

Configuring VMware vCloud Director for Cisco ICFP

- Configuring VMware vCloud Director, page 1
- Workflow for Integrating VCD with Cisco ICFP, page 4
- Creating an External Network, page 5
- Adding a vShield Edge Gateway on an Org VDC, page 6
- Creating an Org VDC Internal Network, page 7
- Creating a Catalog, page 9
- Verifying NAT and Firewall Service Configuration, page 9
- Configuring Cisco ICFP for Cisco Intercloud Fabric, page 11

Configuring VMware vCloud Director

Installing Cisco ICFP at a cloud provider site enables you to support a hybrid cloud environment with Cisco Intercloud Fabric for Business. For VMware vCloud Director (VCD) environments, Cisco ICFP includes a built-in VCD adapter that enables Cisco ICFP to integrate with the VCD platform. This VCD-Cisco ICFP integration can be viewed as the infrastructure that binds the enterprise virtualization platform, such as VMware vCenter, to the provider cloud platform, VCD.

The following illustration depicts how Cisco Intercloud Fabric interfaces with the provider VCD platform through Cisco ICFP.



Figure 1: VCD and Cisco Intercloud Fabric Integration

The secure site-to-site tunnel illustrated in the image is created between an Intercloud Fabric Switch (ICS) on the provider cloud and an Intercloud Fabric Extender (ICX) on the private cloud. In addition to providing secure communications between the private and provider clouds, this site-to-site tunnel enables Cisco Intercloud Fabric Secure Extender to integrate with VCD for each tenant network.

Before the ICS and ICX can communicate via the Internet, you must:

- Assign a public IP address to the ICS so that the ICX can reach the ICS.
- Ensure that the vShield Edge Gateway provides NAT functionality so that the ICS can connect to the Internet.

The following figure shows an example deployment:

Figure 2: vShield Edge Gateway Deployment Example



A vShield Edge Gateway is an interconnecting appliance that provides many edge network service features, including:

- DHCP
- Firewall
- IPsec VPN
- Load-balancer
- NAT

I

• Static route

The following figure shows how Organization X connects the Org Network to an external network through a vShield Edge Gateway and directly to vApp networks.

Figure 3: VCD Networking Model



Workflow for Integrating VCD with Cisco ICFP

To integrate VCD with Cisco ICFP, you must provision certain infrastructure resources in the target VCD platform. The following table identifies the tasks required to provision these resources:

Step	Task	Related Information
1.	Ensure that the following prerequisites are met:	VMware VCD documentation
	• VCD version 5.5 is installed.	
	• You have access to the VCD system administrator account.	
2.	Create an external network.	Creating an External Network, on page 5
3.	Deploy the vShield Edge Gateway.	Adding a vShield Edge Gateway on an Org VDC, on page 6
4.	Create an Org VDC network.	Creating an Org VDC Internal Network, on page 7
5.	Create a catalog.	Creating a Catalog, on page 9
6.	Ensure that NAT and firewall services are configured on the vShield Edge Gateway.	Verifying NAT and Firewall Service Configuration, on page 9

For additional information on any of these topics, see your VMware documentation.

After you have successfully integrated VCD with Cisco ICFP, you can configure a cloud instance and add a tenant as described in Configuring Cisco ICFP for Cisco Intercloud Fabric, on page 11.

Creating an External Network

This procedure describes how to create an external network in a virtual data center (VDC).

Procedure

Slep I Log III to the VCD OUT as system administration	Step 1	the VCD GUI as system administr	ator.
--	--------	---------------------------------	-------

- Step 2 Choose System > Manage & Monitor > Cloud Resources > External Networks.
- Step 3In the External Networks pane, click Add.The New External Network wizard opens, guiding you through the configuration process.
- **Step 4** In the Select vSphere Network screen, choose the VDC vCenter and the DVS port group created for the vSphere management network, and click Next.
- **Step 5** In the Configure External Network screen, click Add.
- **Step 6** In the Add Subnet dialog box, enter the following information for the external network:
 - · Gateway IP address
 - Network mask
 - DNS server IP address
 - · Static IP address or IP address range

