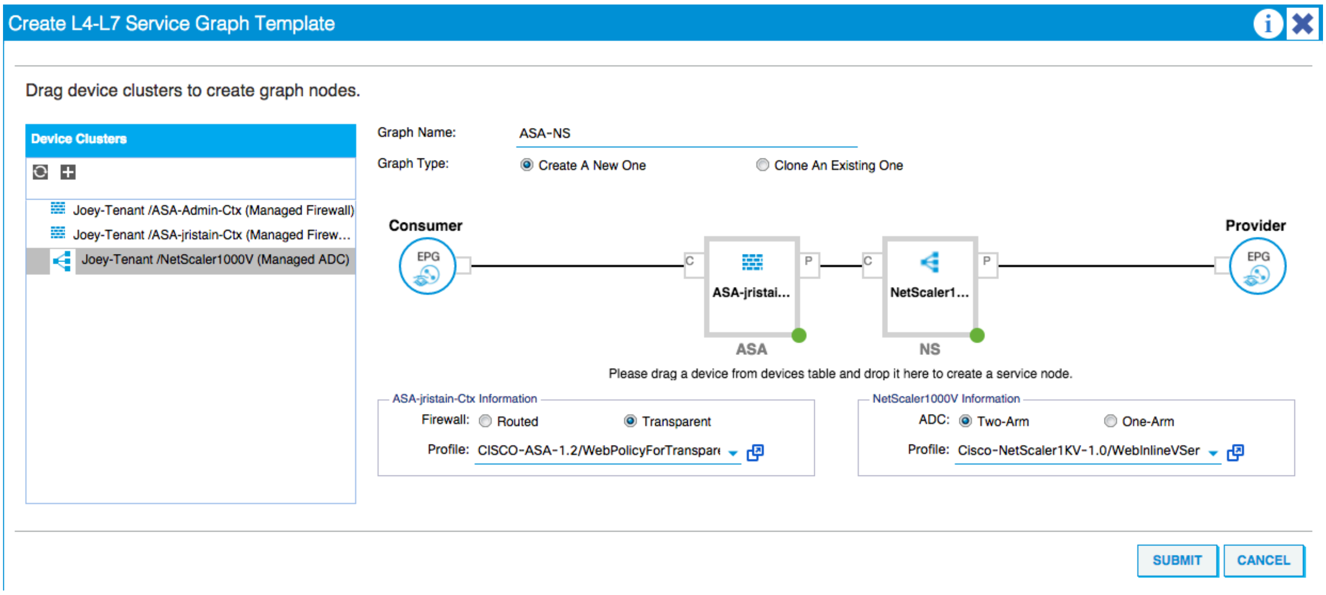
Create the Service Graph Template

Now that the devices are registered, you can create a *Service Graph Template*. Navigate to **Tenant > L4-L7 Services > L4-L7 Service Graph Templates > Create L4-L7** , and complete these steps:

1. Enter a name in the *Graph Name* field.

2. Drag-and-drop the devices from the *Device Clusters* area in the order that they should be deployed. Enter a name for each.

3. Choose the function *Profile* for each device. For the NetScaler, this example uses **Two-Arm** (or *Inline* mode).



Create L4-L7 Service Graph Template

Drag device clusters to create graph nodes.

Device Clusters

- Joey-Tenant /ASA-Admin-Ctx (Managed Firewall)
- Joey-Tenant /ASA-jristain-Ctx (Managed Firew...
- Joey-Tenant /NetScaler1000V (Managed ADC)

Graph Name: ASA-NS

Graph Type: ● Create A New One ○ Clone An Existing One

Please drag a device from devices table and drop it here to create a service node.

