

Configuration et déploiement d'un graphique de services à deux noeuds avec ASA Multi-Context et NetScaler 1000V

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configuration de l'ASA](#)

[Activer la prise en charge multicontexte sur l'ASA](#)

[Configurer le contexte utilisateur sur l'ASA](#)

[Configurer l'adresse IP de gestion pour le contexte utilisateur](#)

[Configurer le démarrage requis pour le contrôleur APIC](#)

[Configurer le contrôleur APIC](#)

[Configurer les domaines de pont requis](#)

[Configurer les groupes de terminaux requis](#)

[Ajouter le contexte Admin en tant que périphérique L4-L7](#)

[Configurer les paramètres Port-Channel](#)

[Ajouter le contexte utilisateur en tant que périphérique L4-L7](#)

[Ajouter le NetScaler 1000V en tant que périphérique L4-L7](#)

[Créer un modèle de graphique de service](#)

[Déployer le modèle de graphique de services](#)

[Vérification](#)

[Dépannage](#)

[Erreurs connues](#)

Introduction

Ce document décrit comment configurer et déployer un graphique de services à deux noeuds au sein de la plate-forme ACI (Application Centric Infrastructure) de Cisco. Les deux périphériques utilisés dans le graphique des services sont un appareil de sécurité adaptatif (ASA) Cisco physique qui fonctionne en mode *transparent* et un appareil virtuel Citrix NetScaler 1000V.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître ces rubriques avant de tenter la configuration décrite dans ce document :

- Fabric Cisco ACI composé de deux commutateurs dorsaux et de deux commutateurs Leaf
- Domaines gérés par les machines virtuelles Cisco (VMM)
- Cisco ASA
- Appareils virtuels NetScaler 1000V

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Structure ACI composée de deux commutateurs dorsaux et de deux commutateurs Leaf qui exécutent le code version 1.1(4e) ou ultérieure, et du package de périphériques version 1.2 ou ultérieure
- Un domaine VMM configuré dans l'ACI pour VMWare
- Un ASA physique avec deux connexions (une connexion à chaque commutateur Leaf)
- Appliance virtuelle NetScaler 1000V déployée dans VMWare vCenter
- Un contrôleur Cisco APIC (Application Policy Infrastructure Controller)

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.

Configuration

Cette section décrit comment configurer les différents composants impliqués dans ce déploiement.

Configuration de l'ASA

Cette section décrit comment terminer la configuration sur l'ASA.

Activer la prise en charge multicontexte sur l'ASA

Pour créer plusieurs contextes sur l'ASA, vous devez activer la fonctionnalité. Connectez-vous à l'ASA et entrez cette commande en mode *Configuration* :

```
ciscoasa(config)#
```

```
mode multiple
```

Vous êtes alors invité à recharger. Une fois le périphérique rechargé, vous pouvez continuer à créer le contexte *utilisateur*.

Note: Un contexte *Admin* doit être créé avant les contextes Utilisateur. Ce document ne décrit pas comment créer le contexte Admin, mais plutôt le contexte Utilisateur. Pour plus d'informations sur la création du contexte Admin, référez-vous à la section [Configuration de contextes multiples](#) du *Guide de configuration CLI de la gamme Cisco ASA, 9.0*.

Configurer le contexte utilisateur sur l'ASA

Afin de créer le contexte Utilisateur sur l'ASA, entrez cette commande à partir du contexte *système* :

```
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
```

Cette configuration crée le contexte, alloue l'interface de gestion à utiliser dans ce contexte et spécifie un emplacement pour le fichier de configuration. Vous devez maintenant entrer ce contexte afin de configurer le bootstrap minimal requis pour que le contrôleur APIC puisse se connecter.

