

vCloud Director Extender 1.0 User's Guide

vCloud Director Extender 1.0

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<https://docs.vmware.com/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1	About the vCloud Director Extender User's Guide	5
	Introduction to vCloud Director Extender	5
2	Installing and Configuring vCloud Director Extender on a Cloud Provider	7
	Compatibility Requirements	8
	Deploying vCloud Director Extender on vCloud Director	8
	Configuring L2 VPN Network Extension on Cloud Provider	11
3	Installing and Configuring vCloud Director Extender on vCenter Server	13
	Compatibility Requirements	13
	Deploying vCloud Director Extender on vCenter Server	14
4	Managing vCloud Director Extender	19
	About Workload Migration	19
	About Hybrid Cloud	21
	Connect to the vCloud Director Organizations	22
	Index	23

About the vCloud Director Extender User's Guide

1

This guide provides information about installing, configuring, and managing vCloud Director Extender.

Intended Audience

This book is intended experienced system administrators who are familiar with Linux, Windows, IP networks, VMware vSphere , and VMware vCloud Director.

Introduction to vCloud Director Extender

VMware vCloud Director Extender is a product that creates a hybrid cloud between an end-user data center and a multi-tenant cloud based on vCloud Director.

vCloud Director Extender is designed to provide enterprise customers with the possibility of connecting their on-premise data center to a multi-tenant cloud environment based on vCloud Director. It provides a secure platform that ensures a seamless migration of on-premise workloads and extension of virtual networks to the cloud.

The L2 extension feature makes it possible to extend on-premise networks to cloud and deploy parts of the application on the same cloud subnet. It provides virtual machine mobility in scenarios such as hybrid cloud and phase migration between cloud provider and tenant sites. With L2 VPN extension, you do not have to reconfigure the applications, for example change their IP addresses, during failover. You can install and configure vCloud Director Extender both on tenant vCenter Server and on vCloud Director for Service Provider deployment.

Installing and Configuring vCloud Director Extender on a Cloud Provider

2

vCloud Director Extender has multiple components that you must install and configure in a specific order. You use the vCloud Director Extender - Cloud Service Setup UI to complete the installation and configuration.

For a service provider environment, the installation order of the required components is as follows.

NOTE You install each of the components on a separate virtual machine created as part of the automated configuration run from the Cloud Service Setup UI. The installation includes a minimum of four virtual machines, including at least one replicator virtual machine per resource vCenter Server. Depending on the workload, you might add additional replicators for a resource vCenter Server.

Components	Description
NSX	NSX is the network virtualization component. For more information, see <i>NSX Installation Guide</i> .
Cloud Continuity Manager	This component is the operational manager of the Cloud Continuity Engine. Runs on the service provider side and takes care of configuring the replicators and staging the replication workflow.
Cloud Continuity Engine	This component is a replication and recovery engine used for the virtual machines migration. Runs both on-premise and on service provider side and takes care of the data transfer and monitoring.
CX Cloud Service	This is the vCloud Director Extender component that is installed and deployed on the cloud provider side . You use it to run the Cloud Service Setup UI for the configuration.

This chapter includes the following topics:

- [“Compatibility Requirements,”](#) on page 8
- [“Deploying vCloud Director Extender on vCloud Director,”](#) on page 8
- [“Configuring L2 VPN Network Extension on Cloud Provider,”](#) on page 11

Compatibility Requirements

Before you install vCloud Director Extender, verify that your environment meets the required software version support and licensing. You can deploy vCloud Director Extender on vCenter Server or on vCloud Director.

Product Release and Licensing Requirements

Products	Requirements
vSphere	<ul style="list-style-type: none"> ■ For more information on product interoperability, see VMware Product Interoperability Matrices. ■ vSphere replication requires VMware vSphere Essentials Plus Kit and above. ■ To download the vCloud Director Extender OVA file you must have a valid vSphere license.
vCloud Director	<ul style="list-style-type: none"> ■ For more information on product interoperability, see VMware Product Interoperability Matrices.
NSX	<ul style="list-style-type: none"> ■ For more information on product interoperability, see VMware Product Interoperability Matrices.