ASA-jristain-Ctx Information

Firewall: ○ Routed ● Transparent

Profile: CISCO-ASA-1.2/WebPolicyForTranspare

NetScaler1000V Information

ADC: ● Two-Arm ○ One-Arm

Profile: Cisco-NetScaler1KV-1.0/WebInlineVSer

Deploy the Service Graph Template

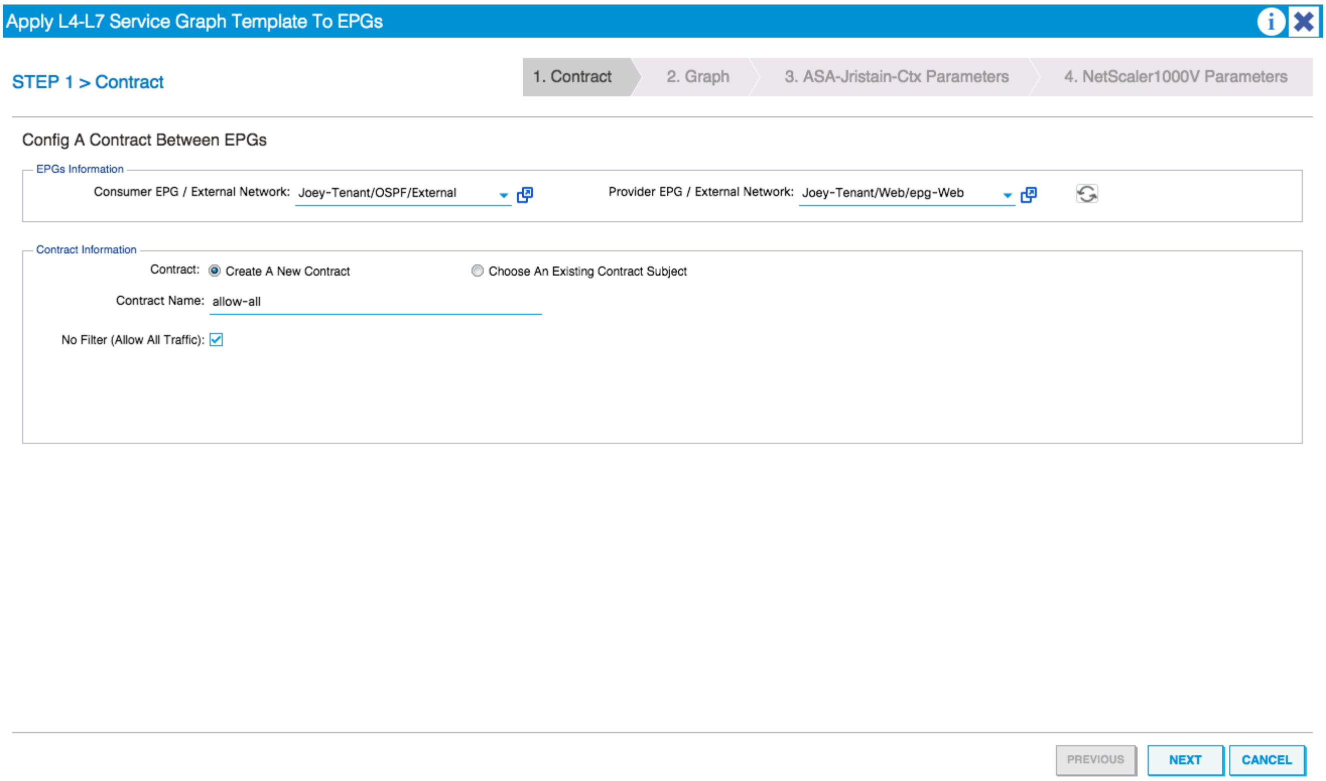
After the template is created, you can deploy it to the devices. Navigate to **Tenant > L4-L7 Services > L4-L7 Service Graph Templates > Service Graph Template > Apply Service Graph Template**.

On the *Contract* tab, complete these steps:

1. Select the consumer EPG from the *Consumer EPG / External Network* drop-down menu.

2. Select the provider EPG from the *Provider EPG / External Network* drop-down menu.

3. Create a new contract, or choose one that already exists, in the *Contract Information* area.



Apply L4-L7 Service Graph Template To EPGs

STEP 1 > Contract

1. Contract | 2. Graph | 3. ASA-Jristain-Ctx Parameters | 4. NetScaler1000V Parameters

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: Joey-Tenant/OSPF/External

Provider EPG / External Network: Joey-Tenant/Web/epg-Web

Contract Information

Contract: ● Create A New Contract ○ Choose An Existing Contract Subject

Contract Name: allow-all

No Filter (Allow All Traffic): ☑

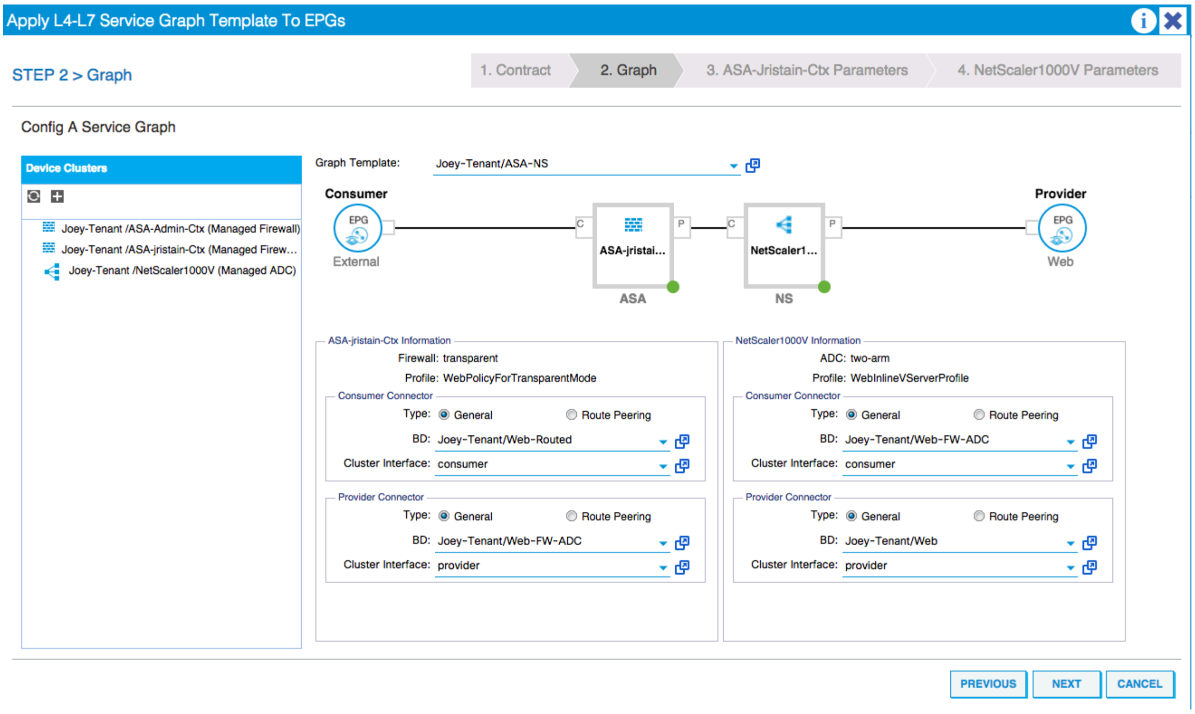
On the *Graph* tab, complete these steps:

1. Select the BD for the ASA external interface from the *BD* drop-down menu.

2. Select the BD For the ASA internal interface from the *BD* drop-down menu.

3. Select the BD for the NetScaler external interface from the *BD* drop-down menu.

4. Select the BD for the NetScaler internal interface from the *BD* drop-down menu.



Apply L4-L7 Service Graph Template To EPGs

STEP 2 > Graph

1. Contract | 2. Graph | 3. ASA-Jristain-Ctx Parameters | 4. NetScaler1000V Parameters

Config A Service Graph

Device Clusters

- Joey-Tenant /ASA-Admin-Ctx (Managed Firewall)
- Joey-Tenant /ASA-jristain-Ctx (Managed Firew...
- Joey-Tenant /NetScaler1000V (Managed ADC)