Configurer l'adresse IP de gestion pour le contexte utilisateur

Une fois le contexte Utilisateur créé, vous pouvez le modifier et configurer l'adresse IP de gestion sur l'interface allouée. Sélectionnez ces commandes :

```
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: L'entrée *name* doit être *management* car c'est l'attente du package de périphérique. Si l'entrée *name* contient des caractères supplémentaires, vous verrez des erreurs dans le déploiement du périphérique L4-L7 dans l'APIC.

Configurer le démarrage requis pour le contrôleur APIC

Pour connecter le contrôleur APIC à l'ASA, une configuration minimale est requise. Cela inclut le serveur HTTP et un compte utilisateur pour le contrôleur APIC. Utilisez cette configuration dans le contexte Utilisateur :

```
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: Entrez votre nom d'utilisateur et votre mot de passe dans les zones **<nom d'utilisateur>** et **<mot de passe>**.

Configurer le contrôleur APIC

Cette section décrit comment effectuer la configuration sur le contrôleur APIC.

Configurer les domaines de pont requis

Trois domaines de pont (BD) sont nécessaires pour déployer un graphique de services à deux nœuds.

Utilisez ces informations afin de configurer le BD pour l'interface ASA externe (consommateur) :

- *L2 Unknown Unicast - Inondation*
- *Inondation ARP - activée*
- Le sous-réseau peut être configuré afin d'agir comme passerelle par défaut pour l'interface externe NetScaler avec *Routage monodiffusion* **activé**

Utilisez ces informations afin de configurer le BD qui est utilisé afin de connecter les deux périphériques :

- *L2 Unknown Unicast - Inondation*
- *Inondation ARP - activée*

- *Routage monodiffusion* - **Désactivé**

Configurer les groupes de terminaux requis

Le graphique de service nécessite la configuration de deux groupes de terminaux (EPG) : un consommateur et un fournisseur. Le groupe de terminaux grand public doit utiliser la BD qui se connecte à l'interface ASA externe. L'EPG du fournisseur doit utiliser un BD qui se connecte aux serveurs d'extrémité.

Ajouter le contexte Admin en tant que périphérique L4-L7

Vous devez ajouter les contextes utilisateur et administrateur ASA au contrôleur APIC. Pour effectuer cette opération, accédez à **Locataire > Services L4-L7 > Périphériques L4-L7**, cliquez avec le bouton droit de la souris et sélectionnez **Créer un périphérique L4-L7**, puis procédez comme suit :

1. Cochez la case **Gestion** dans la zone *Général*, si elle n'est pas déjà activée.
2. Entrez le *nom* du périphérique.
3. Sélectionnez le *type de service* dans le menu déroulant.
4. Sélectionnez le *type de périphérique* (**PHYSIQUE** ou **VIRTUEL**).
5. Sélectionnez le *domaine physique* dans le menu déroulant.
6. Sélectionnez le *mode*.
7. Sélectionnez **CISCO-ASA-1.2** dans le menu déroulant *Package de périphériques*.
8. Sélectionnez le *modèle* ASA dans le menu déroulant.
9. Choisissez le type de fonction (**GoThrough** est *transparent* et **GoTo** est *roulé*).
10. Choisissez une option **APIC to Device Management Connectivity** dans la zone *Connectivity*.
11. Entrez votre **nom d'utilisateur** et votre **mot de passe** dans la zone *Informations d'identification*.
12. Entrez l'adresse IP du contexte Admin dans le champ *Management IP Address* (avec le *port*) de la zone *Device 1*.
13. Créez une interface physique, donnez-lui un nom, choisissez le *groupe de stratégies d'interface* que l'ASA utilise, puis sélectionnez **Fournisseur et consommateur**.
14. Entrez les mêmes informations que celles utilisées pour la zone *Périphérique 1* dans la zone *Cluster*. Créez deux interfaces de cluster (un *consommateur* et un *fournisseur*) qui pointent vers le même canal de port.

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

PREVIOUS NEXT CANCEL

Note: Vous pouvez terminer l'utilisation de l'Assistant à ce stade. Vous n'avez pas besoin de configurer les informations de basculement.