(TE) VN	New External Network						2 8
System Home	Select vSphere Network Configure External Network	Configure External Net Specify the network sett address ranges or IP a	work ings for this new exte ddresses using the S	ernal network. You can have this Static IP Pool control.	s network automatica	illy supply IP addresse	is to VMs in organizations by adding IP
Organ	Name this External Network	Osteway address	Subnet Mask	IP Pool (Used/Total)	Primary DNS	Secondary DNS	Static IP Pools
- Cloud Re	Ready to Complete			Add Subnet		 (a) (b) (c) (c)	
Pre Pre				Gateway address: 10.	2.0.1	•	
a or				Network mask: 255	5.255.0.0		
C Ed				Primary DNS: 171	1.70.168.183		
E Ne				Secondary DNS:			
- vSphere				DNS suffix			
ØvC				Static IP pool:			
E Ho				Enter an IP range (format: 19 address and click Add.	12.168.1.2 - 192.168.1.1	100) or IP	
E Dis				10.2.96.1-10.2.96.254		Add *	
E SM				10.2.96.1 - 10.2.96.254		Modify	
@ Str						Remove	
Block							
		Add					
073		(Total: 254			
NIN OR				-	ОК	Cancel	Next Finish Cancel

- Step 7 In the Name this External Network screen, enter a name for the external network, and click Next.
- **Step 8** In the **Ready to Complete** screen, review the content for accuracy and click **Finish**. The newly created external network is displayed in the **External Networks** pane.

Adding a vShield Edge Gateway on an Org VDC

You must add a vShield Edge Gateway to integrate the Provider VDC and Org VDC with Cisco ICFP.

Before You Begin

Confirm that the following have been configured:

- A Provider VDC
- An Org VDC
- An external network

Procedure

- Step 1 In the VCD GUI, choose System > Manage & Monitor > Cloud Resources > Organization VDCs.
- **Step 2** In the **Organization VDCs** table, double-click the Org VDC where the vShield Edge Gateway is to be added. The screen is refreshed with information about the selected VDC.
- Step 3Choose the Edge Gateways tab and click Add.The New Edge Gateway wizard opens, guiding you through the configuration process.
- **Step 4** In the **Configure Edge Gateway** screen, configure the vShield Edge Gateway for connectivity with the external network as follows, and then click **Next**:
 - a) Choose the required edge gateway configuration: Compact, Full, or Full-4.
 - b) If the edge gateway is to be configured for HA, check the Enable High Availability check box.
 - c) In the Advanced Options section, check the Sub-Allocate IP Pools check box.
- **Step 5** In the **External Networks** screen, choose the external network that you created in Creating an External Network, on page 5 and click **Add**. If the external network is not listed, create a new external network.

	New Edge Gateway					O
System vcd.org ×	Configure Edge Gateway	Configure External Network	ts to which the new edge ga	teway can connect.		
Administration Cloud Resources Cloud Resources	External Networks Sub-Allocate IP Poots Name and Description	If the external network is not	listed, you have to create	e a new external netwo	ork	C
Recent items	Summary	Name 1	IP Pool (Used/Total)		Vaphere Network) (Ш
 B Users B Lost & Found ✓ Settings Ø General Ø Email 		📮 Add 📃 🖛 Remove		N	1-1 of 1	Þ. H.
@ LDAP @ Policies @ Guest Personalization @ Federation @ Metadata		Name	IP Pool (Used/Total)	vSphere Network	Default Gateva	a.
		Use default gateway for E Use the above selected default forwarding.	INS Relay. gateway for DNS relay. Toget	her these parameters w	III be used for the gateways' default rou	öng and DNS

- **Step 6** After the external network is added to the list of networks in the lower portion of the screen, click Next.
- **Step 7** In the **Sub-Allocate IP Pools** screen, identify the range of IP addresses allocated for each externally-connected interface on the external network, and click **Next**.
- Step 8 In the Name and Description screen, enter the edge gateway name and description, and then click Next.
- Step 9 In the Summary screen, review the information for accuracy and click Finish.

Creating an Org VDC Internal Network

Use this procedure to create an internal network for the Org VDC.

Procedure

- Step 1 In the VCD GUI, choose System > Manage & Monitor > Cloud Resources > Organization VDCs.
 Step 2 In the Organization VDCs table, double-click the Org VDC where you want to create the internal network. The screen is refreshed with information about the selected VDC.
- Step 3 In the Org VDC Networks tab, in the toolbar, choose Actions > Add Network.

VMware vCloud Di	rector administrator (System Administrator) Preferences Help +	Logout
System vcd.org ×	atalogs 4% Administration	
Administration	1 test-Org-VDC	
	vApps vApp Templates Media & Other Storage Policies Edge Gateways Org VDC Networks Resource Pools	
✓ ▲ Virtual Datacenters Recent items	AJ Y	CO
Rest-Org-VDC	Name Add Network by Address Type Connected To IP Pool (Used/Total) Shared Owner	
Users		

The New Organization Network wizard opens, guiding you through the configuration process.

Step 4 In the **Select Network Type** screen:

- a) Choose Create a routed network by connecting to an existing edge gateway.
- b) Choose the vShield Edge Gateway that you created in Adding a vShield Edge Gateway on an Org VDC, on page 6.