Graph Template: Joey-Tenant/ASA-NS

ASA-jristain-Ctx Information

Firewall: transparent

Profile: WebPolicyForTransparentMode

Consumer Connector

Type: ● General ○ Route Peering

BD: Joey-Tenant/Web-Routed

Cluster Interface: consumer

Provider Connector

Type: ● General ○ Route Peering

BD: Joey-Tenant/Web-FW-ADC

Cluster Interface: provider

NetScaler1000V Information

ADC: two-arm

Profile: WebInlineVServerProfile

Consumer Connector

Type: ● General ○ Route Peering

BD: Joey-Tenant/Web-FW-ADC

Cluster Interface: consumer

Provider Connector

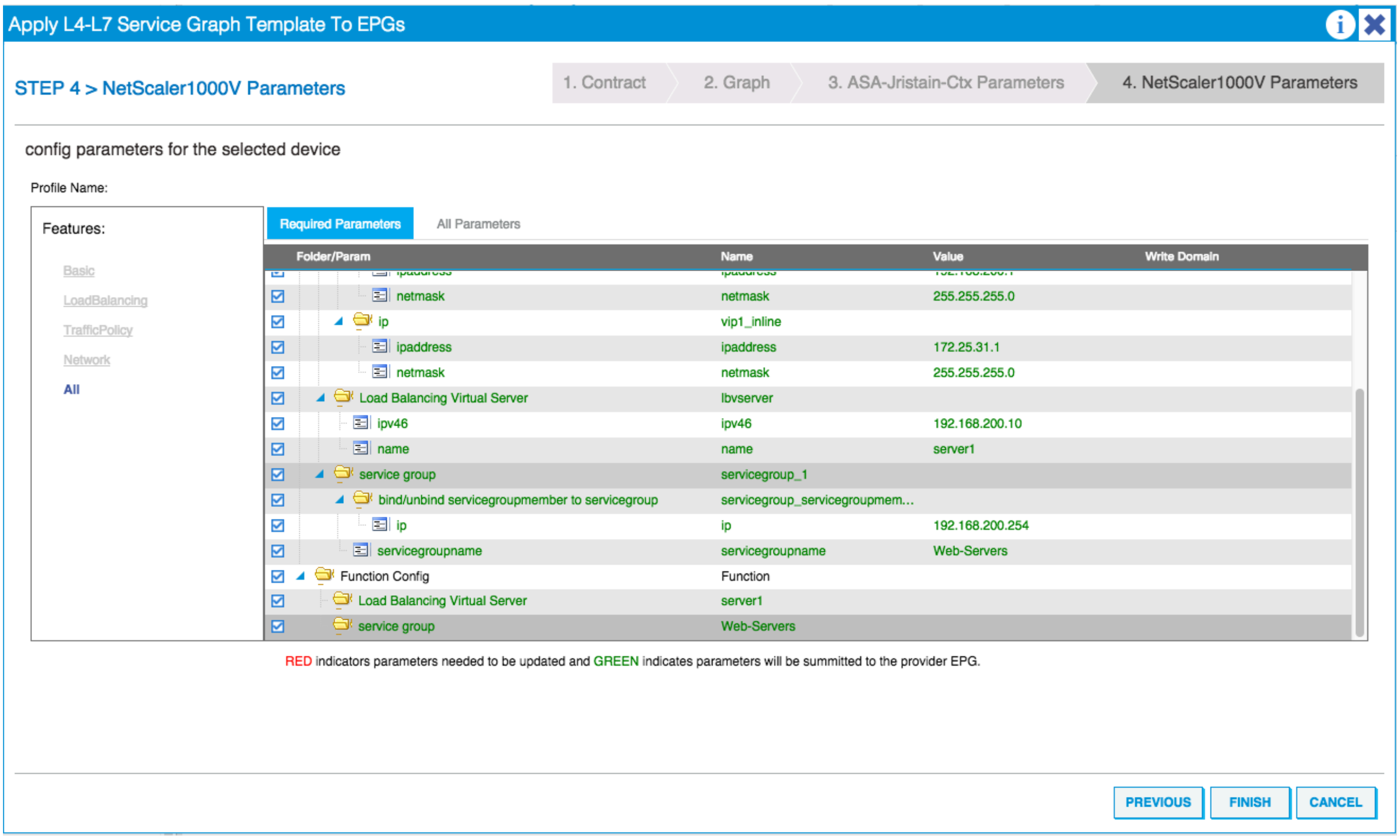
Type: ● General ○ Route Peering

BD: Joey-Tenant/Web

Cluster Interface: provider

On the *ASA Parameters* tab, enter the desired parameters. None of the parameters on this tab are required.