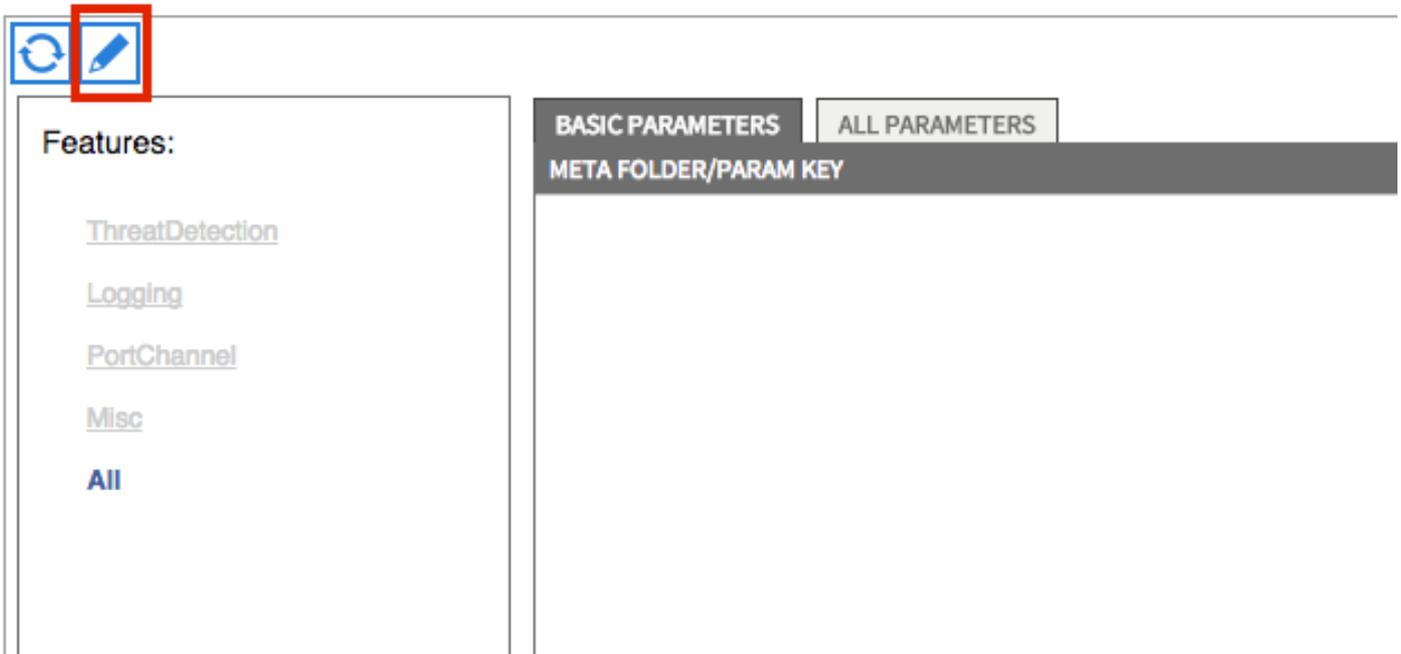
15. Vérifiez que le périphérique est stable et qu'il n'y a pas de défaillance :



Configurer les paramètres Port-Channel

Une fois le périphérique enregistré dans la structure, l'APIC peut transmettre la configuration via les paramètres du périphérique. Après l'enregistrement, vous devez d'abord configurer le port-channel qui connecte l'ASA aux commutateurs Leaf dans un Virtual Port Channel (vPC).

Afin de configurer le canal de port, accédez au périphérique que vous avez créé et cliquez sur l'onglet **Paramètres** dans le coin supérieur du volet de travail. Cliquez sur l'icône *crayon* afin de modifier les paramètres :