Network and Access Requirements

Category	Requirements
Network	<ul style="list-style-type: none"> ■ vCloud Director environment with an existing L2 VLAN network. For more information, see <i>vCloud Director Installation and Upgrade Guide</i>. ■ The network bandwidth between on-premise and vCloud Director VDC must be 100 Mbps or higher. ■ You must assign static IP addresses to the virtual machines for the vCloud Director Extender components. vCloud Director Extender does not run any preliminary checks to verify the validity of the static IP configurations provided during the configuration. NOTE vCloud Director Extender does not support DHCP network configuration. ■ CX Cloud Service appliance must be configured with a DNS server IP. ■ Based on the source and destination networks, the number of edges can vary. Each X-Large edge requires 8GB RAM, 6 CPUs, and 500MB disk space.
Permissions	<ul style="list-style-type: none"> ■ A cloud administrator access to vCloud Director. ■ A vi-admin user account for the Resource vCenter Server and Management vCenter Server.

Deploying vCloud Director Extender on vCloud Director

To deploy vCloud Director Extender on vCloud Director you must install the CX Cloud Service appliance and run the vCloud Director Extender - Cloud Service Setup UI to complete the Setup wizard.

vCloud Director Extender Setup wizard installs all the required components for a seamless first-time configuration.

Install CX Cloud Service on vCloud Director for Service Provider

When installed the CX Cloud Service appliance starts automatically the vCloud Director Extender - Cloud Service Setup UI that helps you configure the underlying replication infrastructure on the cloud provider site.

Procedure

- 1 Download the vCloud Director Extender OVA file.
- 2 Log in to the vSphere Web Client as an administrator.

- 3 In the vSphere Web Client right click on your VDC or folder and select Deploy as .ovf or .ova.
- 4 Enter the path to the OVF or OVA file and click **Next**.
- 5 Select deployment type CX Cloud Service.

NOTE You must assign a static IP to the virtual machine.

- 6 Enter root password.
- 7 Click **Next** to deploy.

What to do next

Run Cloud Service Setup UI on vCloud Director for Service Provider.

Run Cloud Service Setup UI on vCloud Director for a Service Provider

You can install the required components either by running the Setup wizard or by manually selecting them from the vCloud Director Extender - Cloud Service Setup UI menu. For a first-time installation, use the Setup wizard.

Prerequisites

- After deploying the CX Cloud Service appliance, the Cloud Service Setup UI runs automatically.

Procedure

- 1 To access the Cloud Service Setup UI manually, navigate to `https://CX_Cloud_Service_IP/ui/mgmt/dashboard`. For `CX_Cloud_Service_IP`, enter the IP address of the vCloud Director Extender appliance.

NOTE If Cloud Service Setup UI runs automatically you can skip this step.

- 2 Log in with the root user credentials. For more information, see [“Install CX Cloud Service on vCloud Director for Service Provider,”](#) on page 8.
- 3 Click **Start Wizard**.

NOTE You must run the Setup wizard for your first-time configuration to install successfully the workload migration feature.

- 4 Follow the prompts of the wizard.

NOTE In the Cloud Service Setup UI, you can define an appliance configuration for a single data center or a cluster.

Setup	Description
Management vCenter Server	Provide the IP address of the Management vCenter Server. Enter the administrator credentials.
vCloud Director	Link the target cloud vCloud Director . This is the destination for the virtual machines that you migrate from the tenant to the VDC .
Resource vCenters	Register the resource vCenter Server instances. The Cloud Service Setup UI extracts the resource vCenter Server instances that are part of the vCloud Director environment provided in the previous step. NOTE You can specify an optional external Platform Services Controller configuration.

Setup	Description
Replication Manager	Register the Replication Manager by providing details from management vCenter Server: <ul style="list-style-type: none"> ■ Datacenter Name ■ Datastore Name ■ Cluster Name ■ Network Name
Activate Replication Manager	Set new password to activate.
Replicator	Register the Replicator by providing details for the management vCenter Server: <ul style="list-style-type: none"> ■ Test Folder/Datacenter Name NOTE You must provide the full multilevel schema path. ■ Datastore Name ■ Cluster Name ■ Network Name
Activate Replicator	<ol style="list-style-type: none"> 1 Set new <i>root</i> password. 2 Provide the details from the resource vCenter Server. NOTE You must enter the Lookup Service URL field, if you use an external Platform Services Controller. 3 Public Endpoint URL and Port. NOTE You must fill in this field if you use a proxy server. Provide the IP address and the port of the proxy service. For more information, see “Configuring Cloud Service Setup UI with a Proxy Server,” on page 10.