VMware vCloud	New Organization VDC N	letwork					3		
System vcd.org X	Select Network Type	Select Network Typ Create a network for	e r use by vApps in this vi	rtual datacenter.					
Administration Cloud Resources Cources	Name and Description Ready to Complete	You can create a routed network that provides controlled access to machines and networks outside of the VDC via an edge gateway, or an isolated network that only machines in this VDC can connect to. You can also create a network that connects directly to an external network. O Create an isolated network within this virtual datacenter.							
Recent tens		 Create a routed r 	tetwork by connecting t	o an existing edge ga	iteway:				
✓ Members				Al	-		G		
🔓 Users		Name	1 # External Netwo	# Organization V	Avai	able Networks			
🖁 Lost & Found		Stage-gw1	-21	9.0	9				
✓ Settings									
General									
@ Email									
@ Policies						1-1 of 1 📃 🕨	N		
Guest Personalization		Connect directly	to an external network:						
Federation				AI	*		CO		
@Metadata		Name 1 A	IP Pool (Used/Tota		vSphere Network	VCenter			
		-te vCD-exter	53.15%	2 v7	2-pp	Ø vCD-vCenter-	5.5		
11/10/10									
🐐 0 Running 🔮 0 Fail					Back	ext Finish	Cancel		

Step 5 In the **Configure Network** screen:

- a) Enter the following information:
 - · Gateway IP address
 - Network mask
 - DNS server IP address

- b) In the Static IP pool area, enter an IP address or an IP address range and click Add.
- **Step 6** In the **Name and Description** screen, enter a name and description (optional) for the Org VDC internal network.
- **Step 7** In the **Ready to Complete** screen, review the information for accuracy and click **Finish**.

Creating a Catalog

A catalog enables you to upload images from Cisco ICFP to VCD.

For additional information about creating catalogs and selecting options, see your VMware vCloud Director documentation.

Procedure

- **Step 1** In the VCD GUI, choose **System > Manage & Monitor > Cloud Resources > Organization VDCs**.
- **Step 2** In the **Organization VDCs** table, double-click the Org VDC in which to add the catalog. The screen is refreshed with information about the selected VDC.
- Step 3 Choose the Catalogs tab and, in the toolbar, choose Actions > Add Catalog. A dialog box opens with multiple tabs so that you can configure the catalog and user access.
- **Step 4** In the **General** tab, enter a name and a description (optional) for the catalog.
- **Step 5** In the **Sharing** tab:
 - a) Click Add Members.
 - b) Choose the users or groups of users who can access the catalog.
 - c) In the Access Level field, choose the level of access for each user or group of users: Read-only, Read/Write, or Full Control.
- **Step 6** In the **Storage** tab, choose the type of storage.
- **Step 7** In the **Metadata** tab:
 - a) From the **Type** drop-down list, choose the metadata type.
 - b) In the Name field, enter a name for this metadata entry.
 - c) In the User access of metadata field, choose the level of access for the metadata: Read/Write, Read-only, or Hidden.
 - d) In the Value field, enter a text value for the metadata entry.
- **Step 8** After you have configured the catalog, click **OK**.

Verifying NAT and Firewall Service Configuration

When VCD is integrated with Cisco ICFP, NAT and firewall services are configured automatically, enabling the vShield Edge Gateway to communicate with the external network. This procedure enables you to confirm that NAT and firewall services have been configured on the vShield Edge Gateway as expected.

Procedure

- Step 1 In the VCD GUI, choose System > Manage & Monitor > Cloud Resources > Organization VDCs.
- **Step 2** In the **Organization VDCs** table, double-click the Org VDC where you created the vShield Edge Gateway (Adding a vShield Edge Gateway on an Org VDC, on page 6).

The screen is refreshed with information about the selected VDC.

- Step 3 In the Edge Gateways tab, right-click the required edge gateway and choose Edge Gateway Services.
- **Step 4** In the **Configure Services** dialog box, confirm the following:
 - a) In the **NAT** tab, confirm that Source NAT and Destination NAT rules are displayed, as shown in the following example:

VMware vClou	Configure Services	: Edge-gw1						0
System	DHCP NAT	Firewall St	tatic Routing VPN Load Bala	ancer				
🕼 Home 😡 Manage & M								
lanage & Monitor	Network Addres Source NAT (SI	ss Translation (NAT) translates	NAT) modifies the source/destin the source address of a packet t	ation IP address	es of packets arriving to and lea s gateway, whereas Destination	ving from this Edg NAT(DNAT) tran	ge Gateway. Islates the des	tination IP
Crganizations	address/port of	a packet receiv	red by this gateway.					
Cloud Resources	Applied On	Туре	Original IP	Original Port	Translated IP	Translated Port	Protocol	Enabled
Cloud Cells	vCD-external-	SNAT	192.168.233.2-192.168.233	any	10.2.96.200-10.2.96.210	any	ANY	~
Reprovider VDCs	vCD-external-	DNAT	10.2.96.200-10.2.96.210	anv	192 168 233 2-192 168 233	anv	ANY	~
Organization VDCs								
🗑 Edge Gateways								
-La External Networks								
Network Pools								
vSphere Resources								
@vCenters								
Resource Pools								
Hosts								
Datastores & Datast								
Storage Policies								
Switches & Port Grou								
Stranded Items								
Logs								
Blocking Tasks								
					Add SN/	Add DNA	T Edit.	Delete
🗿 0 Running 🕥 0 Fa							(OK Cance