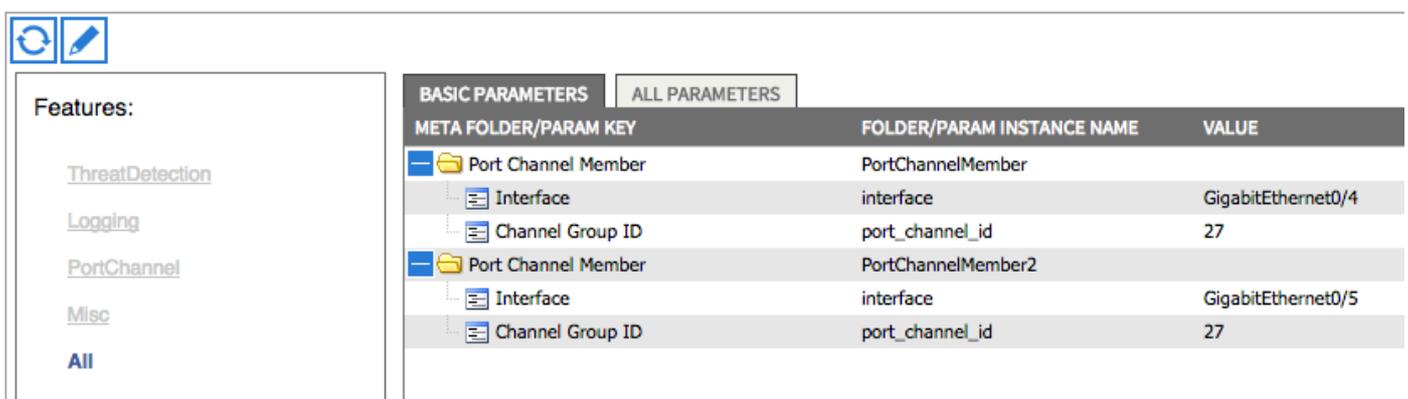


La fenêtre *Modifier les paramètres du cluster* apparaît. Cliquez sur **PortChannel** afin de limiter la portée de l'option. Développez le dossier **Port Channel Member** et complétez les *options de configuration*. Voici une explication de chaque option :

- *ID de groupe de canaux* - Dans le champ *Valeur*, saisissez l'ID de PC que vous souhaitez attribuer aux interfaces de l'ASA (1 à 48 sont pris en charge).
- *Interface* - Dans le champ *Valeur*, saisissez l'interface sur l'ASA que vous souhaitez affecter au groupe de canaux.

Répétez ce processus pour chaque interface que vous souhaitez affecter :