Configuring Cloud Service Setup UI with a Proxy Server

With vCloud Director Extender - Cloud Service Setup UI, you can access the replicator and the replicator manager through a proxy server or a firewall. One of the appliance requirements are to provide a proxy with a public endpoint and configure rules to route the network traffic to the replication components.

Cloud Provider Proxy Configuration

For cloud provider configuration both the replicator and replicator manager require proxy server settings. You must make sure that a bidirectional communication between the on-premise replicator and the cloud provider replicator manager is possible. The replicator manager listens on port 8044.

Table 2-1. Example

Category	IP Address
Cloud Provider Proxy	10.10.10.10
Replication Manager IP	192.168.10.10:8044
Replicator IP	192.168.20.20:44045
vCloud Director Extender IP	192.168.30.30:443

Rules

For example, you must configure the rules from.

- 10.10.10.10:443 to 192.168.30.30:443
- 10.10.10.10: 8044 to 192.168.10.10:8044
- 10.10.10.10: 44045 to 192.168.20.20:44045

Configuring L2 VPN Network Extension on Cloud Provider

vCloud Director Extender uses network paths that exist between the vCloud Director organizations.

Enable vCloud Director Organizations for L2 VPN Configuration Permissions

To enable L2 VPN network stretching, you must have L2 VPN configuration permissions assigned to your administrator account.

For more information, see *Edit Organization Rights* in *vCloud API Programming Guide for Service Providers* and *Predefined Roles and Their Rights* in *vCloud Director Administrator's Guide*.

Configure vCloud Director Organization Rights for L2 VPN stretching

You must have L2 VPN configuration rights assigned to the vCloud Director administrator for network stretching.

Procedure

- 1 Log in to the vCloud Director and use curl to create a user session:

```
curl -i -k -H "Accept:application/*+xml;version=1.5" -u 'root@System:password' -X POST
https://vCD_IP/api/sessions
```

- 2 Send a GET request to retrieve the organization ID.

```
GET https://{vcdServer}/api/query?type=organization
```

For example: `./../org/0712aa06-d241-4423-a6e7-80daeee8f71e`

- 3 Send a GET request to retrieve all vCloud Director instance rights.

```
GET https://{vcdServer}/api/admin?fields=RightReferences
```

- a From the displayed result, search for type *Organization vCD Gateway* and copy/save them into a text editor.

- 4 Send a GET request to retrieve the list of rights assigned to the organization.

```
GET https://{vcdServer}/api/admin/org/Organization_ID/rights
```

Use the *Organization_ID* retrieved in [Step 2](#).

- 5 Prepare an XML payload using the saved organization gateway rights retrieved in [Step 3](#).

This is an example of how the XML payload must look.

```
<OrgRights xmlns="http://www.vmware.com/vcloud/v1.5">

<RightReference href="https://10.139.112.187/api/admin/right/9dc33fcb-346d-30e1-8ffa-
cf25e05ba801" name="Organization vDC Gateway: Convert to Advanced Networking"
type="application/vnd.vmware.admin.right+xml"/>
<RightReference href="https://10.139.112.187/api/admin/right/105191de-9e29-3495-
a917-05fcb5ec1ad0" name="Organization vDC Gateway: View L2 VPN"
type="application/vnd.vmware.admin.right+xml"/>
<RightReference href="https://10.139.112.187/api/admin/right/eeb2b2a0-33a1-36d4-
a121-6547ad992d59" name="Organization vDC Gateway: Configure L2 VPN"
type="application/vnd.vmware.admin.right+xml"/>
  <RightReference
href="https://10.139.112.187/api/admin/right/b755b050-772e-3c9c-9197-111c286f563d"
name="Organization vDC Gateway: Configure Firewall" type="application/vnd.vmware.admin.right
+xml"/>
```

```

    <RightReference href="https://10.139.112.187/api/admin/right/b0cfe989-521b-3d7f-9bc2-
    f23c74a99633" name="Organization vDC Network: Edit Properties"
    type="application/vnd.vmware.admin.right+xml"/>
    <RightReference href="https://10.139.112.187/api/admin/right/2c8d98ef-4acc-3be4-9214-
    fcb9682b7a19" name="Organization vDC Network: View Properties"
    type="application/vnd.vmware.admin.right+xml"/>

</OrgRights>

```

- 6 Send a PUT request to add the new permissions.

