



Community Experience Distilled

VMware vCloud Director Essentials

Build VMware vCloud-based cloud datacenters from scratch

Lipika Pal

[PACKT] open source*
PUBLISHING community experience distilled

www.allitebooks.com

VMware vCloud Director Essentials

Build VMware vCloud-based cloud datacenters
from scratch

Lipika Pal

[PACKT] open source 
PUBLISHING community experience distilled

BIRMINGHAM - MUMBAI

VMware vCloud Director Essentials

Copyright © 2014 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: August 2014

Production reference: 1190814

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78398-652-1

www.packtpub.com

Cover Image by Duraid Fatouhi (duraidfatouhi@yahoo.com)

Credits

Author

Lipika Pal

Reviewers

Oleg Aravin

Andy Grant

Ryan Johnson

Daniel Langenhan

Mario Russo

Preetam Zare

Commissioning Editor

Andrew Duckworth

Acquisition Editor

Rebecca Pedley

Content Development Editor

Ruchita Bhansali

Technical Editors

Pankaj Kadam

Neha Mankare

Edwin Moses

Copy Editors

Alisha Aranha

Mradula Hegde

Gladson Monteiro

Project Coordinators

Kranti Berde

Aaron S.Lazar

Proofreaders

Simran Bhogal

Ameesha Green

Indexer

Rekha Nair

Graphics

Ronak Dhruv

Disha Haria

Abhinash Sahu

Production Coordinator

Saiprasad Kadam

Cover Work

Saiprasad Kadam

About the Author

Lipika Pal is a Technical Lead in Colt Technology Services for Cloud and Virtualization, where she provides users with technical guidance to design, implement, and manage VMware vCloud Datacenter IaaS services, rendering enterprise-class access to on-demand or long-term virtualized resources across UK and Europe.

She has more than 7 years of expertise in professional services, designing and deploying virtualization solutions, and rolling out new technology and solution initiatives. Her primary focus is on the VMware vSphere infrastructure and public cloud using VMware vCloud Suite.

One of her other ambitions is to own the entire life cycle of a VMware-based IaaS, especially, vSphere, vCloud Director, vShield Manager, and vCenter Operations. She holds certifications from VMware, Citrix, Red Hat, Cisco, and Zerto. Prior to joining Colt, she was a subject matter expert and an infrastructure architect at fine organizations such as IBM, HP, and Red Hat.

I would like to thank and dedicate this book to my parents. Without their endless and untiring support, this book would not have been possible.

About the Reviewers

Oleg Aravin is a passionate engineer with an interest in distributed systems, highly available web services, and virtualization technologies. He received a Master's degree in Computer Science from Saratov State University, Russia. He also worked as a teacher and researcher at the university, studying the application of artificial neural networks for scientific research and has several publications on artificial neural networks. His skills have been enhanced by working for Grid Dynamics, where he worked with large retail customers such as eBay and Kohl's, designing and implementing distributed e-commerce platform solutions. He is presently a senior software engineer at VMware and lives and works in Palo Alto, California.

Ryan Johnson is a staff technical account manager for VMware as part of professional services. He has over 18 years of enterprise experience, ranging from engineering, research and development, enterprise technology, business architecture, service management to professional services.

Prior to joining VMware, he was the Enterprise Technology Architect for Citizens Property Insurance Corporation of Florida, where he led the Enterprise Architecture program and was responsible for the aspects of technology, applications, and information architecture.

He holds numerous industry certifications from VMware, Microsoft, EMC, Red Hat, and others. He has also been a technical reviewer for various Packt Publishing books, including *VMware Horizon Workspace Essentials*, *Peter von Oven*, *Peter Björk*, and *Joel Lindberg* as well as *Getting Started with VMware Fusion*, *Michael Roy*.

For a mix of hypertext fragments, pixels, and all things underanalyzed, follow him on Twitter at @tenthirtyam, or LinkedIn, at [linkedin.com/in/tenthirtyam](https://www.linkedin.com/in/tenthirtyam).

Daniel Langenhan is a client-focused virtualization expert with more than 18 years of international industry experience.

His skills span the breadth of virtualization, ranging from architecture, design, and implementation of large multi-tier enterprise client systems to delivering captivating education and training sessions in security technologies and practices to diverse audiences.

Utilizing his extensive knowledge, experience, and skills, he has a proven track record of successfully integrating virtualizations into different business areas, while minimizing cost and maximizing the reliability and effectiveness of solutions for his clients.

He gained extensive experience with Australian, European, and international enterprise clients. His consulting company is well established with strong industry ties in many verticals, for example, finance, telecommunications, and print. His consulting business also provided services to VMware International.

He has authored books such as *Instant VMware vCloud Starter*, *VMware View Security Essentials*, and *VMware vCloud Director Cookbook*, all by Packt Publishing. He is currently writing a book on vCenter Orchestrator for Packt Publishing

www.PacktPub.com

Support files, eBooks, discount offers, and more

You might want to visit www.PacktPub.com for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.PacktPub.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at service@packtpub.com for more details.

At www.PacktPub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<http://PacktLib.PacktPub.com>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free access for Packt account holders

If you have an account with Packt at www.PacktPub.com, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface	1
Chapter 1: Configuring and Maintaining vCloud Director	5
Configuring centralized logging	6
Modifying the default Log4j configuration	7
Configuring syslog in the vCloud Director GUI	10
Configuring logging for vShield Manager	11
Configuring vCloud Director for scalability	13
Setting up the transfer storage space	15
Using vCNS for vCloud cell load balancing	16
Maintaining vCloud using command-line tools	20
Using vCloud Director shell commands	21
Understanding the vCloud support bundle	24
Configuring alarms and notifications	25
Managing vCenter Chargeback reports	28
Summary	29
Chapter 2: Managing vSphere Resources	31
vSphere compute resources	32
Registering the vCenter Server	32
Managing ESXi host resources in vCloud Director	36
Adding ESXi hosts to a provider virtual datacenter	36
Disabling and unpreparing ESXi hosts	38
Monitoring vSphere resources in vCloud Director	40
vSphere storage resources	42
Configuring storage profiles	43
Monitoring storage profiles in vCloud Director	47
Managing vSphere network resources	49
Adding the vSphere network port group	50
Understanding VXLANs	53

Preparing VXLAN for vCloud Director	57
Summary	61
Chapter 3: Managing vCloud Director Resources	63
Managing provider vDCs	64
Creating a provider vDC	65
Merging provider vDCs	68
Managing vCloud Director network resources	70
Network pools	71
VLAN-backed network pools	72
vCDNI-backed network pools	73
Port group-backed network pools	73
VXLAN-backed network pools	74
Creating VLAN-backed network pools	74
Provider external networks	76
Creating a provider external network	78
Managing a vCloud Director organization	81
Creating a vCloud Director organization	83
Managing organization vDCs	86
Organization vDC allocation model	88
Creating organization vDCs	89
Summary	93
Chapter 4: Managing Complex vCloud Director Networks	95
Configuring organization network services	95
Configuring DNS relay	97
DHCP services in vCloud Director	100
Configuring DHCP pools in vCloud Director	102
Understanding VPN tunnels in vCloud Director	104
Configuring a virtual private network	106
Understanding static routes in vCloud Director	108
Configuring static routes in an Org Gateway	110
Understanding the firewall service in vCloud Director	111
Configuring the vShield Edge device firewall	111
Understanding DNAT rules in vCloud Director	114
Configuring a destination NAT	115
Understanding SNAT rules in vCloud Director	117
Configuring a source NAT	118
Creating and managing vShield edge and vCloud networks	119
Configuring vShield Edge devices for compact/full configuration	121
vCloud Org networks	122
Configuring a Direct Connect organization network	123
Configuring a routed organization network	124
Configuring an isolated organization network	125
Summary	127

Chapter 5: Managing Catalogs and vApps	129
Creating and deploying vApps	130
Custom vApp properties	131
Creating a vCloud Director vApp	132
Understanding catalogs	148
Creating and configuring a catalog	149
Understanding vApp templates	154
Importing an OVF as a template	155
Summary	158
Chapter 6: Managing Security	159
Creating and processing certificate requests	159
Creating a self-signed certificate	160
Replacing certificates in vCloud Director	161
Configuring and managing vCloud Director access control	163
Configuring organization access	164
Creating roles to improve organization security	169
Configuring vCenter SSO as access management for vCloud Director	171
Summary	175
Index	177

Preface

Welcome to *VMware vCloud Director Essentials*. In this book, we will teach you how to implement a private cloud running VMware vCloud Director. This book equips you with the required knowledge, skills, and abilities to build a highly scalable and secured private cloud running VMware vCloud. We will also use screenshots throughout this book, which are usually not available in vCloud product manuals.

You will learn how to configure and manage vCloud Director. You will also learn how to use VXLAN, vSphere storage profiles, vSphere network port groups, and vCenter Chargeback Manager, which can help you to strengthen your cloud implementation.

We discuss some advanced concepts of cloud, such as DNS and DHCP relay, VPN, static routes, and firewall management, which are available worldwide. You will also learn how to manage vCloud organization and its security as well as maintain vApp and vApp templates.

What this book covers

Chapter 1, Configuring and Maintaining vCloud Director, covers the installation and configuration of vCloud Director for first-time use. It also shows you how to configure centralized logging, maintain vCloud using command lines, and manage chargeback reports.

Chapter 2, Managing vSphere Resources, walks you through the process of adding vSphere compute resources to vCloud Director. We also discuss the management of vSphere storage and networking resources.

Chapter 3, Managing vCloud Director Resources, explains the management of provider vDCs, vCloud director network resources, and organization vDCs.

Chapter 4, Managing Complex vCloud Director Networks, shows you how to configure organization and vApp networks as well as create and maintain vCloud networks.

Chapter 5, Managing Catalogs and vApps, elaborates on how you can share vApps and catalogs. Also, we go through the process of creating and deploying vApps. Finally, we show you how to manage vApp storage profiles.

Chapter 6, Managing Security, shows you how to create and replace SSL certificates for vCloud Director. We also go through the procedures to configure and manage vCD access control using a custom LDAP option and vSphere SSO.

What you need for this book

You need VMware vSphere 5.1, which includes VMware vSphere ESXi, vCenter Server, any SSH Client (PuTTY), and vSphere Client. Also, you require VMware vCloud Director and the vCloud Networking and Security (vCNS) product suite.

Who this book is for

If you are a technical professional with cloud administration skills and some amount of VMware vSphere experience, this is the book for you. It also helps you learn about advanced cloud products as well as where they fit and how to configure them. You will also learn to implement VMware vCloud run on private cloud.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "They are in `/opt/vmware/vcloud-director/bin`."

A block of code is set as follows:


```
log4j.appender.vcloud.system.syslog=
org.apache.log4j.net.SyslogAppender
log4j.appender.vcloud.system.syslog.syslogHost=
remoteSyslogHost.example.com
#Logs go to port 514 unless you specify a port,
as in the disable example below.
```


Any command-line input or output is written as follows:

```
vmware-vcd-support
```

```
vmware-vcd-multi-cell-log-collector
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Click on the **Administrator** tab."

 Warnings or important notes appear in a box like this.

 Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book – what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to feedback@packtpub.com, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on www.packtpub.com/authors.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books – maybe a mistake in the text or the code – we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting <http://www.packtpub.com/submit-errata>, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from <http://www.packtpub.com/support>.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at copyright@packtpub.com with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at questions@packtpub.com if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Configuring and Maintaining vCloud Director

A VMware vCloud combines a vCloud Director server group with the vSphere platform. When you install one or more vCloud Director software instances, they create a vCloud Director server group by connecting the servers to a shared database as well as the shared NFS storage directory and integrating the vCloud Director server group with a vSphere platform. **vCloud Director (vCD)** is web server appliance. So, when you install vCloud Director on one or more servers, you can form a vCloud Director server group and this group can be balanced behind a load balancer. Each vCloud Director is referred to as a cell. Multiple cells form a vCloud Director server group, which leverages a single database.

The installation and configuration procedure for VMware vCloud Director describes how to create the vCloud Director cells, connect them to the shared database, and establish the first connections to a vCenter Server, vShield Manager, and ESX/ESXi hosts. It is then the system administrator's job to use the vCloud Director web console to connect additional vCenter Servers, vShield Manager servers, and ESX/ESXi servers to a vCloud Director cell at any time

This chapter covers the following topics:

- How to configure centralized logging
- How to configure vCloud Director for scalability
- How to maintain vCloud using command-line tools

Configuring centralized logging

Centralized logging is the most important feature of vCD that allows us to see what happens within the cloud from one central place. The following are the various important logs and tasks you can view from one central location.

To understand how to configure a centralized logging system, we need to explain the role of the administrator and why you have to manually configure centralized logging.

vCloud Director provides the log in information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues.

As a vCloud System Administrator, you can do the following:

- View the system log to monitor system-level tasks that are in progress. System logs show you which tasks are currently running in vCloud Director or are already completed tasks in vCloud Director, which includes tasks that are in progress and failed tasks.
- Find the failed tasks that have been logged and troubleshoot them.
- Analyze vCloud Director logs to monitor vCloud Director cells.
- Similarly, as an organization admin, you can view the tasks at the organization level.

We are essentially discussing system-level tasks and organization-level tasks.

As the name suggests, these tasks are specific to the system- and organization-level tasks and events that get logged there. If you are running a small private cloud with just a single-cell cloud deployment, then there is not much scope or use in configuring centralized logging. However, for a large-scale cloud implementation, especially where a public cloud is running, you should have an external syslog server configured to send logs to a centralized location.

You can find the logs for a cell at `/opt/vmware/cloud-director/logs`.

Apart from the diagnostics logs in vCloud Director, you have audit logs as well, which you can see in the following table:

Log name	What the log shows
<code>cell.log</code>	This logfile is the console output from the vCloud Director cell
<code>vcloud-container-debug.log</code>	This logfile shows the debug-level log messages from the cell
<code>vcloud-container-info.log</code>	This container information log shows the warnings or errors encountered by the cell

Log name	What the log shows
vmware-vcd-watchdog.log	When the cell crashed, restarted, and so on, then this logfile shows us what possibly went wrong
diagnostics.log	This logfile shows diagnostics information; however, this log first needs to be enabled in the local logging configuration
YYYY_MM_DD.request.log	HTTP request from vCloud Director cells logs in the Apache common log format to this file

However, by default, these files do not get forwarded to the centralized logging server. You have to manually configure the vCloud cell to forward these to the centralized logging server. It is recommended that you configure this option for the following reasons:

- Remote logging allows audit logs from all cells to be viewed together in a central location at the same time.
- Database logs are not retained after 90 days, but logs transmitted via syslog can be retained as long as desired.
- The vCloud cell protects the audit logs from any loss on the local system due to failure, lack of disk space, compromise, and so on.
- It supports forensics operations in the face of problems, like those listed in the preceding points.
- Logging to a remote system, instead of the cell, provides data integrity by inhibiting tampering. Even if the cell is compromised, it does not necessarily enable access to, or alteration of, the audit log.

Modifying the default Log4j configuration

To implement centralized logging in vCloud Director, you need to modify the Log4j configuration that vCloud Director uses and add an additional appender to the loggers. However, as a prerequisite, you need to know the IP address or FQDN of the log server and the port this server is listening to (the default port: UDP 514). On another note, you also need to figure out the level of logging information you want to send to the logging server.

There are seven levels of logging available in vCloud director, which are as follows:

- **FATAL:** This level designates very severe error events that will presumably lead the application to abort
- **ERROR:** This level designates error events that might still allow the application to continue running

- **WARN:** This level designates potentially harmful situations
- **INFO:** This level designates informational messages that highlight the progress of the application at a coarse-grained level
- **DEBUG:** This level designates fine-grained informational events that are most useful to debug an application
- **TRACE:** This level is designed to log informational events at a level finer than DEBUG logging
- **OFF:** This level is intended to turn off logging

Let's look at how to enable centralized logging in vCloud Director by performing the following steps:

1. Before you start the activity, you should confirm that the remote logging server supports listening to remote connections.



Make sure that the appropriate firewall configuration is in place for vCloud Director—the outbound UDP access and inbound UDP access for the syslog host.

2. Log in to the cell using the console or SSH.
3. Change the directory to `/opt/vmware/vcloud-director/etc`.
4. Create a backup of the logging configuration:

```
# cp log4j.properties log4j.properties.default
```
5. Open the `log4j.properties` file in a text editor and add the following lines:

```
log4j.appender.vcloud.system.syslog=
org.apache.log4j.net.SyslogAppender
log4j.appender.vcloud.system.syslog.syslogHost=
remoteSyslogHost.example.com
#Logs go to port 514 unless you specify a port,
as in the disable example below.
#log4j.appender.vcloud.system.syslog.syslogHost=
remoteSyslogHost.example.com:5555
log4j.appender.vcloud.system.syslog.facility=
LOCAL1
log4j.appender.vcloud.system.syslog.layout=
com.vmware.vcloud.logging.CustomPatternLayout
log4j.appender.vcloud.system.syslog.layout.ConversionPattern
=%d{ISO8601} | %-8.8p | %-25.50t | %-30.50c{1} | %m | %x%n
log4j.appender.vcloud.system.syslog.threshold=DEBUG
```

- Modify line 2 of this file to append the name of the new syslog appender, as follows:

```
log4j.rootLogger=ERROR, vcloud.system.debug,
    vcloud.system.info, vcloud.system.syslog
```

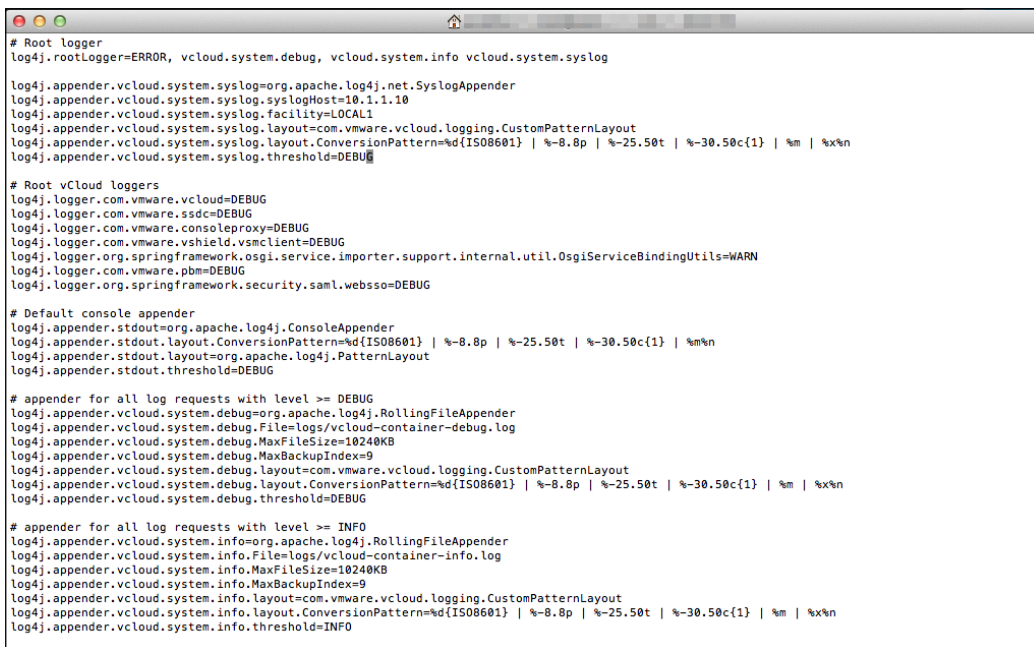
- Save the file.
- Restart the vCloud Director server service:

```
# service vmware-vcd restart
```

After the cell starts, the diagnostic log output from the cell appears on the central syslog server.

- Repeat this procedure for each cell in your vCloud Director server group.

The following screenshot illustrates a sample configuration of centralized logging for vCloud Director:



```
# Root logger
log4j.rootLogger=ERROR, vcloud.system.debug, vcloud.system.info vcloud.system.syslog

log4j.appender.vcloud.system.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.vcloud.system.syslog.syslogHost=10.1.1.10
log4j.appender.vcloud.system.syslog.facility=LOCAL1
log4j.appender.vcloud.system.syslog.layout=com.vmware.vcloud.logging.CustomPatternLayout
log4j.appender.vcloud.system.syslog.layout.ConversionPattern=%d{ISO8601} | %-8.8p | %-25.50t | %-30.50c(1) | %m | %x%n
log4j.appender.vcloud.system.syslog.threshold=DEBUG

# Root vCloud loggers
log4j.logger.com.vmware.vcloud=DEBUG
log4j.logger.com.vmware.ssdcc=DEBUG
log4j.logger.com.vmware.consoleproxy=DEBUG
log4j.logger.com.vmware.vshield.vsaclient=DEBUG
log4j.logger.org.springframework.osgi.service.importer.support.internal.util.OsgiServiceBindingUtils=WARN
log4j.logger.com.vmware.pbm=DEBUG
log4j.logger.org.springframework.security.saml.websso=DEBUG

# Default console appender
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout.ConversionPattern=%d{ISO8601} | %-8.8p | %-25.50t | %-30.50c(1) | %m%n
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.threshold=DEBUG

# appender for all log requests with level >= DEBUG
log4j.appender.vcloud.system.debug=org.apache.log4j.RollingFileAppender
log4j.appender.vcloud.system.debug.File=logs/vcloud-container-debug.log
log4j.appender.vcloud.system.debug.MaxFileSize=10240KB
log4j.appender.vcloud.system.debug.MaxBackupIndex=9
log4j.appender.vcloud.system.debug.layout=com.vmware.vcloud.logging.CustomPatternLayout
log4j.appender.vcloud.system.debug.layout.ConversionPattern=%d{ISO8601} | %-8.8p | %-25.50t | %-30.50c(1) | %m | %x%n
log4j.appender.vcloud.system.debug.threshold=DEBUG

# appender for all log requests with level >= INFO
log4j.appender.vcloud.system.info=org.apache.log4j.RollingFileAppender
log4j.appender.vcloud.system.info.File=logs/vcloud-container-info.log
log4j.appender.vcloud.system.info.MaxFileSize=10240KB
log4j.appender.vcloud.system.info.MaxBackupIndex=9
log4j.appender.vcloud.system.info.layout=com.vmware.vcloud.logging.CustomPatternLayout
log4j.appender.vcloud.system.info.layout.ConversionPattern=%d{ISO8601} | %-8.8p | %-25.50t | %-30.50c(1) | %m | %x%n
log4j.appender.vcloud.system.info.threshold=INFO
```

The preceding procedure will configure centralized logging for a vCloud cell; however, you need to configure the syslog servers for networks and other components. In the **Administration** tab, the **General** page allows you to type in up to two IP addresses for the syslog servers that the networks will use. This setting does not apply to syslog servers used by cloud cells.

There is a possibility to view the syslog server settings for a routed organization network. vCloud Director also supports logging events to a syslog server, where the events are related to firewall rules. If an administrator does not enable the logging permissions for an organization network, then they can synchronize the network with the most current syslog server settings.

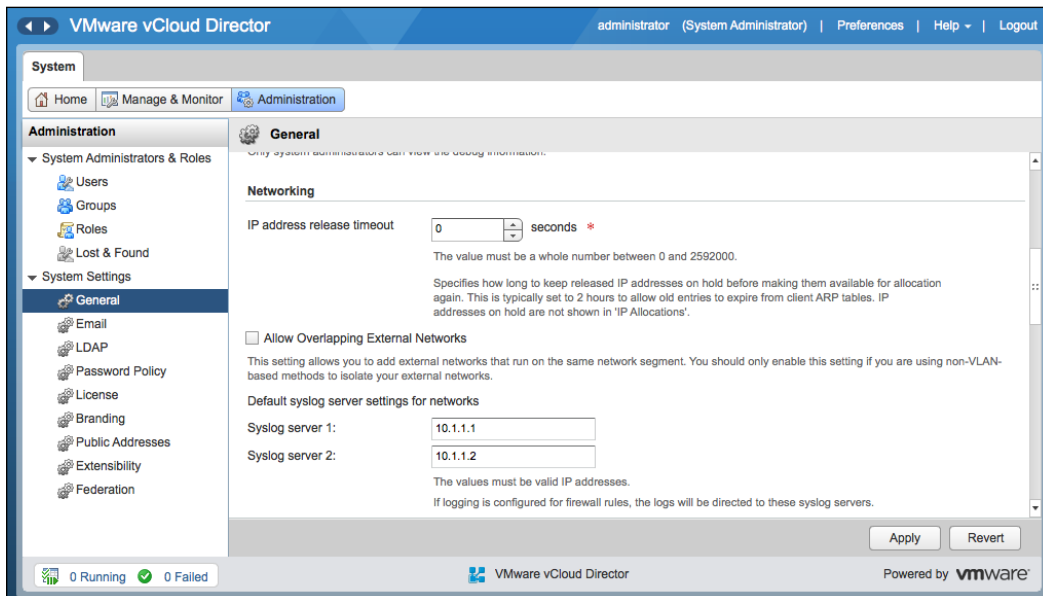
The syslog file is usually found in the `messages` file under `/var/log` in your syslog receiver.

Configuring syslog in the vCloud Director GUI

Let's look at how to configure the syslog settings in vCloud Director.

To configure a syslog server in vCloud Director, use the following steps:

1. Open a browser. Go to the URL of the vCD server; for example `https://serverFQDN/cloud`.
2. Log in to vCD by typing in an administrator user ID and password.
3. Click on the **Administrator** tab.
4. Click on **General** in the left panel.
5. Scroll down to the **Networking** section. Specify the syslog server IP address or FQDN for syslog server 1, as shown in following screenshot. Optionally, if you have another server, then specify the IP address or FQDN for that syslog server. Your screen should look similar to what is shown in the following screenshot:



6. Click on **Apply**.

Configuring logging for vShield Manager

vShield Manager can manage vShield Edge Gateway, which is a multi-interface vShield Edge virtual device that connects the vCloud Director organization vDC networks to external networks through the vCloud GUI. Each vShield Manager can be configured to send its logs to up to two remote syslog servers. Additionally, the protocol (UDP/TCP) can be specified as well, and these will be applied to every Edge device that's deployed (either Edge Gateways or vApp Edges).

When configured, audit logs and system events for vShield Manager are sent to the syslog servers via UDP using the default port (514) unless a different port is specified.

The system event message logged in syslog has the following structure:



```

syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter ':'
(double colons)
Each name/value pair separated by delimiter ';'
(double semi-colons)