L4-L7 Devices - ASA-Admin-Ctx



Une fois terminé, vous devriez voir une création de canal de port sur l'ASA dans le contexte du système. Afin de vérifier ceci, accédez au contexte système et entrez la commande **show port-channel summary** :

```
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)

Ajouter le contexte utilisateur en tant que périphérique L4-L7

Vous devez enregistrer le contexte utilisateur en tant que périphérique L4-L7 dans le fabric. Accédez à **Locataire > Services L4-L7 > Périphériques L4-L7**, cliquez avec le bouton droit de la souris et sélectionnez **Créer un périphérique L4-L7**, puis complétez ces étapes :

1. Cochez la case **Gestion** dans la zone *Général*, si elle n'est pas déjà activée.
2. Entrez le *nom* du périphérique.
3. Sélectionnez le *type de service* dans le menu déroulant.
4. Sélectionnez le *type de périphérique*.
5. Sélectionnez le *domaine physique* dans le menu déroulant.
6. Sélectionnez le *mode*.
7. Sélectionnez **CISCO-ASA-1.2** dans le menu déroulant *Device Package*.
8. Sélectionnez le *modèle ASA* dans le menu déroulant.
9. Choisissez une option **APIC to Device Management Connectivity** dans la zone *Connectivity*.
10. Choisissez le type de fonction (**GoThrough** est *transparent* et **GoTo** est *roulé*).
11. Entrez votre **nom d'utilisateur** et votre **mot de passe** dans la zone *Informations d'identification*.
12. Entrez l'adresse IP du contexte Utilisateur dans le champ *Management IP Address (Adresse IP de gestion)* (avec le *port*) de la zone *Device 1*.
13. Créez une interface physique, donnez-lui un nom, choisissez le *groupe de stratégies d'interface* que l'ASA utilise, puis sélectionnez **Fournisseur et consommateur**.
14. Entrez l'*adresse IP de gestion* du contexte Admin (avec le *port*) dans la zone *Cluster*. Créez deux interfaces de cluster (un *consommateur* et un *fournisseur*) qui pointent vers le même canal de port.

Create L4-L7 Devices

STEP 1 > General

1. General 2. Device Configuration

Please select device package and enter connectivity information.

General

Managed:

Name: ASA-jr1stain-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

User Ctx IP

Management IP Address: 192.168.20.10

Management Port: https

Device Interfaces:

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

Cluster

Admin Ctx IP

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

PREVIOUS NEXT CANCEL

Note: Vous pouvez terminer l'utilisation de l'Assistant à ce stade. Vous n'avez pas besoin de configurer les informations de basculement.

15. Vérifiez que le périphérique est stable et qu'il n'y a pas de défaillance :



Ajouter le NetScaler 1000V en tant que périphérique L4-L7

Le deuxième noeud de cet exemple de configuration est un NetScaler 1000V. NetScaler fournit des fonctionnalités d'équilibrage de charge aux serveurs connectés. Vous devez également enregistrer ce périphérique auprès du contrôleur APIC. Accédez à **Locataire > Services L4-L7 > Périphériques L4-L7**, cliquez avec le bouton droit de la souris et sélectionnez **Créer un périphérique L4-L7**, puis complétez ces étapes :

1. Cochez la case **Gestion** dans la zone *Général*, si elle n'est pas déjà activée.
2. Entrez le *nom* du périphérique.
3. Sélectionnez le *type de service* dans le menu déroulant (NetScaler est un *ADC*, ou *contrôleur de livraison d'applications*).

4. Sélectionnez le *type de périphérique*.
5. Sélectionnez le *domaine VMM* (si virtuel) dans le menu déroulant.
6. Sélectionnez le *mode*.
7. Sélectionnez **Cisco-NetScaler1KV-1.0** dans le menu déroulant *Package de périphériques*.
8. Sélectionnez le *modèle* dans le menu déroulant (Virtual Appliance is the *NetScaler-VPX*).
9. Choisissez une option **APIC to Device Management Connectivity** dans la zone *Connectivity*.
10. Entrez votre **nom d'utilisateur** et votre **mot de passe** dans la zone *Informations d'identification*.
11. Entrez l'adresse IP du contexte Admin dans le champ *Management IP Address* (avec le *port*) de la zone *Device 1*. Sélectionnez la machine virtuelle (si virtuelle).
12. Créez une interface *externe* dans la zone *Interfaces du périphérique* et choisissez une carte réseau inutilisée. **Note:** *L'adaptateur réseau 1* est utilisé à des fins de gestion. Ne l'utilisez donc pas.
13. Créez une interface *interne* dans la zone *Interfaces du périphérique* et choisissez une carte réseau inutilisée.
14. Entrez les mêmes informations que celles utilisées pour la zone *Périphérique 1* dans la zone *Cluster*. Créez deux interfaces de cluster (un *consommateur* et un *fournisseur*).

Create L4-L7 Devices

STEP 1 > General

1. General 2. Device Configuration

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

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

Connectivity

APIC to Device: Out-Of-Band In-Band

Management Connectivity: In-Band

Credentials

Username: nsroot

Password:

Confirm Password:

PREVIOUS NEXT CANCEL

15. Vérifiez que le périphérique est stable et qu'il n'y a pas de défaillance :