PUT `https://{{vcdServer}}/api/admin/org/Organization_ID/rights`

Use the *Organization_ID* obtained in [Step 2](#).

What to do next

- After the new permissions are added you can proceed to enable advance gateway networking and VDC network subinterface in the vCloud Director Web console menu.

Assign vCloud Director Organization Rights for L2 VPN stretching.

An organization administrator must have the configuration permissions to perform an L2 VPN network stretch.

Procedure

- 1 Log in vCloud Director as an administrator.
- 2 Click **Manage System Administrator**.
- 3 Select the organization administrator to whom you want to assign extended permissions.
- 4 Click **Organization vDC Network > Edit Properties**.
- 5 Select the **Configure L2 VPN** check box to assign administration permissions to the VDC.
- 6 Click **OK** to save.

Configure L2 VPN tunnels to vCloud Director

With L2 VPN, you can configure a tunnel between vCloud Director and an on-premise vCenter Server. Because CX Connector installs a VPN client on on-premise side you must have NSX Edge installed and configured at the cloud provider side.

To create the L2 VPN tunnel, you configure an L2 VPN Server and L2 VPN Client.

- For more information, see *L2 VPN Overview* in *NSX Administration Guide*.
- For more information on L2 VPN configuration and troubleshooting, see *L2 VPN* in *NSX Troubleshooting Guide*.

Installing and Configuring vCloud Director Extender on vCenter Server

3

vCloud Director Extender has multiple components that you must install and configure in a specific order. You use the vCloud Director Extender - OnPrem Setup UI to complete the installation and configuration.

For tenant environments, the installation order of the required components is as follows.

NOTE You install each of the components on a separate virtual machine created as part of the automated configuration run from the OnPrem Setup UI.

Component	Description
(Optional) NSX Manager	NSX is the L2 VPN client used for the network stretching. For more information, see <i>NSX Installation Guide</i> . If NSX is not installed, vCloud Director Extender uses NSX for vSphere Standalone Edge - Client 6.3.0 included in vCloud Director Extender. NOTE You can configure the NSX Manager from the setup UI.
Cloud Continuity Engine	This component is a replication and recovery engine used for the virtual machines migration. Runs both on-premise and on cloud provider side and takes care of the data transfer and monitoring.
CX Connector	This is the vCloud Director Extender plug-in on the on-premise vCenter Server.

This chapter includes the following topics:

- “[Compatibility Requirements](#),” on page 13
- “[Deploying vCloud Director Extender on vCenter Server](#),” on page 14

Compatibility Requirements

Before you install vCloud Director Extender, verify that your environment meets the required software version support and licensing. You can deploy vCloud Director Extender on vCenter Server or on vCloud Director.

Product Release and Licensing Requirements

Products	Requirements
vSphere	<ul style="list-style-type: none">■ For more information on product interoperability, see VMware Product Interoperability Matrices.■ vSphere replication requires VMware vSphere Essentials Plus Kit and above.■ To download the vCloud Director Extender OVA file, you must have a valid vSphere license.

Network and Access Requirements

Category	Requirements
Network	<ul style="list-style-type: none"> ■ The network bandwidth between on-premise and vCloud Director vDC must be 100 Mbps or higher. ■ The virtual machines for the components must have static IP addresses assigned. vCloud Director Extender does not run any preliminary checks to verify the validity of the static IP configurations provided during the vCloud Director Extender configuration. NOTE vCloud Director Extender does not support DHCP network configuration.. ■ Based on the source and destination networks you select, the number of edge instances can vary. Each X-Large edge requires 8GB RAM, 6 CPUs, and 500MB disk space.
Permissions	<ul style="list-style-type: none"> ■ A user account that has organization administrator rights for the target vCloud Director. For more information about organizations, see <i>vCloud Director User's Guide</i>. ■ A vi-admin user account for the source vCenter Server.