- b) In the Firewall tab, confirm that inbound traffic is allowed for the following destination ports and protocols:
 - 22—TCP
 - 443—TCP
 - 500—TCP, UDP
 - 4500—TCP, UDP
 - 6644-TCP, UDP
 - 6646—TCP, UDP

The information should resemble the following example:

System	DHCP NAT	Firewall Static Routing	VPN Load Balanc	er				
🕼 Home 😡 Manage & M								
Manage & Monitor	Rules can be ad dropping them a	dded to the Firewall to allow o at the desired location in the I	r deny specific networ st. The order of any s	k traffic. The order of the elected rules is preserv	ese rules can be ed after dropping	changed by sele them into a diffe	ecting one or m erent location w	ore rules, dragging within the list.
Crganizations	Enable firewa	all						
Cloud Resources	Default action	Denv Allow Lo						
Cloud Cells	Applicable to traff	ic that does not match the rules in	the list					
Provider VDCs								
Organization VDCs	Rule Id	Name	Source	Destination	Protocol	Action	Log	Enabled
Edge Gateways	3	InBound ACL Rules	Any:Any	Any:22	TCP	Allow	1.5	~
	4	InBound ACL Rules	Any:Any	Any:6644	TCP	Allow	140	×
Network Pools	5	InBound ACL Rules	AnvAnv	Anv:6644	UDP	Allow		~
vSphere Resources	6	InBound ACL Rules	Anychny	ADV BBAB	TCP	Allow	-	~
VCenters	-	In Dound ACE Rules	Any Any	Any:0040	LIDD	Allens		
Resource Pools	1	InBound ACL Rules	Any:Any	Any:0040	ODP	Allow		
Detectores & Detect	8	InBound ACL Rules	Any:Any	Any:443	TCP	Allow	-	*
El Storage Policies	9	InBound ACL Rules	Any:Any	Any:500	TCP	Allow	-	×
Switches & Port Grou	10	InBound ACL Rules	Any:Any	Any:500	UDP	Allow	-	~
D Stranded Items	11	InBound ACL Rules	Any:Any	Any:4500	TCP	Allow	-	×
Logs	12	InBound ACL Rules	Any:Any	Any:4500	UDP	Allow	1. . .	×
(Par.)								

Configuring Cisco ICFP for Cisco Intercloud Fabric

After you have installed Cisco ICFP on a VMware server and launched a Cisco ICFP instance, you can configure Cisco ICFP for use with Cisco Intercloud Fabric.

Before You Begin

Confirm the following:

- Cisco ICFP has been installed on a VMware server and an instance has been launched.
- You know the Cisco ICFP public IP address.

Procedure

Sten 2	In the New	Cloud Instance	dialog box	provide the	following	information	and click	Create [.]
	In the root	Ciouu instance	unulog box,	provide the	10110 willig	mitormation,	and ener	Cicate.

Field	Description
Cloud Instance Name	Name of the cloud instance.
Туре	The cloud instance type: Cisco or Custom.

Field	Description
Module Name	For a Cisco cloud instance type, choose the module name, such as VCDP for VMware vCloud Director Platform. For a custom cloud instance, enter the custom module name.
Endpoint URI	The endpoint hostname or IP address of the cloud instance.

Step 3	In the Cisco ICFP GU	Л, choose	Tenant Accounts	, and click the Add	Tenant Account icon
--------	----------------------	-----------	-----------------	---------------------	---------------------

Step 4 In the New Tenant Account dialog box, provide the following information, and click Create:

Field	Description			
Tenant Name	Enter the tenant name.			
	You cannot change the name after adding the tenant.			
Select Cloud	Choose the name of the cloud instance that you created in the previous steps.			
	You cannot change the cloud instance name after adding the tenant.			
Org Name	For VMware vCloud Director clouds, enter the name of the organization to which the tenant belongs.			
Max Servers	Enter the maximum number of servers provisioned for the tenant, including stopped VMs.			
Username	Enter the tenant account username.			
Email	Enter the tenant account email address.			