Créer un modèle de graphique de service

Maintenant que les périphériques sont enregistrés, vous pouvez créer un *modèle de graphique de service*. Accédez à **Service partagé > Services L4-L7 > Modèles de graphiques de services L4-L7 > Créer un modèle de graphique de services L4-L7**, puis complétez ces étapes :

1. Entrez un nom dans le champ *Nom du graphique*.
2. Faites glisser et déposez les périphériques de la zone *Clusters de périphériques* dans l'ordre dans lequel ils doivent être déployés. Entrez un nom pour chaque.
3. Choisissez le *profil* de fonction pour chaque périphérique. Pour NetScaler, cet exemple utilise le mode *bibras* (ou *en ligne*).

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:

Graph Type: Create A New One Clone An Existing One

ASA-jristain-Ctx Information

Firewall: Routed Transparent

Profile:

NetScaler1000V Information

ADC: Two-Arm One-Arm

Profile:

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

Déployer le modèle de graphique de services Une fois le modèle créé, vous pouvez le déployer sur les périphériques. Accédez à **Service partagé > Services de couches 4 à 7 > Modèles de graphiques de services de couches 4 à 7 > Modèle de graphique de services > Appliquer le modèle de graphique de services.** Dans l'onglet *Contrat*, procédez comme suit :

1. Sélectionnez l'EPG consommateur dans le menu déroulant *Consumer EPG / External Network*.
2. Sélectionnez l'EPG du fournisseur dans le menu déroulant *Provider EPG / External Network*.
3. Créez un nouveau contrat ou choisissez-en un qui existe déjà dans la zone *Informations sur le contrat*.

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:

Provider EPG / External Network:

Contract Information

Contract: Create A New Contract Choose An Existing Contract Subject

Contract Name:

No Filter (Allow All Traffic):

Dans l'onglet *Graphique*, procédez comme suit :

1. Sélectionnez le BD pour l'interface externe ASA dans le menu déroulant *BD*.
2. Sélectionnez le BD pour l'interface interne ASA dans le menu déroulant *BD*.

3. Sélectionnez le BD pour l'interface externe NetScaler dans le menu déroulant **BD**.

4. Sélectionnez le BD pour l'interface interne de NetScaler dans le menu déroulant **BD**.

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

Graph Template: Joey-Tenant/ASA-NS

Consumer: EPG External

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

PREVIOUS NEXT CANCEL

Dans l'onglet *Paramètres ASA*, saisissez les paramètres souhaités. Aucun des paramètres de cet onglet n'est requis. Dans l'onglet *Paramètres NetScaler*, saisissez la configuration NetScaler via l'assistant

:

Apply L4-L7 Service Graph Template To EPGs

STEP 4 > NetScaler1000V Parameters

1. Contract 2. Graph 3. ASA-Jristain-Ctx Parameters 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	lbserver		
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 submitted to the provider EPG.

PREVIOUS FINISH CANCEL

Vérification Aucune procédure de vérification n'est disponible pour cette

configuration. **Dépannage** Cette section fournit des renseignements qui vous permettront de régler les problèmes de configuration. **Erreurs connues** Voici deux défauts connus liés aux configurations décrites dans ce document :

- Avertissement de script : Le câble est incorrect ou n'est pas branché sur le connecteur d'interface :

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/IDevVip-ASA-Admin-Ctx_Device_1]/devHealth-[uni/tn-Joey-Tenant/IDevVip-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

Afin de résoudre ce problème, assurez-vous que les paramètres port-channel sont configurés et que le port-channel est actif sur l'ASA. Référez-vous à la section [Configurer les paramètres de canal de port](#) de ce document pour plus d'informations sur la façon de vérifier ceci.

Si l'interface est activée, mais que vous voyez toujours ces erreurs, elle est probablement due à l'ID de bogue Cisco [CSCuw56882](#). Ce bogue est corrigé dans la prise en charge *du package de périphériques 1.2(x)* pour la version du logiciel ACI 1.2(x). Les paquets de périphériques peuvent être téléchargés [ici](#).

- Erreur de script majeure : Erreur de connexion : 401 Erreur client : Non autorisé :

2015-12-08T21:27:16.948+00:00	uni/ten-[uni/tn-Joey-Tenant]-scriptHandlerState/cDevState-[uni/tn-Joey-Tenant/IDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1]/devHealth-[uni/tn-Joey-Tenant/IDevVip-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/IDevVip-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

Fault Properties i X

GENERAL HISTORY

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-\[uni/tn-Joey-Tenant/IDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1\]/devHealth-\[uni/tn-Joey-Tenant/IDevVip-ASA-jristain-Ctx/cDev-ASA-jristain-Ctx_Device_1\]](#)

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

Afin de résoudre ce problème, assurez-vous que les informations d'identification appropriées sont provisionnées sur les périphériques et configurées correctement dans le contrôleur APIC.