Deploying vCloud Director Extender on vCenter Server

To deploy vCloud Director Extender on vCenter Server you must first install the vCloud Director Extender - OnPrem Setup UI and configure the required components.

Install CX Connector on a Tenant vCenter Server

The CX Connector appliance deploys the vCloud Director Extender - OnPrem Setup UI through which you prepare your on-premise environment.

Prerequisites

- Verify that your target vCloud Director has been enabled from the CX Cloud Service installed on the cloud provider site.
- Verify that you have the vCloud Director Extender OVA file.

Procedure

- 1 Log in to the vSphere Web Client as an administrator.
- 2 In the vSphere Web Client, right click on your VDC or folder and select Deploy as .ovf or .ova.
- 3 Enter the path to the OVF or OVA file and click **Next**.
- 4 Select CX Connector as the deployment type.

NOTE You must assign a static IP to the virtual machine.

- 5 Enter the password for the root user and click **Next**.
- 6 Copy the IP address of CX Connector.

You need that IP address to access the vCloud Director Extender - OnPrem Setup UI.

What to do next

Run OnPrem Setup UI on the Tenant vCenter Server.

Run OnPrem Setup UI on a Tenant vCenter Server

You can install the required components either by running the Setup wizard or by manually selecting them from the vCloud Director Extender - OnPrem Setup UI menu.

Prerequisites

- Verify that vCloud Director Extender OVA file is installed on vCenter Server.

Procedure

- 1 Navigate to `https://CX_Connector_IP/ui/mgmt/dashboard`.

For `CX_Connector_IP`, provide the IP address of the virtual machine where the appliance is installed.

- 2 For a first time configuration, log in with the `root` credentials that you created in [“Install CX Connector on a Tenant vCenter Server,”](#) on page 14.

NOTE After you register the Management vCenter Server with the CX Cloud Service on the service provider site, you can log in with user name `admin` and password `admin`.

- 3 Click **Start Wizard** to run the setup wizard.

NOTE You must run the Setup wizard for your first-time configuration and if you want to install the workload migration feature. You can skip running the wizard and continue to [Step 5](#) if you want to configure only an L2 VPN network extension.

- 4 Follow the prompts of the wizard.

NOTE In the OnPrem Setup UI, you can define an appliance configuration only for a single data center or a cluster. You can extend the networks based only on the appliance configuration.

Setup	Description
On-prem vCenter Server	Enter the vCenter Server fully qualified domain name and IP address and the administrator credentials.
Register Plug-in with vCenter Server	Register with a valid version number. NOTE You must increment the version number for the subsequent configuration. Identify the correct installed plug-in version from the Managed Object Browser.
Replicator	Register the Replicator by providing the details of your vCenter Server: <ul style="list-style-type: none"> ■ Name ■ Folder/Datacenter Name NOTE You must provide the full multilevel schema path. ■ Hosts or Cluster Name ■ Datastore Name ■ Network Name ■ Static IP Configuration
Activate Replicator	<ol style="list-style-type: none"> 1 Set a new password for the root user. 2 Provide the details from the resource vCenter Server. NOTE You must enter the Lookup Service URL field, if you use an external Platform Services Controller 3 Public Endpoint URL and Port. NOTE You must fill in this field if you are using an environment with a proxy server. Provide the IP address and the port of the proxy server. For more information, see “Configuring OnPrem Setup UI with Proxy Server,” on page 16.
Complete	Click Next to complete the setup wizard.

- 5 Click the **DC Extensions** tab in the vCloud Director Extender - OnPrem Setup UI menu to configure and add an L2 appliance and a NSX Manager.

NOTE You must complete both steps, L2 Appliance Configuration and NSX Manager Configuration if NSX Manager is installed on the on-premise vCenter Server instance. If you do not have NSX Manager installed on the on-premise vCenter Server then only L2 Appliance Configuration is required.