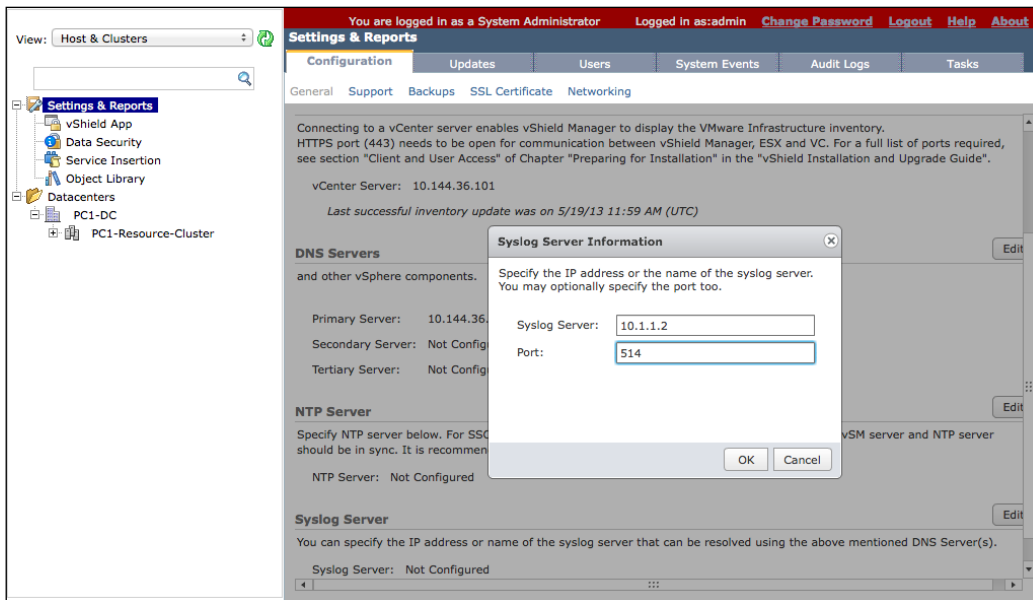
```

The fields and types of the system event contain the following information:

- Event ID :: 32 bit unsigned integer
- Timestamp :: 32 bit unsigned integer
- Application name :: string
- Application submodule :: string
- Application profile :: string
- Event code :: integer (possible values: 10007 10016 10043 20019)
- Severity :: string (possible values are INFORMATION LOW MEDIUM HIGH CRITICAL)
- Message: string

Let's look at how to configure logging for VMware vShield Manager. To configure a syslog server in vShield Manager, follow the ensuing steps:

1. Open a browser. Go to the URL of vShield Manager.
2. Log in with an enterprise-level account.
3. Click on **Settings & Reports** from the vShield Manager inventory panel.
4. Click on the **Configuration** tab.
5. Ensure that you are in the **General** tab.
6. Click on **Edit** next to **Syslog Server**.
7. Type in the IP address of the syslog server, as shown in the following screenshot:



8. Type in the port number for the syslog server (this is an optional step).
9. If you do not specify a port, the default UDP port for the IP address/host name of the syslog server is used.
10. Click on **OK**.

Configuring vCloud Director for scalability

After you have installed vCloud Director, the very next step is to do the initial configuration. Once you are done with the installation of the vCloud Director software, you will be asked to configure the software as well. However, we tend to skip this step as we normally do not have the SSL certificates ready by this time. So, as a prerequisite, you need to create self-signed SSL certificates. In a cloud environment, where trust concerns are minimal, self-signed certificates can provide an easy way to configure SSL for vCloud Director.

Each vCloud Director cell requires two SSL certificates, one for each of its IP addresses, in a Java keyStore file. We need two IP addresses in a vCloud director cell: one is for the web UI and the other is for the console proxy that requires the user to open up the VM console within the vCloud Director web UI. An administrator must create two SSL certificates for each server that they intend to use in their vCloud Director server group.

To finish off the configuration, we need to run the following script:

```
# /opt/vmware/vcloud-director/bin/configure
```

With this script, you need to provide the following information:

- The HTTP service IP address
- The remote console Proxy IP address
- The Java KeyStore path
- The Java KeyStore password
- The Syslog server hostname of the IP address
- The database host
- The database port
- The database name
- The database instance
- The database username
- The database password

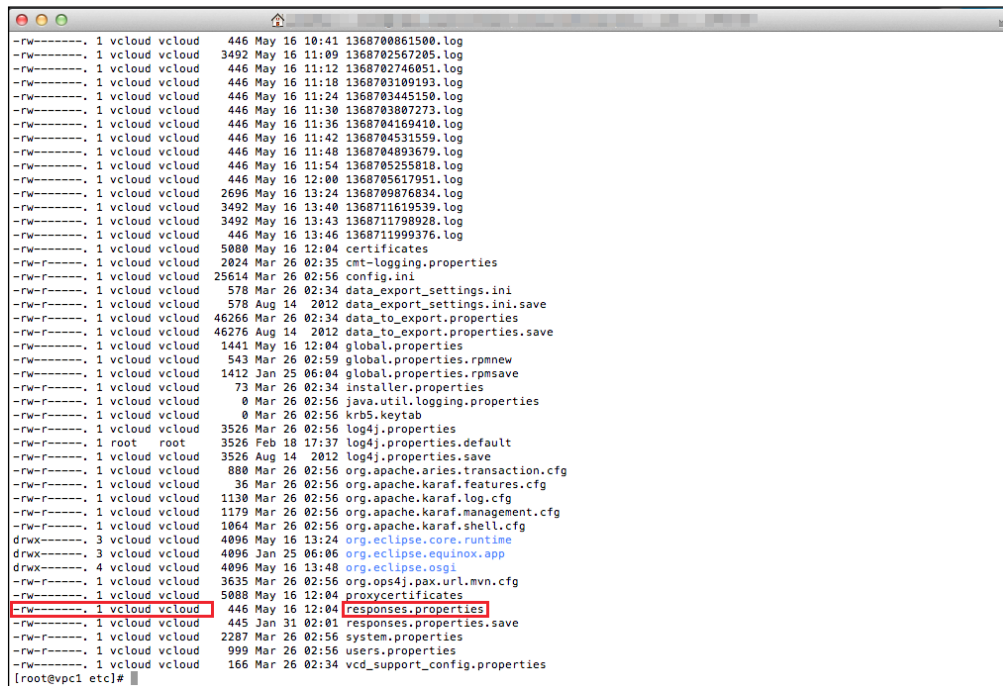


The database connection information and other reusable responses you provided during configuration are preserved in a `responses.properties` file located at `/opt/vmware/vcloud-director/etc/` on the vCloud server. This file will store the reusable information, that you can reuse when you add more servers to a server group.

Let's look at how to generate the vCloud Director response file. You need a response file when you configure another vCloud Director cell in the same group. It is created automatically once you configure the first vCloud Director cell. The steps to configure the cell have been discussed in the preceding steps.

Once you configure the first vCD cell and start the service, you will get the `responses.properties` file located at `/opt/vmware/vcloud-director/etc`.

This file must be owned by `vcloud.vcloud` and have read and write permissions for the owner vCloud and the group vCloud, as shown in the following screenshot:



```
--r----- 1 vcloud vcloud 446 May 16 10:41 1368700861500.log
--r----- 1 vcloud vcloud 3492 May 16 11:09 1368702567205.log
--r----- 1 vcloud vcloud 446 May 16 11:12 1368702746051.log
--r----- 1 vcloud vcloud 446 May 16 11:18 1368703109193.log
--r----- 1 vcloud vcloud 446 May 16 11:24 1368703445150.log
--r----- 1 vcloud vcloud 446 May 16 11:30 1368703807273.log
--r----- 1 vcloud vcloud 446 May 16 11:36 1368704169418.log
--r----- 1 vcloud vcloud 446 May 16 11:42 1368704531559.log
--r----- 1 vcloud vcloud 446 May 16 11:48 1368704893679.log
--r----- 1 vcloud vcloud 446 May 16 11:54 1368705255818.log
--r----- 1 vcloud vcloud 446 May 16 12:00 1368705617951.log
--r----- 1 vcloud vcloud 2696 May 16 13:24 1368709876834.log
--r----- 1 vcloud vcloud 3492 May 16 13:40 1368711619539.log
--r----- 1 vcloud vcloud 3492 May 16 13:43 1368711798928.log
--r----- 1 vcloud vcloud 446 May 16 13:46 1368711999376.log
5000 May 16 12:04 certificates
--r----- 1 vcloud vcloud 2024 Mar 26 02:35 cmt-logging.properties
--r----- 1 vcloud vcloud 25614 Mar 26 02:56 config.ini
--r----- 1 vcloud vcloud 578 Mar 26 02:34 data_export_settings.ini
--r----- 1 vcloud vcloud 578 Aug 14 2012 data_export_settings.ini.save
--r----- 1 vcloud vcloud 46266 Mar 26 02:34 data_to_export.properties
--r----- 1 vcloud vcloud 46276 Aug 14 2012 data_to_export.properties.save
--r----- 1 vcloud vcloud 1441 May 16 12:04 global.properties
--r----- 1 vcloud vcloud 543 Mar 26 02:59 global.properties.rpmnew
--r----- 1 vcloud vcloud 1412 Jan 25 06:04 global.properties.rpmsave
--r----- 1 vcloud vcloud 73 Mar 26 02:34 installer.properties
--r----- 1 vcloud vcloud 0 Mar 26 02:56 java.util.logging.properties
--r----- 1 vcloud vcloud 0 Mar 26 02:56 krb5.keytab
--r----- 1 vcloud vcloud 3526 Mar 26 02:56 log4j.properties
--r----- 1 root root 3526 Feb 18 17:37 log4j.properties.default
--r----- 1 vcloud vcloud 3526 Aug 14 2012 log4j.properties.save
--r----- 1 vcloud vcloud 880 Mar 26 02:56 org.apache.aries.transaction.cfg
--r----- 1 vcloud vcloud 36 Mar 26 02:56 org.apache.karaf.features.cfg
--r----- 1 vcloud vcloud 1130 Mar 26 02:56 org.apache.karaf.log.cfg
--r----- 1 vcloud vcloud 1179 Mar 26 02:56 org.apache.karaf.management.cfg
--r----- 1 vcloud vcloud 1064 Mar 26 02:56 org.apache.karaf.shell.cfg
drwx----- 3 vcloud vcloud 4096 May 16 13:24 org.eclipse.core.runtime
drwx----- 3 vcloud vcloud 4096 Jan 25 06:06 org.eclipse.equinox.app
drwx----- 4 vcloud vcloud 4096 May 16 13:48 org.eclipse.osgi
--r----- 1 vcloud vcloud 3635 Mar 26 02:56 org.ops4j.pax.url.mvn.cfg
--r----- 1 vcloud vcloud 5088 May 16 12:04 proxycertificates
--r----- 1 vcloud vcloud 446 May 16 12:04 responses.properties
--r----- 1 vcloud vcloud 445 Jan 31 02:01 responses.properties.save
--r----- 1 vcloud vcloud 2287 Mar 26 02:56 system.properties
--r----- 1 vcloud vcloud 999 Mar 26 02:56 users.properties
--r----- 1 vcloud vcloud 166 Mar 26 02:34 vcd_support_config.properties
[root@vpc1 etc]#
```

The following screenshot shows the typical content in this file:

```
[root@vpc1 etc]# cat responses.properties
user.keystore.path = \opt\vmware\vcloud-director\stareng-correct.ks
user.keystore.password = UyuNDh01L7M4WqP6rP34gxyKcN4E9xad4CbWkQEgQEJ5Qx7LyFgFiWR9FGsyXivo
database.jdbcUrl = jdbc:jtds:sqlserver://\10. :1433\vcloud1;socketTimeout=90
database.username = vcloud
database.password = yTmghESfJhGgXIqaCJ9o5DkX2YfLFI\YRLM1tbDZsHc=
system.info = X5BpcRBwnn7k1sRX7CHsug==
system.version = 2
audit.syslog.host =
audit.syslog.port = 514
[root@vpc1 etc]#
```

You can use this response file to add an additional vCloud Director server to the existing vCloud Director server's group. As a prerequisite, you need to use the same database details, and there you can leverage this response file from the first server. Also, you need a shared NFS directory.

When you use multiple cells in your vCloud environment, you need to have a shared spooling area that will be accessed by all your cells. It is called the **NFS Transfer Server Storage**. Transfer Server Storage is used for uploading and downloading vApps when you import VMs into your vCD from the vCenter Server. If you have larger vApps or ISO images, whose size is 100 GBs or greater, then the default Transfer Server Storage will not be sufficient. If your Transfer Server Storage capacity is small, it will result in the inability to upload or download vApps.



In order to provide temporary storage for uploads and downloads, an NFS or other shared storage volume must be accessible to all servers in the vCloud Director cluster. You should have the write permissions for the root to this volume (`No_Root_Squash`). All of your hosts should mount this volume at `$VCLLOUD_HOME/data/transfer`, which is typically `/opt/vmware/vcloud-director/data/transfer`.

Let's look at how to add additional vCloud Director cells using the response file. To add additional cells using the `responses.properties` file, perform the following steps:

1. Log in to the server where you want to install the vCloud Director software.
2. Retrieve the response file from the first server and put it in the target server's `/tmp` directory.
3. Run the following command:

```
./installation-file -r /tmp/responses.properties
```

Setting up the transfer storage space

Let's see how to set up the vCloud Director transfer storage space.

As a prerequisite, you need to have the NFS export details. Let's execute the given steps to set up the transfer storage space:

1. You need to add a line in `/etc/fstab` to make sure that the NFS server export is persistent in the vCloud cell. The following statement is an example line:

```
<NFS-Server-IP>: /<Export-Directory>  
/opt/vmware/vcloud-director/data/transfer nfs rw,  
soft,_netdev 0 0
```

2. Now, you can mount the NFS. Run the following command:

```
# mount -a
```
3. You need to set the permissions for your transfer directory. Run the following command that will provide the RWX permission to the owner and the read permission to everyone else:

```
chmod 750 /opt/vmware/vcloud-director/data/transfer
```
4. You need to change the User and Group ownership of your transfer folder as well. Run the following command:

```
chown -R vcloud:vcloud /opt/vmware/vcloud-director/data/transfer
```
5. Finally, you need to restart the vCD service by using the following command:

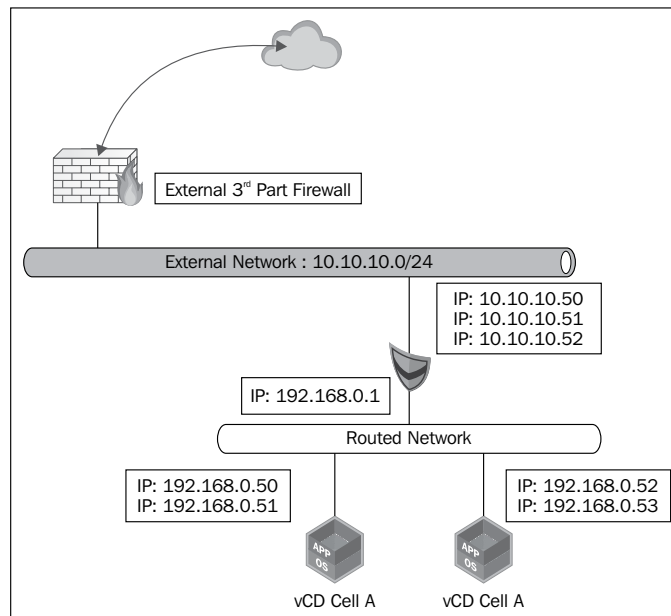
```
service vmware-vcd restart
```

When you deploy vCloud Director in a multi-cell environment, you tend to use it for high availability and load balancing. In these scenarios, you need a load balancer for your vCloud environment. For this matter, you can choose a hardware-based load balancer (for example, F5) or a software-based load balancer (for example, VMware vCloud Networking and Security (vCNS), Citrix Netscaler, and so forth).

The new version of vShield, which is vCNS, comes up with a lot of new features. Some of them are load balancing HTTPS and generic TCP connections. It also inherits the old mechanism of load balancing HTTP connections.

Using vCNS for vCloud cell load balancing

We will see how to use the Edge device to configure load balancing for a vCloud environment. Each Edge virtual appliance can have a total of ten uplink and internal network interfaces. In the following setup, we have two vCD cells inside a routed network, and we will use the vCNS to load balance the web portal and VMRC console proxy connections too.

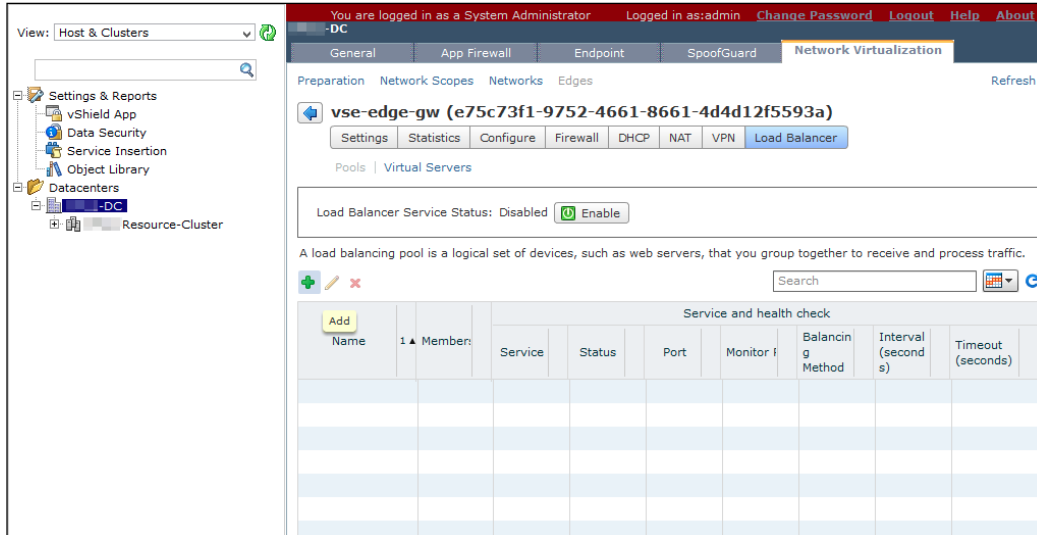


We will use an external IP address from Edge Gateway to load balance the vCD cell. The first vCD cell uses 192.168.0.50 as the web portal IP and .51 as the VMRC console proxy IP address. The second vCD cell uses 192.168.0.52 as the web portal IP and .53 as the console proxy IP address.

Let's look at how to configure load balancing of vCloud Director using vCNS. You need to go through the following steps to set up load balancing using Edge:

1. Create a pool of servers.
2. Create a virtual server.
3. Enable the Edge load balancer service.
4. Log in to the vCNS web portal.
5. Go to the **Host and Clusters** view, select **Datacenter**, and click on the **Network Virtualization** tab.
6. Click on the **Edges** link.
7. Select the appropriate Edge device and click on **Actions** and select **Manage**.
8. Go to the **Load Balancer** tab.
9. At this point, you need to add a pool of servers. We will add two pools: one for the vCD web portal and one for the VMRC console proxy.

- Click on the green colored + icon. Your screen should look similar to what is shown in the following screenshot:



- Name this pool and click on **Next**. I have named it vCD-Web-80-443.
- Select **HTTP** and **HTTPS** and set the **Balancing Method** option to **ROUND_ROBIN**.

There are four load balancing methods available in vCNS, as shown in the following table:

The load balancing method	Description
IP_Hash	This policy selects a server based on a hash of the source IP address of each packet.
LEAST_CONN	This policy makes sure that any new connections are sent to the server that has the fewest connections.
ROUND_ROBIN	In this policy, each server is used in turns according to the weight it was assigned while it was configured.
URI	The left part of the URI is hashed and divided by the total weight of the servers being run. The result determines which server will receive the request. However, this is only applicable for HTTP service load balancing.

- Select the default **Health Check** settings and click on **Next**.
- On the **Members** screen, add the vCD HTTP service members. In this case, it is 192.168.0.50. Set the Weight to **1** and click on **Add**.

15. Repeat step 11 and add the second vCD HTTP address, which in this case is 192.168.0.52. Click on **Next** once you are done.
16. Now select the green + icon one more time to add the VMRC.
17. Give it a name; in this example, I have named it VMRC-443.
18. On the **Services** screen, select **TCP** and **Balancing Method** as **ROUND_ROBIN**. Choose **443** as the port and click on **Next**.
19. Select the default settings for **Health Check**.
20. On the **Members** screen, add the members of VMRC. In this example, it is 192.168.0.51 and 192.168.0.53.
21. Click on **Next**.
22. On this final screen, review the configuration and select **Finish**.
23. Click on **Publish Changes** to make this effective.
24. Now go to the **Virtual Servers** tab where you need to create the load balancer virtual IP (VIP) for these two services (HTTP and VMRC). Click on the green + icon.
25. On the **Add Virtual Server**, name the first service, which is HTTP. In this example, I named it "vCloud-HTTP".
26. Specify the load-balanced IP Address (10.10.10.51) and choose the existing pool (vCD-Web-80-443). Your screen should look similar to what is shown in the following screenshot:

Name	Members	Service	Status	Port	Monitor IP	Balancing Method	Interval (seconds)	Timeout (seconds)
VMRC-443	2	TCP		443	8080	ROUND_RO	5	15
vCD-Web-80-443	2	HTTP HTTPS		80 443	80 443	ROUND_RO ROUND_RO	5 5	15 15

27. Click on **Add**.

28. Click on the green + icon one more time to add the Virtual Server IP for VMRC.
29. Give it a name. In this example, I named it "vCloud-VMRC".
30. Specify the load balanced IP address (10.10.10.52) and choose the existing pool VMRC-443.
31. Click on **Publish Changes** to make it persistent.
32. Now go to the pools screen and click on the **Enable** button to enable the Load balancer service.

Maintaining vCloud using command-line tools

Today, most of the activities that you perform in your vCloud Director cell are done through the command line. A cell management tool has been created to help you manage your vCloud Director. If you want to manage a cell and its SSL certificates or export tables from the vCloud Director database, then this is essential. You need to be the super user on a vCD cell VM to carry out these operations.

Managing a vCloud Director cell includes the following:

- Quiesce
- Shutdown
- Maintenance
- Status

With the vCloud Director 5.1 cell tool, you can generate self-signed certificates, replace the SSL certificates, and change a forgotten system administrator password. Before vCloud 5.1, you had to use several other tools to do this.

When you plan to upgrade your vCloud Director cell, you should use the cell management tool to gracefully shutdown the vCloud Director cell. However, shutdown is not recommended if you have an active cell and did not quiesce the cell first.

Quiesce means that vCloud Director creates a task object to track and manage each asynchronous operation that a user requests. Information about all the running tasks and the recently completed tasks is stored in the vCloud Director database. Due to a database upgrade invalidating this task information, you must make sure that no tasks are running when you begin the upgrade process.

The cell management tool can also be used to suspend the task scheduler so that new tasks cannot be started and then used to check the status of all active tasks. Either you need to wait for the active tasks to be completed, or you can proactively log in to the vCloud Director and cancel the ongoing tasks. If you do not have any tasks running on the cell, you can stop the services.

Using vCloud Director shell commands

There are a lot of shell commands that are helpful in maintaining and configuring vCloud Director. This section will explore them.

Sometimes you have to perform maintenance activities on the vCloud Director cell. During this time, you can turn on the maintenance message to let the users know that the cell is in maintenance and cannot be contacted. If you turned on the maintenance message, then the users who try to log in to the cell from a browser will see a message that states the cell is down for maintenance. Also, the users who try to reach the cell using the VMware vCloud API will receive a similar message.

Follow the ensuing steps to show the cell maintenance message to a cloud user during a planned maintenance:

1. Log in to the vCloud Director cell using root credentials.
2. Go to the directory by using the following command:

```
# cd /opt/vmware/vcloud-director/bin
```
3. Run the following command to put this cell in the maintenance mode:

```
# ./vmware-vcd-cell maintenance
```
4. When you need to come out of the maintenance mode, run the following command:

```
# ./vmware-vcd-cell stop
```



The cell needs to be started after you run the preceding command using `service vmware-vcd start`.

Let's look at how to quiesce and shutdown vCloud Director using the cell management tool.

The cell management tool can be used to quiesce and shut down a vCloud cell. To do this, follow the ensuing steps:

1. Log in to the vCloud cell using the root credentials.
2. First try to see if there are any active tasks being performed by this cell by using the following commands:

```
# cd /opt/vmware/vcloud-director/bin
# ./cell-management-tool -u administrator -p <password> cell -t
Job count = 5
Is Active = true
```

3. Any job count that is more than 0 means there are active tasks on this cell. You need to quiescent the cell now to stop the task scheduler:

```
# ./cell-management-tool -u administrator -p <password> cell -q true
```
4. After this point, check the cell status again using step 2, and if the `Job count` parameter becomes 0 and `Is Active` becomes false, then it is safe to shut down the cell by executing the following command:

```
# ./cell-management-tool -u administrator -p <password> cell -s
```

Let's look at generating self-signed SSL certificates using the cell management tool. The `generate-certs` command can be used if you need to generate new self-signed SSL certificates for the cell. Let's execute the following steps to create and retrieve self-signed SSL certificates:

1. You can run the following command to create the self-signed SSL certificates:

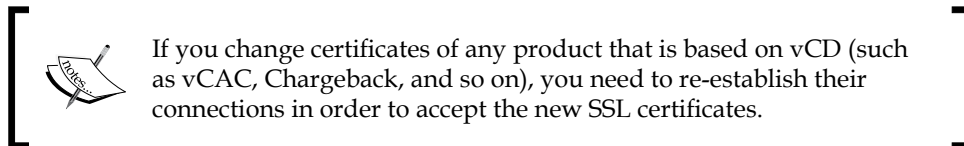
```
# ./cell-management-tool generate-certs -o /tmp/cert.ks -w vmware -i "CN=vCD, L=Bangalore, C=IN" -s 2048 -x 90
```

This example creates the new certificates using the custom values for the key size, issuer name, and a keyStore at `/tmp` that have the password `vmware`. This certificate uses 2048-bit encryption and expires 90 days after creation.

2. If you want to retrieve the recently created self-signed SSL certificates, then use the following command:

```
# keytool -storetype JCEKS -storepass vmware -keystore /tmp/cert.ks -list -v
```

Let's look at replacing self-signed SSL certificate using the cell management tool. The `certificates` command can be used if you want to replace a cell's existing certificate.



This command reads the existing certificate location from the `responses.properties` file under `/opt/vmware/vcloud-director/etc/`. Let's execute the following steps to replace the cell's certificates:

1. Run the following command to replace the cell's existing certificates with the just created new self-signed SSL certificate:

```
# ./cell-management-tool certificates -s /tmp/cert.ks -w vmware
```

2. You need to restart the cell services to make this certificate effective by using the following command:

```
# vmware-vcd restart
```

Let's look at recovering the system administrator password. You can use the `recover-password` command to recover the system administrator password, provided that you know the vCloud Director database username and password.

Use the following command to recover the system administrator password:

```
# ./cell-management-tool recover-password -dbuser vcloud -dbpassword VMware123
```

```
Please enter the system administrator username whose password is to be changed: administrator
```

```
Please enter the new password:
```

```
Reenter the password:
```

```
Successfully changed password
```

For troubleshooting and maintenance purposes, sometimes you stop/start the vCloud Director server service. This is what you have to do from the command line of your vCloud cell.

Let's look at how to manage vCloud services using command-line tools.

To start, stop, restart, and list vCloud process, follow the given steps:

1. Log in to the cell as the administrator.
2. To stop the service, run the following command:

```
# ./cell-management-tool -u username -p password cell -s
```

However, I will not recommend this method. You should use `vmware-vcd-cell stop` first.

3. To check the status of the VMware vCloud Director service, run the following command:

```
# service vmware-vcd status
```

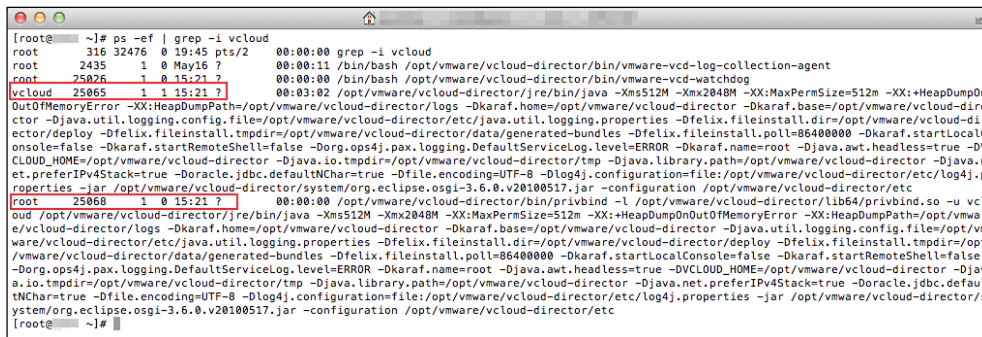
4. To start the VMware vCloud Director service, run the following command:

```
# service vmware-vcd start
Starting vmware-vcd-watchdog: [ OK ]
Starting vmware-vcd-cell [ OK ]
```

- You may wish to check whether the vCloud process is running. Use the following command to check this:

```
# ps -ef | grep -i vcloud
```

Ensure that the command prompt outputs the process as running, as shown in the following screenshot:



```
[root@ ~]# ps -ef | grep -i vcloud
root      316 32476  0 19:45 pts/2    00:00:00 grep -i vcloud
root      2435   1  0 May16 ?        00:00:11 /bin/bash /opt/vmware/vcloud-director/bin/vmware-vcd-log-collection-agent
root      25826   1  0 15:21 ?        00:00:00 /bin/bash /opt/vmware/vcloud-director/bin/vmware-vcd-watchdog
vcloud    25865   1  1 15:21 ?        00:03:02 /opt/vmware/vcloud-director/jre/bin/java -Xms512M -Xmx2048M -XX:MaxPermSize=512m -XX:HeapDumpOn
OutOfMemoryError -XX:HeapDumpPath=/opt/vmware/vcloud-director/logs -Dkaraf.home=/opt/vmware/vcloud-director -Dkaraf.base=/opt/vmware/vcloud-dire
ctor -Djava.util.logging.config.file=/opt/vmware/vcloud-director/etc/java.util.logging.properties -Dfelix.fileinstall.dir=/opt/vmware/vcloud-dire
ctor/deploy -Dfelix.fileinstall.tmpdir=/opt/vmware/vcloud-director/data/generated-bundles -Dfelix.fileinstall.poll=86400000 -Dkaraf.startLocalC
onsole=false -Dkaraf.startRemoteShell=false -Dorg.ops4j.pax.logging.DefaultServiceLog.level=ERROR -Dkaraf.name=root -Djava.awt.headless=true -DV
CLOUD_HOME=/opt/vmware/vcloud-director -Djava.io.tmpdir=/opt/vmware/vcloud-director/tmp -Djava.library.path=/opt/vmware/vcloud-director -Djava.n
et.preferIPv4Stack=true -Doracle.jdbc.defaultNChar=true -Dfile.encoding=UTF-8 -Dlog4j.configuration=file:/opt/vmware/vcloud-director/etc/log4j.p
roperties -jar /opt/vmware/vcloud-director/system/org.eclipse.osgi-3.6.0.v20100517.jar -configuration /opt/vmware/vcloud-director/etc
root      25868   1  0 15:21 ?        00:00:00 /opt/vmware/vcloud-director/bin/privbind -l /opt/vmware/vcloud-director/lib64/privbind.so -u vcl
oud /opt/vmware/vcloud-director/jre/bin/java -Xms512M -Xmx2048M -XX:MaxPermSize=512m -XX:HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/vmwar
e/vcloud-director/logs -Dkaraf.home=/opt/vmware/vcloud-director -Dkaraf.base=/opt/vmware/vcloud-director -Djava.util.logging.config.file=/opt/vm
ware/vcloud-director/etc/java.util.logging.properties -Dfelix.fileinstall.dir=/opt/vmware/vcloud-director/deploy -Dfelix.fileinstall.tmpdir=/opt
/vmware/vcloud-director/data/generated-bundles -Dfelix.fileinstall.poll=86400000 -Dkaraf.startLocalConsole=false -Dkaraf.startRemoteShell=false
-Dorg.ops4j.pax.logging.DefaultServiceLog.level=ERROR -Dkaraf.name=root -Djava.awt.headless=true -DVCLLOUD_HOME=/opt/vmware/vcloud-director -Djav
a.io.tmpdir=/opt/vmware/vcloud-director/tmp -Djava.library.path=/opt/vmware/vcloud-director -Djava.net.preferIPv4Stack=true -Doracle.jdbc.default
NChar=true -Dfile.encoding=UTF-8 -Dlog4j.configuration=file:/opt/vmware/vcloud-director/etc/log4j.properties -jar /opt/vmware/vcloud-director/s
ystem/org.eclipse.osgi-3.6.0.v20100517.jar -configuration /opt/vmware/vcloud-director/etc
```

- You can switch the service on or off manually in case you don't want an automatic start of the cell when the OS boots. To check the run level information for VMware vCloud Director, run the following command:

```
# chkconfig --list | grep -i vmware-vcd
```

Understanding the vCloud support bundle

Logfiles are more important in cases where you are troubleshooting any issues of vCloud Director. VMware has two scripts to capture all of the logfiles in the vCloud Director cell. They are in `/opt/vmware/vcloud-director/bin`. Let's use the following commands to use the logs:

```
vmware-vcd-support
vmware-vcd-multi-cell-log-collector
```

Once you execute this, all of the logfiles from `/opt/vmware/vcloud-director/logs` will be zipped into a `.tgz` file and will be saved under the user's home directory. This is a new behavior in vCD 5.5 since vCD 5.1 save the log from where one user runs the scripts.

The first script is pretty straightforward, and you need to run this from each cell to generate the log bundle. However, when you have a bigger environment where multiple cells are connected, then you may wish to run the second support script from any of the servers. This multi-cell log collection process is automated, faster, and less complicated. However, you can run the first script also with the `-m` option to call the second script.

When you invoke the multi-cell log collector script in one cell, either using the dedicated command or using the `-m` option with the standard script, a marker file will be created in the `transfer` directory under `$VCLLOUD_HOME/data` to signal a log collection. At the same time, `vmware-vcd-watchdog` will check whether the marker file exists or not; if yes, then it will execute the log collection script. The resulting support bundle (named `vmware-vcd-support-XXXX.tgz`) should be copied into `$VCLLOUD_HOME/data/transfer/`. The filename should contain the UUID cell and/or hostname so that the bundle file for each cell is unique. If this copy fails, the bundle should be left in its normal directory (under `logs`).

Let's look at how to collect logs for troubleshooting using the support script. To capture single vCloud cell deployment logs and a multi-cell deployment logs, follow the given steps:

1. Log in to the vCloud Director cell using root credentials.
2. Run the following command to capture the logs:

```
# ./opt/vmware/vcloud-director/bin/vmware-vcd-support
```

The preceding command will capture the log from just one cell.

3. Run either of the following commands to capture a multi-cell log:

```
# ./opt/vmware/vcloud-director/vmware-vcd-multi-cell-log-collector
```

Configuring alarms and notifications

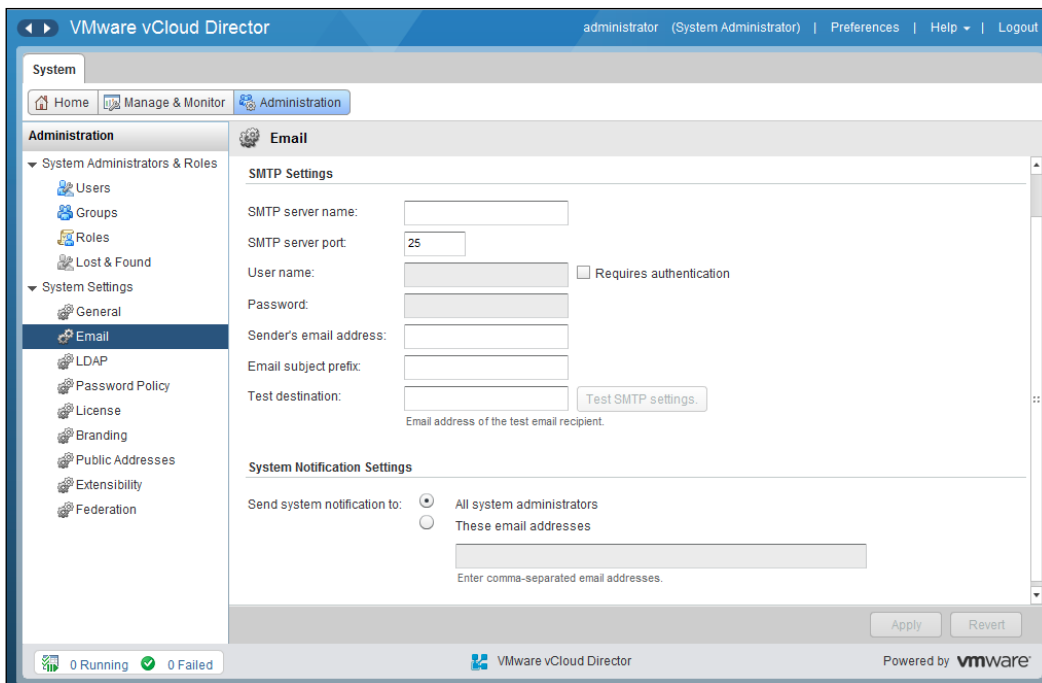
vCloud Director sends user notifications and system alert e-mails through the SMTP server. You can modify the settings you specified while you created the organization. Today, you have the feasibility to send these notifications to all users in the entire installation, all system administrators, or all organization administrators; for example, if you are planning for a planned maintenance, you can notify the users about it.

If configured, when your datastore free space is too low (out of space condition), vCloud Director sends system alert e-mails. You can configure vCloud Director to send e-mail alerts to all system administrators or to a specified list of e-mail addresses.

As an organization administrator, you can change the settings for both the SMTP and e-mail notifications, or you can keep it as system administrator-defined settings. An organization administrator may also wish to override SMTP settings if an SMTP server is available for organizational use.

Let's look at configuring SMTP alert settings in vCloud Director. To configure SMTP alert settings in vCloud Director, follow the given steps:

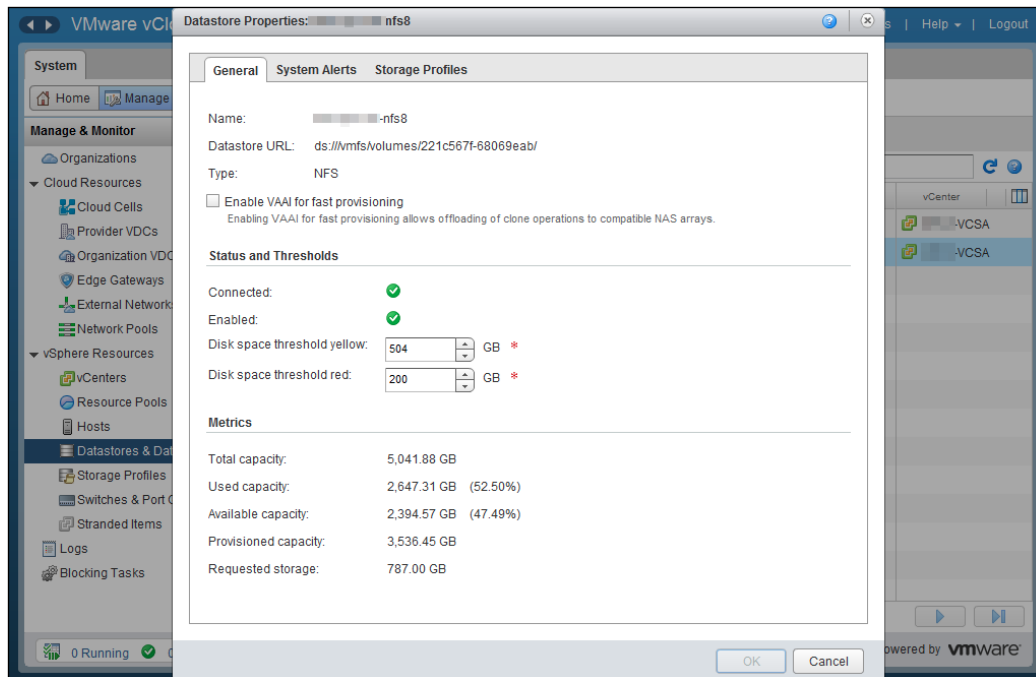
1. Log in to the vCD web portal as a system administrator.
2. Click on the **Administration** tab and click on **Email** in the left pane.
3. Type in the DNS host name or the IP address of the SMTP mail server.
4. Type in the SMTP server port number.
5. If the SMTP server requires a username, select the **Requires authentication** checkbox and type in the username and password for the SMTP account (this step is optional).
6. Type in an e-mail address as the sender for vCloud Director e-mails. vCloud Director uses the sender's e-mail address to send runtime and storage lease expiration alerts.
7. Type in the text to use as the subject prefix for vCloud Director e-mails.
8. Type in a destination e-mail address to test the SMTP settings and click on **Test SMTP settings**.
9. Click on **Apply**. Your screen should look similar to what is shown in the following screenshot:



Let's look at configuring warning alert settings in vCloud Director.

You can also configure the warning alerts in vCloud Director; for example, if your datastore is out of space, you can set the warning alert threshold. To do this, follow the given steps:

1. Log in to the vCloud web portal as a system administrator.
2. Click on the **Manage & Monitor** tab, and click on **Datastores & Datastore Clusters** in the left pane.
3. Right-click on the datastore name and select **Properties**.
4. On the **General** tab, select the disk space threshold values for the datastore.
5. You can set two thresholds: yellow and red. When vCloud Director sends an e-mail alert, the message indicates which threshold was crossed. By default, the yellow threshold is set at 90 percent and red is set at 95 percent. However, if you increase the datastore size via the backbone, the setting needs to be adjusted.
6. Click on **OK**. Your screen should look similar to what is shown in the following screenshot:



vCloud Director sends an e-mail alert to all VDCs where this datastore is attached when the datastore crosses a threshold.

Managing vCenter Chargeback reports

You can generate cost reports using VMware vCenter Chargeback Manager. This will include the cost and utilization information for each computing resource for the hierarchy or entity on which the report is generated. This information is based on the cost configured in the hierarchy and the pricing model selected during report generation.

Let's look at how to generate and archive basic reports. You can use vCenter Chargeback Manager to generate reports for a chargeback hierarchy and also for the entities within that hierarchy.

Also, if you look at the **Archived Reports** page of the **Reports** tab, it shows you a table that lists all the reports that are archived in the Chargeback Manager. This archived report includes manually generated and saved reports as well as reports that are generated by report schedules. Let's generate and manage archived basic reports by executing the following steps:

1. Log in to the Chargeback Manager.
2. In the **Reports** tab, click on **Create Reports**.
3. Select the required chargeback hierarchy from the drop-down menu on the left pane of the page.
4. Right-click on the hierarchy or the entity on which you want to generate the report and select **Generate Cost Report** from the pop-up menu.
5. Provide the requested report details and click on **Next**.
6. On the **Report Summary** page, select **Include resource summary** in report.
You must also select the type of resource summary to be reported.
The resource summary can either be complete (default) or basic.
7. Select the computing resources whose usage and cost details have to be included in the report.
8. Select **Include cost summary** in the report to include the summary of costs in the report. The cost summary can be either complete (default) or basic.
Select basic.
9. Click on **Next**.
10. On the **Details** page, select the fixed cost details, usage-related details, and other information to be displayed in the report, and click on **Next**.

11. (Optional) on the **Attributes** page, select **Filter the report based on attributes** to define attribute filters.
12. Click on **Submit**.
 - The report is queued for generation. After the report is generated, it is displayed in vCenter Chargeback Manager.
 - A generated report can be archived and stored in the application. After you generate a report, the application displays the generated report.
13. Click on the **Archive Report** icon above the generated report. A dialog that reports whether the action was successful or not is displayed.
14. Click on **OK**.

If the report is archived successfully, the report can be accessed from the **Archived Reports** page.

Summary

In this chapter, we discussed the centralized logging facility of vCloud Director. We have also discussed and learned how to configure logging and how to configure vCloud Director for a scalable deployment. We have also learned how you can efficiently use the cell management tool to maintain vCloud Director better. This chapter also focuses on how to use Chargeback Manager for metering vCloud Director resource as well.

In the next chapter, we will focus on how to add vSphere resources to vCloud Director and manage vSphere storage and network resources.

2

Managing vSphere Resources

vSphere plays a core role in **VMware vCloud Director (vCD)**, that is, providing the required compute, storage, and networking resources. This chapter addresses the crucial requisite to understand the management of these vSphere resources using vCD.

vCenter Server instances expose the vSphere resources and help create cloud constructs using them. VMware vCloud Director treats vCenter and vSphere resources as a pool of resources. On the other hand, the core of a vCloud implementation— containing provider and organization vDCs, external and organization networks, and network pools— is considered as a cloud resource. In this chapter, we discuss how you can modify these vSphere resources and elucidate the properties of their relationship once these cloud resources are added to vCloud Director.