On the *NetScaler Parameters* tab, enter the NetScaler configuration via the wizard:


Apply L4-L7 Service Graph Template To EPGs
1. Contract
2. Graph
3. ASA-Jristain-Ctx Parameters
4. NetScaler1000V Parameters
Required Parameters
All Parameters
PREVIOUS
FINISH
CANCEL

STEP 4 > NetScaler1000V Parameters

config parameters for the selected device

Profile Name:

Features:

- Basic
- LoadBalancing
- TrafficPolicy
- Network
- All

	Folder/Param	Name	Value	Write Domain
☑	ipaddress	ipaddress	192.168.200.1	
☑	netmask	netmask	255.255.255.0	
☑	ip	vip1_inline		
☑	ipaddress	ipaddress	172.25.31.1	
☑	netmask	netmask	255.255.255.0	
☑	Load Balancing Virtual Server	lbvserver		
☑	ipv46	ipv46	192.168.200.10	
☑	name	name	server1	
☑	service group	servicegroup_1		
☑	bind/unbind servicegroupmember to servicegroup	servicegroup_servicegroupmem...		
☑	ip	ip	192.168.200.254	
☑	servicegroupname	servicegroupname	Web-Servers	
☑	Function Config	Function		
☑	Load Balancing Virtual Server	server1		
☑	service group	Web-Servers		

RED indicators parameters needed to be updated and GREEN indicates parameters will be summitted to the provider EPG.

Verify

There is currently no verification procedure available for this configuration.

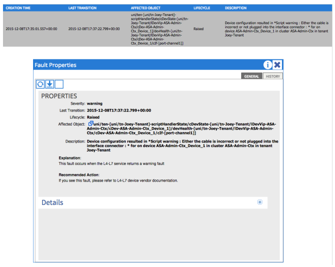
Troubleshoot

This section provides information that you can use in order to troubleshoot your configuration.

Known Faults

Here are two known faults that are related to the configurations that are described in this document:

- **Script Warning: Either the cable is incorrect or not plugged into the interface connector**:



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

Fault Properties

PROPERTIES

Severity: **warning**
Last Transition: **2015-12-08T17:37:22.799+00:00**
Lifecycle: **Raised**
Affected Object: **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]]**
Description: **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**

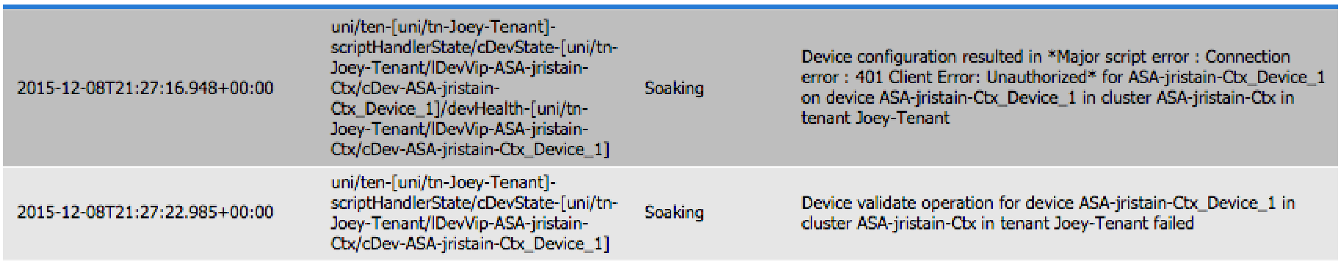
Explanation:
This fault occurs when the L4-L7 service returns a warning fault

Recommended Action:
If you see this fault, please refer to L4-L7 device vendor documentation.