Setup	Description
L2 Appliance Configuration	<p>Configure an L2 appliance by providing the following details:</p> <ul style="list-style-type: none"> ■ Folder Name/Datacenter Name NOTE You must provide the full multilevel schema path. ■ Cluster Name ■ Datastore Name ■ Uplink Network Name ■ Uplink Network Pool IP ■ Uplink Default Gateway IP NOTE Make sure the provided information is correct, no preliminary checks are run to verify the validity of the data. ■ Uplink Prefix Length NOTE This is a mandatory field, you must provide this information for a successful configuration. <p>Click Create to add an L2 appliance.</p>
NSX Manager Configuration	<p>Configure an NSX Manager by providing the following details:</p> <ul style="list-style-type: none"> ■ Name ■ HostURL ■ Username ■ Password

What to do next

Run vCloud Director Extender.

Configuring OnPrem Setup UI with Proxy Server

With vCloud Director Extender - OnPrem Setup UI you can access the replicator service through a proxy server or a gateway. One of the appliance requirements are to provide a proxy with a public endpoint and configure rules to route the network traffic to the replication components.

On-premise Proxy Configuration

For on-premise configuration, only the replicator requires proxy server settings. You must configure the proxy rules before adding a new cloud provider. During the replicator registration, the messages go through the proxy to the replicator, therefore you must make sure that a bidirectional communication between the on-premise replicator and the cloud provider replicator manager is possible. The replicator listens on port 8083 for management data and on port 44045 for replicator data.

Table 3-1. Example

Category	IP Address
On-premise Proxy	20.20.20.20
Replicator	172.168.10.10:8043

Rules

For example, you must configure the rules from.

- 20.20.20.20:443 to 172.168.10.10:8043.

Run vCloud Director Extender

After you complete the installation and configuration of all required components, you can run vCloud Director Extender. To start a migration or create an L2 VPN extension, you must run vCloud Director Extender from the Home menu of the vSphere Web Client.

Procedure

- 1 Log in to the vSphere Web Client as administrator.
- 2 Navigate to Home page.
- 3 Click the vCloud Director Extender icon.

Managing vCloud Director Extender

You can start network stretching and virtual machines migration only from tenant on-premise vCenter Server. With vCloud Director Extender tenants can preserve their current IP and MAC address scheme after the migration is complete.

This chapter includes the following topics:

- [“About Workload Migration,”](#) on page 19
- [“About Hybrid Cloud,”](#) on page 21
- [“Connect to the vCloud Director Organizations,”](#) on page 22

About Workload Migration

With vCloud Director Extender, you can migrate your workload from an on-premise vCenter Server instance to the cloud provider environment. You can migrate virtual machines both when they are powered on or powered off depending on the available downtime.

Migration of an entire data center is often done in stages and might take a long period of time. To ensure a minimal downtime of clients applications vCloud Director Extender provides flexibility in the different types of migrations.

You can chose from two types of migration.

- With warm migration you can keep your virtual machines active while the migration runs and ensure minimal downtime. After the migration completes, you start a manual cutover to make the virtual machines available on the cloud provider site and finalize the migration. The cutover is a process that powers on the virtual machines after the warm migration completes.
- With cold migration you power down your virtual machines and start the migration. No cutover process is required in this case, you can choose whether to power on the virtual machines from the migration setup menu.

Manage Workload Migration

You can start a migration of the virtual machines workload from vCenter Server to vCloud Director right away or by scheduling it for a later time.

Prerequisites

Identify the groups of virtual machines to be migrated.

NOTE Based of the amount of virtual machines to be migrated, the service provider defines the resource profile and size of the VDC .

Procedure

- 1 Log in to the vSphere Web Client as an **administrator**.
- 2 Navigate to the **Home** tab.
- 3 Click the vCloud Director Extender plug-in.

NOTE vCloud Director Extender is supported with vSphere Client (HTML5).

- 4 Click **New Migration**.
- 5 Specify the type of migration.

Option	Description
Warm	The virtual machines remain active during the migration and parts of the workload continue running while others are migrated. NOTE After the warm migration completes, the status of the migration job changes to Cutover ready . A Cutover is required for the migrated virtual machine to be available on the cloud after the migration. You can still make changes to the virtual machine until you click Start Cutover .
Cold	The virtual machines will be inactive during the migration.

NOTE You can migrate up to 10 workloads at a time.

- 6 Select the data center, from which you want to migrate virtual machines.
- 7 From the drop down menu, select the virtual machines you want to migrate and click **Next**.
- 8 Select a target cloud destination for the virtual machines by providing the requested information.

Category	Description
Select Target Cloud	Provide the registered target vCloud Director.
Select vDC	Provide the registered vDC.
Select storage profile	Provide a storage profile name.
Select network	Provide a network name.
vApp layout	Select a layout option. <ul style="list-style-type: none"> ■ Each VM stays individually. ■ Group all VMs into a single vApp.

- 9 Schedule the time and date for the migration.
 - a For warm migration, specify the target recovery point objective time.
 - b For cold migration, specify if you want the virtual machine to be powered on after the migration.
- 10 Click **Start** to run the migration.

You can monitor the migration status in the **Workloads** tab of the **Migrations** screen.

NOTE You must perform a manual **Cutover** after the warm migration job completes to power on the virtual machine.

About Hybrid Cloud

With Hybrid Cloud, you can stretch an L2 VPN network from the on-premise VDC to a network on the cloud provider side.

vCloud Director Extender uses NSX Edge to extend the networks, the type of the L2 VPN Edge deployed on premise depends on whether NSX is installed or not. The number of edges deployed can vary based on the source and destination networks selected for extension.

About Network Monitoring

You can monitor the status of all stretched networks throughout the vCloud Director Extender user interface.

vCloud Director Extender shows a list of all the stretched Layer 2 VPN networks with their status. This information can be seen in the **DC Extensions** tab after vCloud Director Extender is started.

Options	Description
Name	Extension name.
Source Network	Source network name.
Target Network	Target network name.
Target vDC	Target data center.
Provider Cloud	Provider cloud data center.
Connected	The stretched network is available.
Disconnected	The stretched network is unavailable.
Updated On	Update history.

NOTE Alternatively, you can monitor the network status with NSX Edge user interface. For more information, see *View L2 VPN Statistics* in the *NSX Administration Guide*.

Manage Data Center Extensions

With Network Stretching, you can have a high-availability solution. Old and traditional applications cannot perform disaster recovery resolutions on the application layer without having to make changes, network virtualization gives that edge so that is no longer the case.

Prerequisites

- Verify that the edge has advance gateway networking and VDC network subinterface enabled on vCloud Director.

Procedure

- 1 Log in to the vSphere Web Client as an **administrator**.
- 2 Click the vCloud Director Extender plug-in.
- 3 Click **New Extension** and fill in the requested information for source and destination.

NOTE A single on-premise VDC edge is connected to a single cloud provider VDC edge, if you extend a new network from the same on-premise VDC edge to another network on a different cloud-provider VDC-edge, a new edge and a trunk port group are created, the trunk port group being attached to the new edge.

4 Click **Start**.

Automatic checks are run to verify if L2 VPN gateways exist.

NOTE If no L2 VPN gateway is installed, hybrid cloud installs high availability enabled L2 VPN gateways in the on-premise organization environment.

After the checks complete, a confirmation message states that the network is stretched.

Connect to the vCloud Director Organizations

After you install the vCloud Director Extender, you can click on vCloud Director Extender icon and connect to different vCloud Director organizations.

Procedure

- 1 Log in vSphere Web Client as an **administrator**.
- 2 In the Home page select vCloud Director Extender.
- 3 Select **New Provider Cloud**.
- 4 Provide the required details to connect to the target vCloud Director organization.
- 5 Click **Test** to verify the connection status and accept the trust certificates.
- 6 Click **Add** to connect to the vCloud Director organization.

You have successfully connected to a vCloud Director organization.

Index

A

Administration, Managing 19

C

Compatibility 8, 13

configuration 8

configuration, Tenant 15

configure 11

D

deploy 14

deployment 9

Deployment 17

I

installation 8, 13

Installation 7

installation, configuration UI 14

introduction 5

L

L2 VPN organization rights 11

M

migration 19

migration, to migrate 19

N

network stretching 21

network stretching, Hybrid Cloud 21

Network, Connection 21

Network, Connection, Stretching 21

R

requirements 8, 13

S

Service Provider 7, 8, 11

T

Technical Support 5, 8, 9, 11, 14, 15, 17, 19, 21,
22

Tenant 13

to execute 17

to start 17

to monitor 21

to obtain 5

V

vCD Org, organizations, connect 22