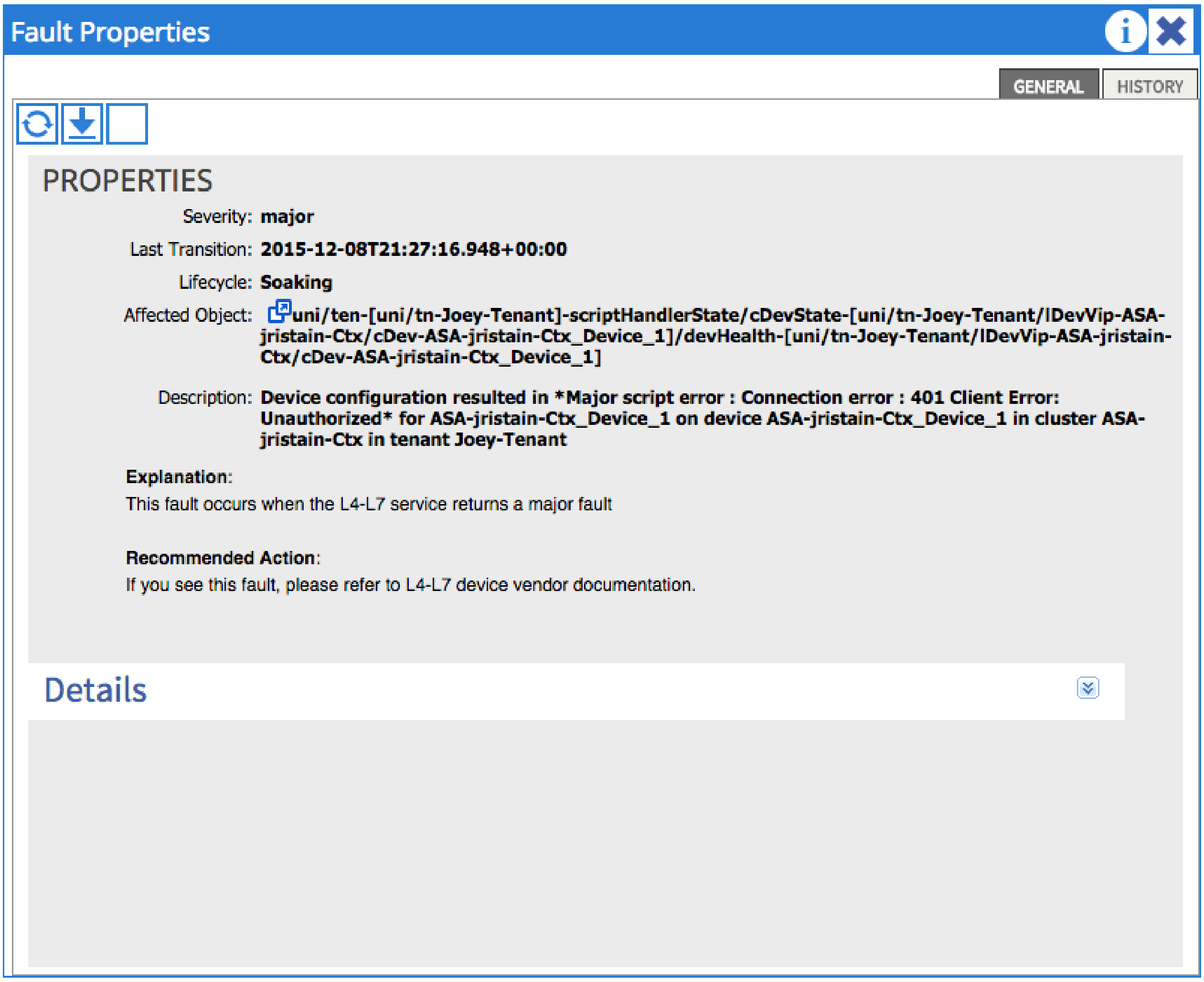
In order to resolve this issue, ensure that the port-channel parameters are configured and that the port-channel is up on the ASA. Refer to the Configure the Port-Channel Parameters section of this document for information about how to verify this.

If the interface is up, but you still see these faults, it is likely due to Cisco bug ID CSCuw56882. This bug is fixed in the *1.2.3 Device Package* support for the 1.2(x) ACI software release. The device packages can be downloaded here.

- **Major Script Error: Connection error : 401 Client Error: Unauthorized**:



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



PROPERTIES

Severity: **major**

Last Transition: **2015-12-08T21:27:16.948+00:00**

Lifecycle: **Soaking**

Affected Object: **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]**

Description: **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**

Explanation:
This fault occurs when the L4-L7 service returns a major fault

Recommended Action:
If you see this fault, please refer to L4-L7 device vendor documentation.

Details

In order to resolve this issue, ensure that the proper credentials are provisioned on the devices and configured correctly in the APIC.