The effective management of vCloud Director (providers and networks) ensures that customers always have the resources they need while using corporate IT assets as well as the highest efficiency and cost effectiveness in their use.

This chapter covers the following topics:

- vSphere compute resources
- vSphere storage resources
- vSphere network resources

vSphere compute resources

vCloud Director depends on vCenter Server to provide vSphere resources to its tenants and on vShield Manager to provide network services to the cloud. Therefore, vShield Manager should be deployed and configured even before vCloud Director is installed.



A unique instance of vShield Manager should be associated with each vCenter Server.

vCD will appear as an extension when you add vCenter server to it, similar to other extensions in the **Solutions Manager** tab in the vSphere client.

Once vCenter Server is added to vCD, the vSphere client sets a property on the vCD-managed VMs, called **managed by property**. This property protects vCD-managed VMs from being modified by the vSphere client.

In addition, changing the vCenter Server connection settings for the vShield Manager is possible; you could even use a different vShield Manager altogether. If vCloud Director loses its connection to a vCenter Server instance or if you change the connection settings, you can reconnect it.

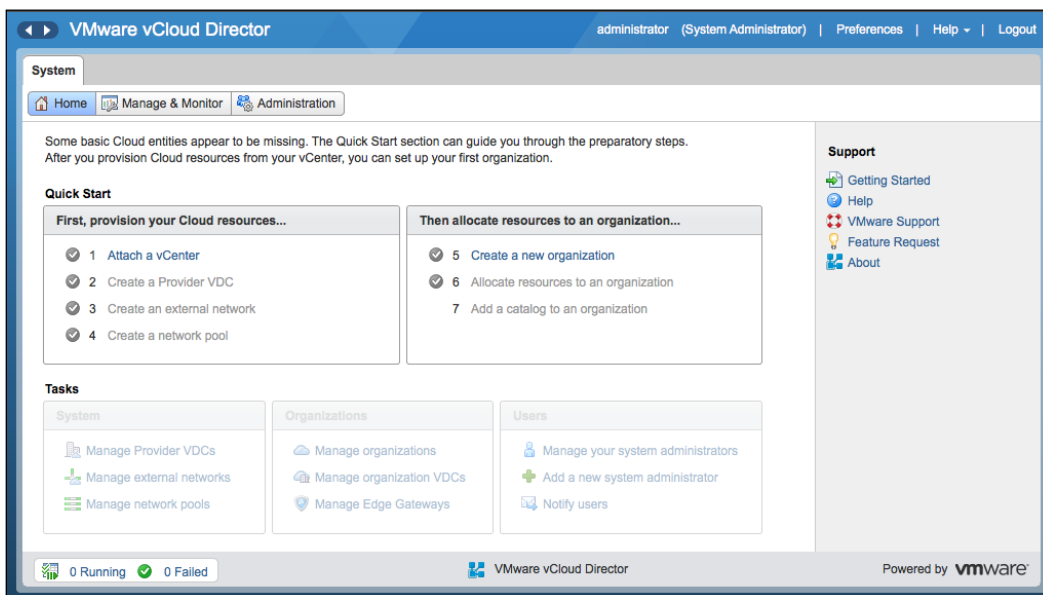
Let's look at how we can add a new vCenter Server instance to vCloud Director.

Registering the vCenter Server

Before adding a new vCenter Server instance, it is mandatory that you register the vCenter Server with vShield Manager. If you don't, you will be prompted with an error—vShield Manager is not registered with the VC <VC Name>—when registering vCenter Server with vCD. In this case, all you need to do is go back and complete the VC registration. To register your vCenter Server with vShield Manager, perform the following steps:

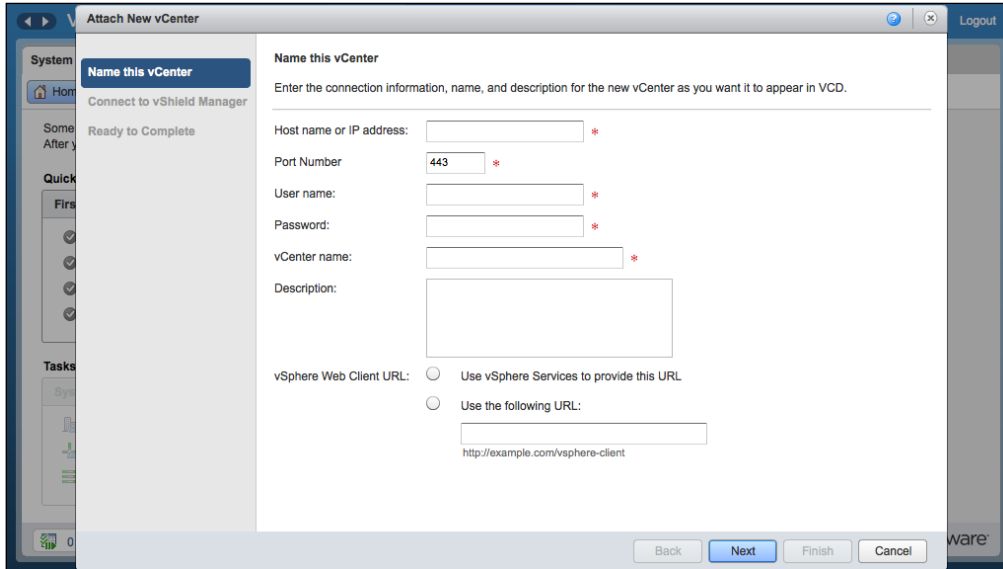
1. Open a browser and type in the vShield Manager URL.
2. Log in as an administrator.
3. By default, you will be redirected to the **Settings and Reports** screen.
4. Go to the **vCenter Server** section and click on **Edit**.
5. Specify the vCenter Server information and credentials.
6. Click on **OK**.
7. You will receive a security warning; click on **Yes**.

8. vCenter Server should now be configured.
Add a new vCenter Server instance before starting the activity. You will need the IP addresses and admin credentials for the vCenter Server instance and vShield Manager.
9. Open the vCloud Director URL in a browser that supports it.
10. Log in to the cloud as an administrator, which should have been done as part of the initial configuration.
11. You will be directed to the screen shown as follows. From here, you can perform the initial setup of vCloud Director:

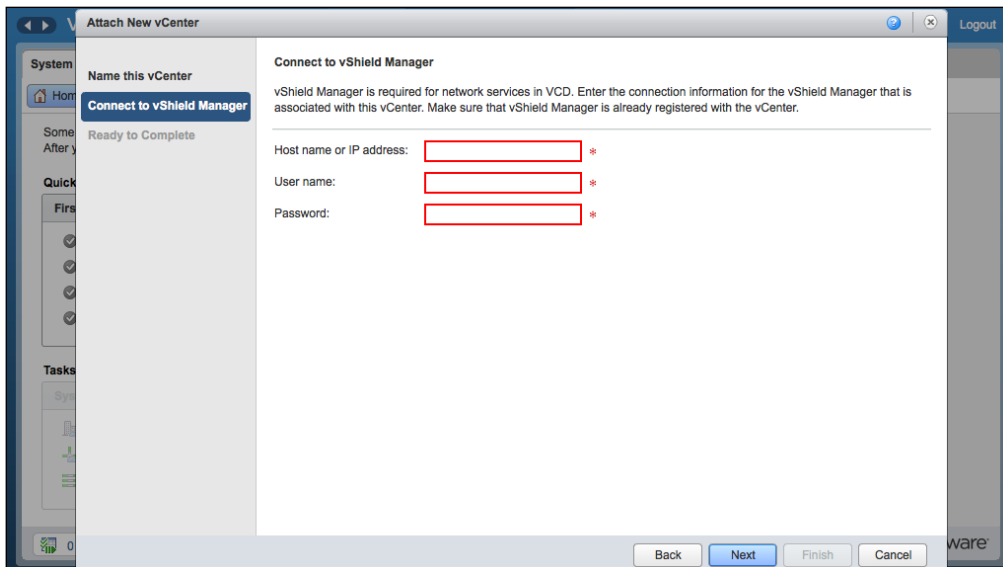


12. The first step is to attach vCenter Server and vShield Manager.
13. Next, click on **Attach a vCenter**.

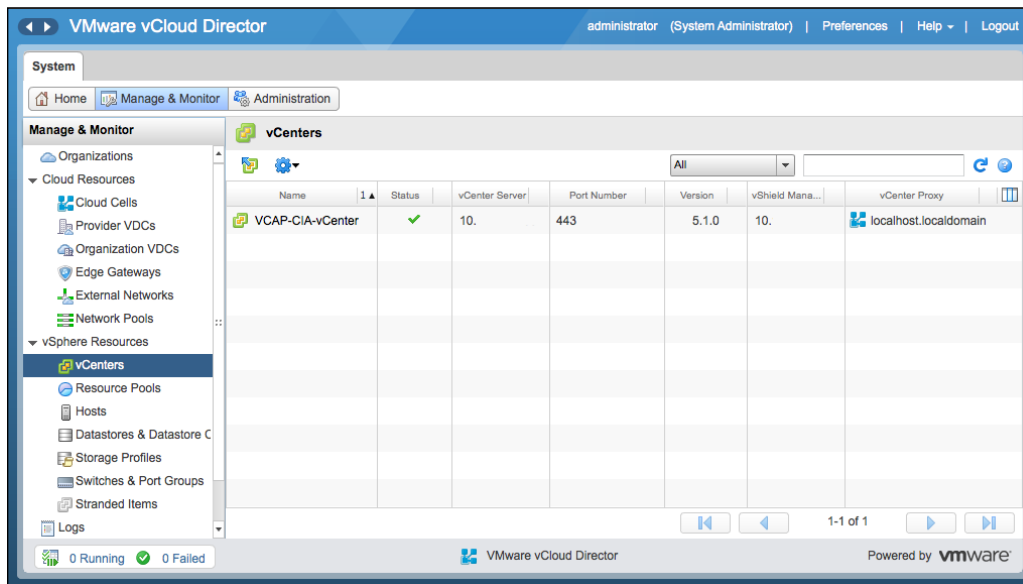
14. This will take you to the **Name this vCenter** page, where you need to specify information for vCenter and click on **Next**.



15. You will now see the **Connect to vShield Manager** page, as shown in the following screenshot. Provide the requisite information for vShield Manager. It is a good practice to use a dedicated user for vCD in vCenter and vShield connections.



16. Once you have specified the requisite information for the vShield Manager Server, click on **Next**.
17. This will take you to the final screen; click on **Finish**.
18. Once you add vCenter Server, you will see it under the **Manage & Monitor** tab.
19. Go to the **Manage & Monitor** tab, and under the **vSphere Resources** section, click on **vCenters**. You will see what is shown in the following screenshot:



Managing ESXi host resources in vCloud Director

Our next step is to create a provider vDC. However before initiating this step, in this chapter, we will learn how to add an ESXi Server in vCenter; this way, we can prepare them for consumption in vCD. Then, we will learn how to disable, unprepare ESXi hosts, and use cases of this. (We will detail the creating of a provider vDC in *Chapter 3, Managing vCloud Director Resources*.)

Adding ESXi hosts to a provider virtual datacenter

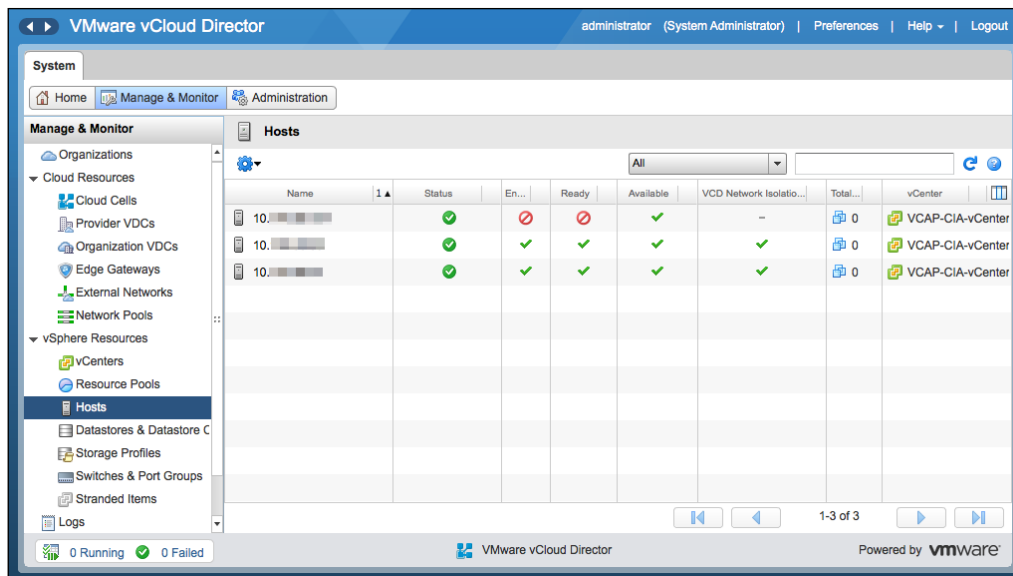
An easy way to increase the compute resources for your provider virtual datacenter is adding ESXi hosts in the cluster backing PvDC. It is crucial that you prepare your ESXi host in vCloud Director once you have added it to vCenter Server; only then will you be able to use its resources.



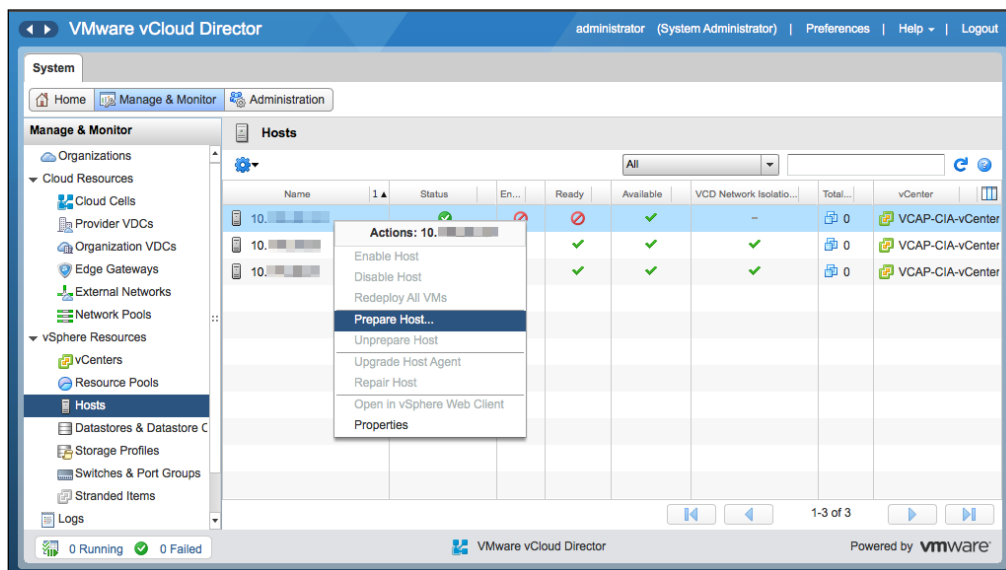
Keep in mind that you cannot prepare a host that is in Lockdown mode; however, you can enable the host once you prepare it.

Preparing an ESXi host will install a specialized agent on the ESXi host for vCloud. Let's look at how to add an ESXi host to vCenter and prepare it in the vCloud Director using the following steps:

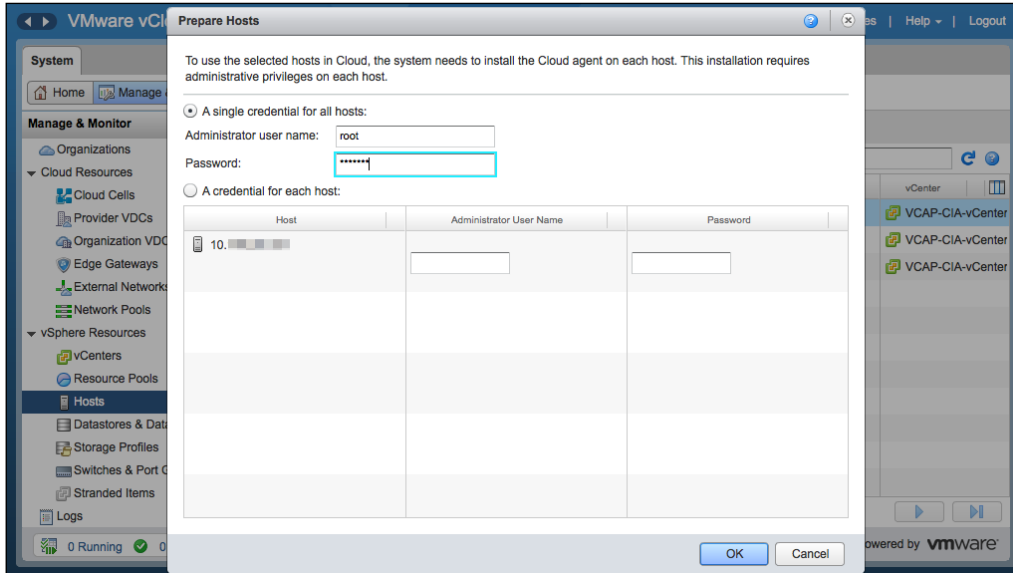
1. Log in to the vCenter Server.
2. Click on the **Hosts and Clusters** option.
3. Right-click on the cluster and select **Add Host**.
4. Input the ESXi host connection information – IP address, hostname, and credentials – and add the ESXi host.
5. Open a web browser and type in the vCD URL, for example, `https://serverFQDN/cloud`.
6. Log in to vCD as the administrator.
7. Click on **Manage & Monitor**.
8. Click on **Hosts**, as shown in the following screenshot:



9. Right-click on the newly added ESXi host and select **Prepare Host**, as shown in the following screenshot:




10. Provide the requisite credentials for the ESXi host, as shown in the following screenshot:



You can perform some of the management functions from vCloud Director once you have added the vSphere resources to vCloud Director. You can also use vSphere Client to manage these resources. However, resorting to the vSphere resources assigned to vCloud is not the best practice.

Disabling and unpreparing ESXi hosts

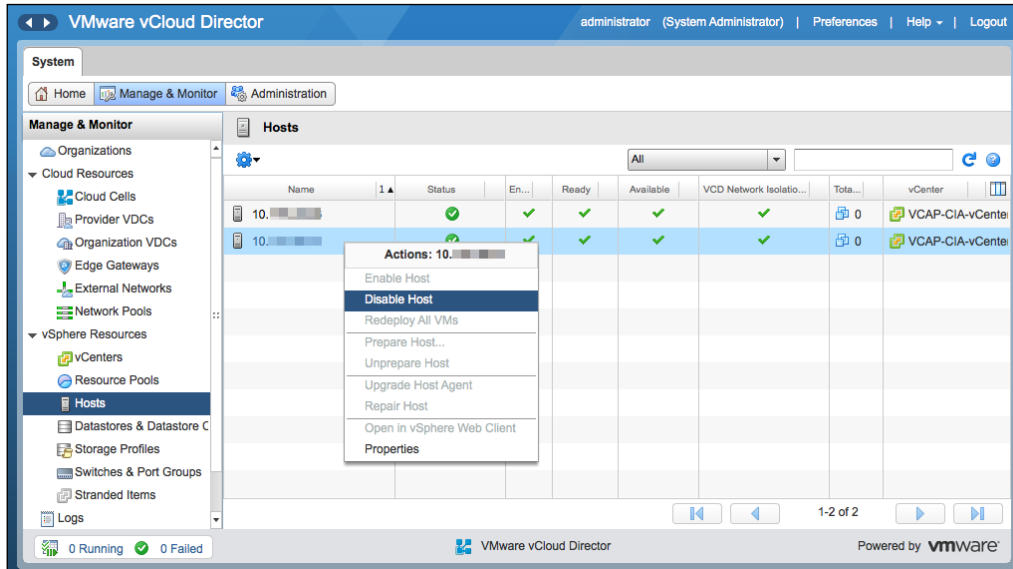
When you plan for a maintenance activity, that is, upgrading or patching the host, you can disable a host to prevent vApps from starting up on it. Virtual machines that are already running on the host are not affected.

 vCloud Director enables or disables the host for all provider vDCs that use its resources.

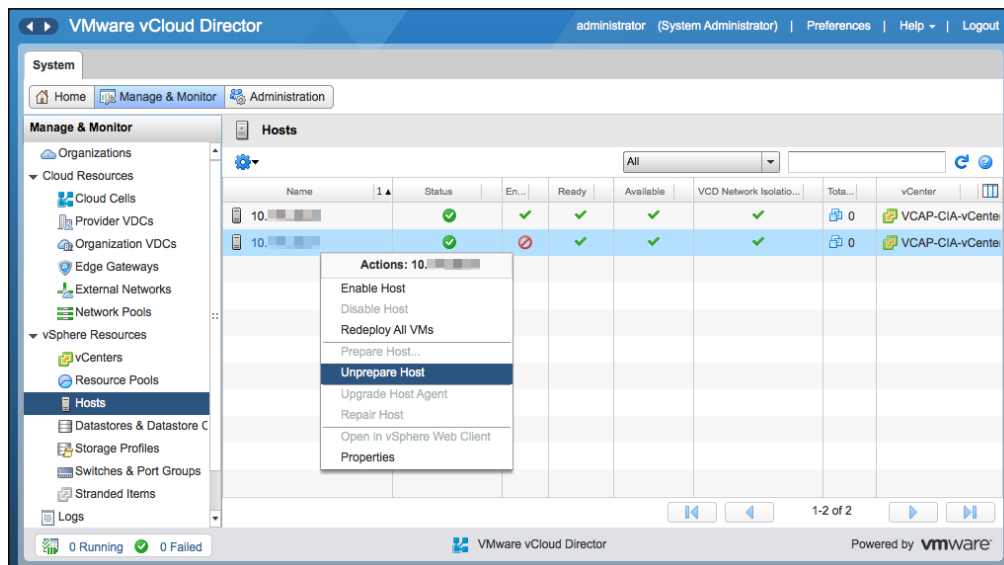
You can also unprepare that ESXi hosts in vCloud Director using the following steps::

1. Open a web browser and type in the vCD URL, for example, `https://serverFQDN/cloud`.
2. Log in to vCD as the administrator.
3. Click on the **Manage & Monitor** tab.

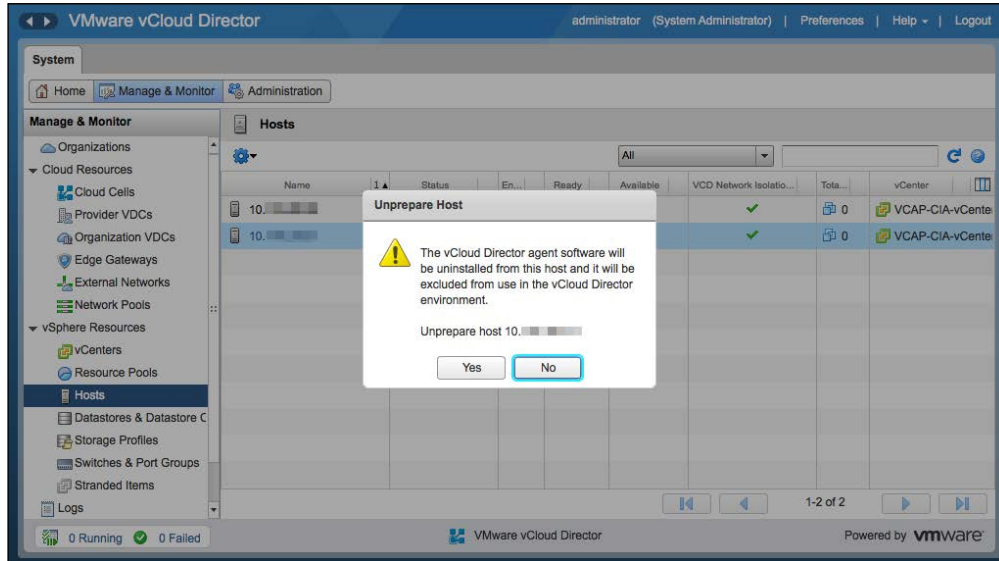
4. Click on **Hosts**.
5. Right-click on any ESXi host and select **Disable Host**, as shown in the following screenshot:



6. Once this is complete, right-click on the host and select **Unprepare Host**, as shown in the following screenshot:




7. Select **Yes** on the warning screen, as shown in the following screenshot:



Upon submitting the unprepared task, a signal is sent to the ESXi host to place it in the maintenance mode. Once this operation is complete, the vCloud agent is uninstalled from the host and the host will exit the maintenance mode.

8. You can also use ESXCLI to manually unprepare a host:

```
~ # esxcli software vib remove -n vcloud-agent
```

 Run this command on the ESXi server; it has to be in maintenance. This will uninstall the agent, however; vCD continues to think it's prepared. So you will still have to run the unprepared task in vCD; otherwise, you will be out of sync.

Monitoring vSphere resources in vCloud Director

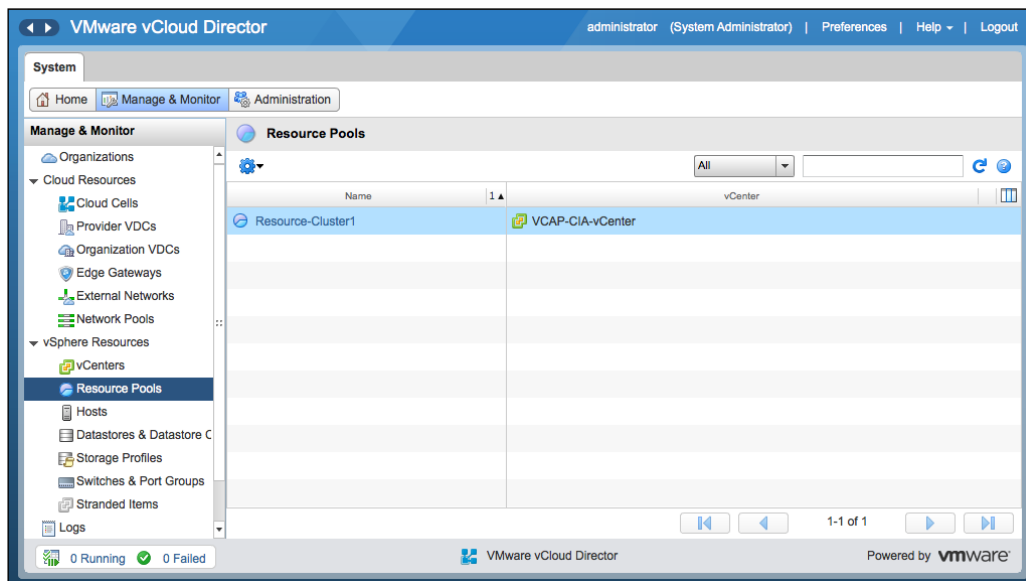
Create and configure resource pools, which can be vSphere clusters as well. You will be able to view information about the resource pools that PvDC uses from vCloud Director. Viewing the used and total CPU as well as memory reservations for a resource pool is possible and easy. You can also see the data stores available in the resource pool.



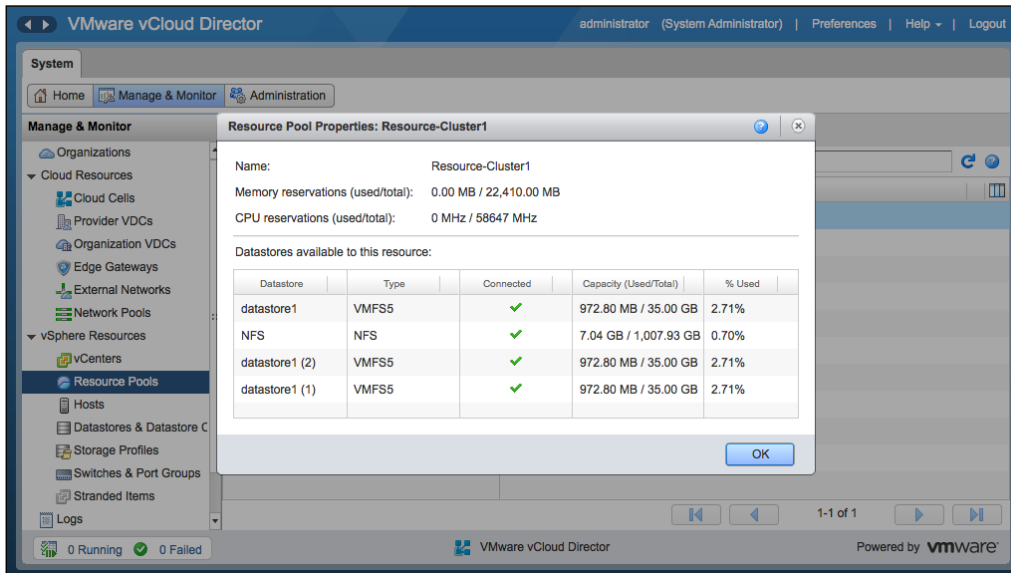
We recommend that you dedicate an entire cluster to a provider vDC. However, having multiple resource pools in a single cluster is possible, with each resource pool assigned to a Provider vDC.

Using the following steps, you can manage and monitor vSphere resource pools:

1. Open a web browser and type in the vCD server URL, for example, `https://serverFQDN/cloud`.
2. Log in to vCD as the administrator.
3. Click on the **Manage & Monitor** tab.
4. Click on the **Resource Pools** option.
5. Resource pools are visible in the **Resource Pools** panel, as shown in the following screenshot:



- Right-click on any of the resource pools and click on **Properties**. This will show you CPU and memory reservations and the datastore name with its utilization, as shown in the following screenshot:



vSphere storage resources

vCloud Director 5.1 introduced the use of **storage profiles**. vCloud Director now leverages the capabilities of vSphere storage profiles and clusters (SDRS or Storage DRS clusters) to provide profile- or class-driven storage to vCloud tenants. vSphere provides a generic, default storage profile without you having to create a storage profile. The storage profile is denoted by * (or any). This profile includes all of the datastores from your ESXi hosts in the vSphere cluster, which means your local datastores will also be added to it.

Typically, do not host your workloads on a local datastore. Creating a storage profile that will access only the specified datastores (shared) and using it to create your PvDC and assign class-driven storage profiles (for example, gold, silver, and bronze) is not recommended.

vSphere storage profiles are based on VASA capabilities or user-defined storage capabilities. When creating a Provider vDC, you can assign one or more vSphere storage profiles. Organization vDCs receive their storage from a single provider vDC. This means when the Provider vDC accesses storage from multiple instances in the vSphere storage profile, storage from those instances is also accessible by the organization vDC.



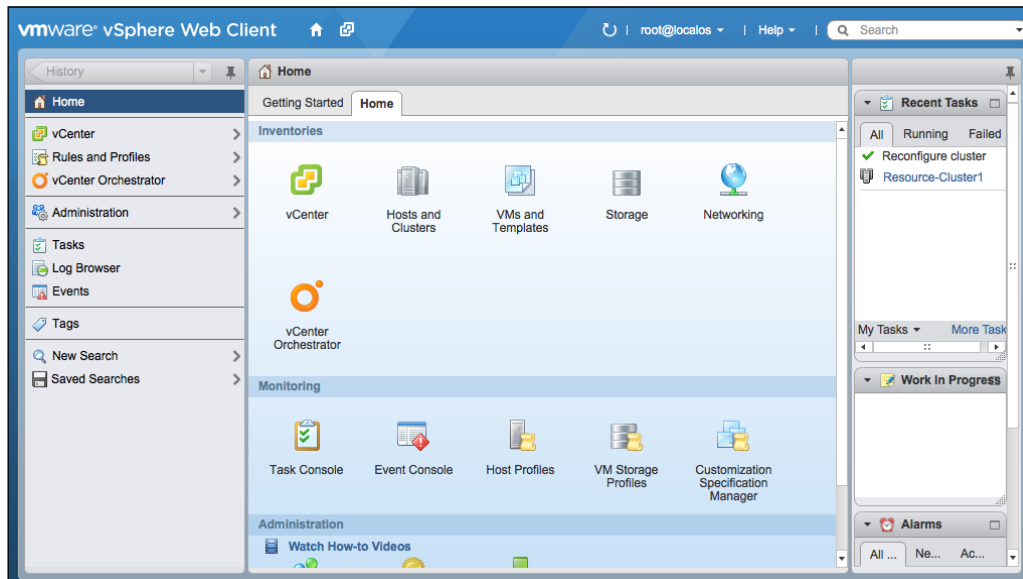
When upgrading vCloud Director from 1.5 to 5.1, you need to consider a minor aspect. For more information, read the following blog:

<http://stretch-cloud.info/2013/01/upgrading-your-vcloud-from-1-5-to-5-1-watch-out-for-the-any-storage-profile-caveat/>

Configuring storage profiles

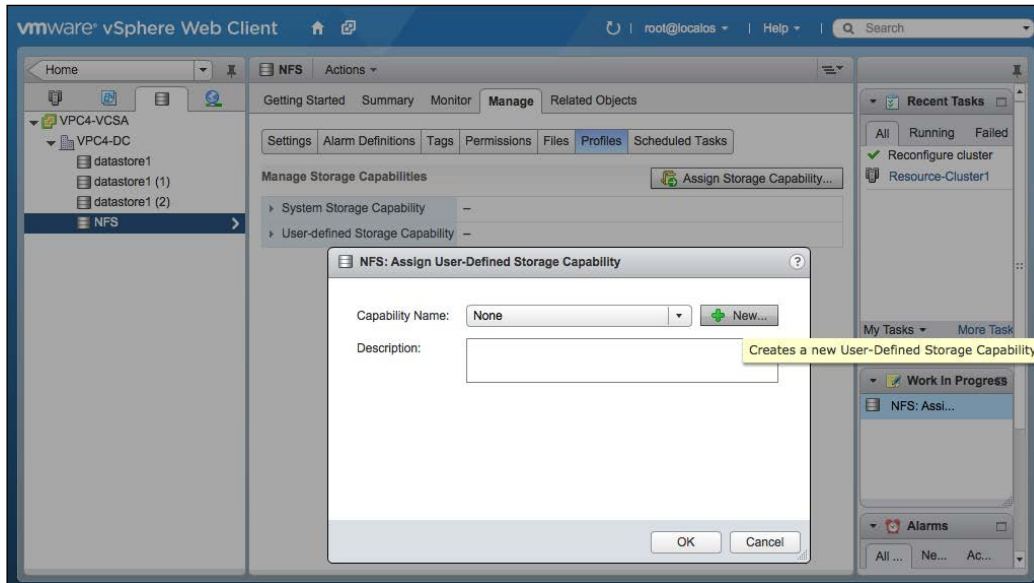
Let's now discuss how we can configure storage profiles in vCenter. First, define the storage capabilities as datastores can be used in storage profiles. To do so, perform the following steps:

1. Open a browser and log in to the vCenter Server through the vSphere Web Client. You will be redirected to the **Home** screen, as shown in the following screenshot:



2. Click on the **Storage** link.
3. Expand the datastores.

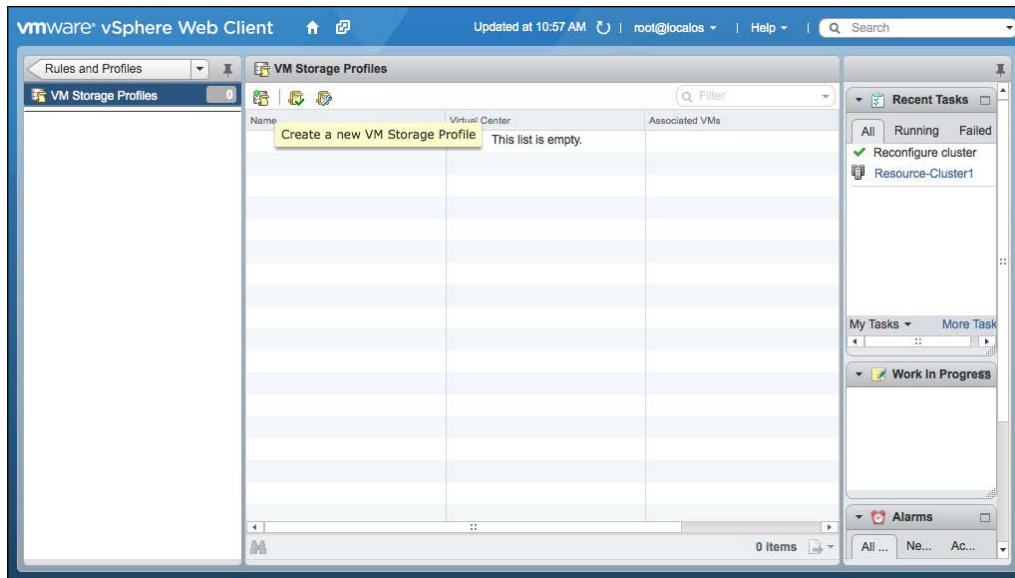
4. Click on your datastore and then on **Assign Storage Capability**, as shown in the following screenshot:



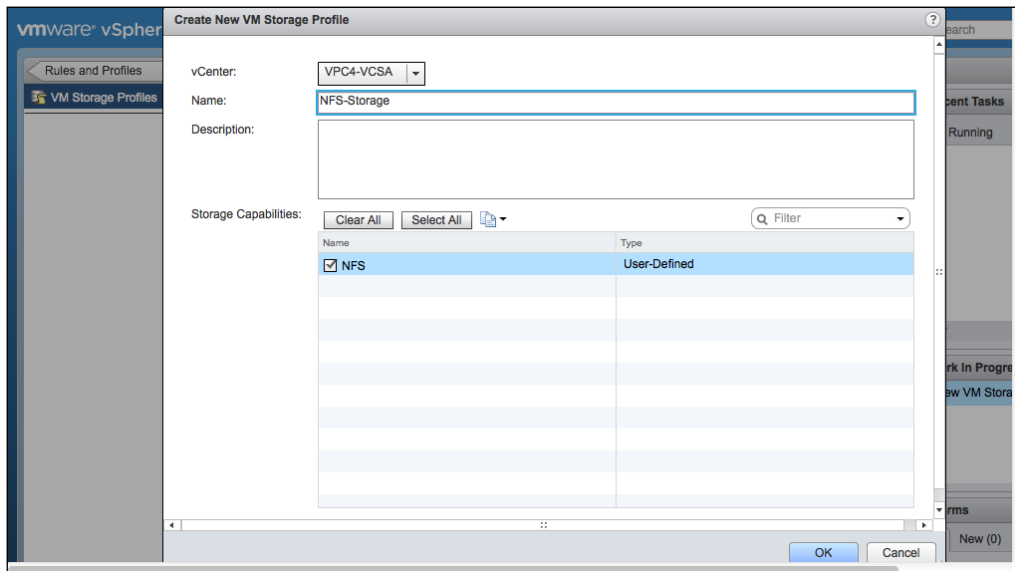
5. Click on **New**.
6. Specify a storage capability name.
7. Double-click on **OK**.

This will create the user-defined storage capability. Now, let's create the storage profile that will use this recently created storage capability.

1. Click on **Home**.
2. Next, click on the **Rules and Profiles** option.
3. Click on **VM Storage Profiles**.
4. Then click on the **Create a new Storage Profile** icon, as shown in the following screenshot:

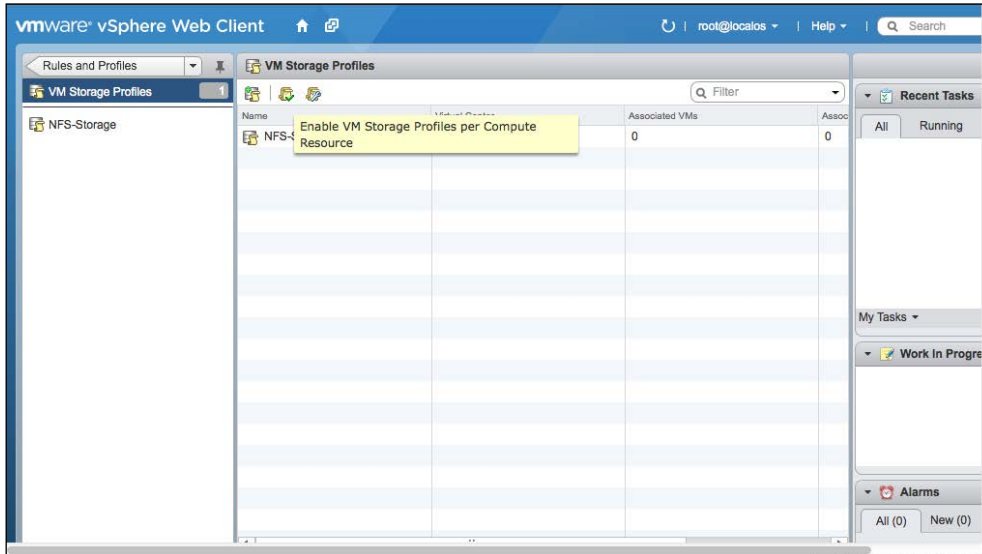


5. Specify a name in the **Name** textbox in the **Create New VM Storage Profile** dialog box and select the storage capability you created in the sixth step of the *Configuring storage profiles* section. Once you have done this, you will see the output shown in the following screenshot:

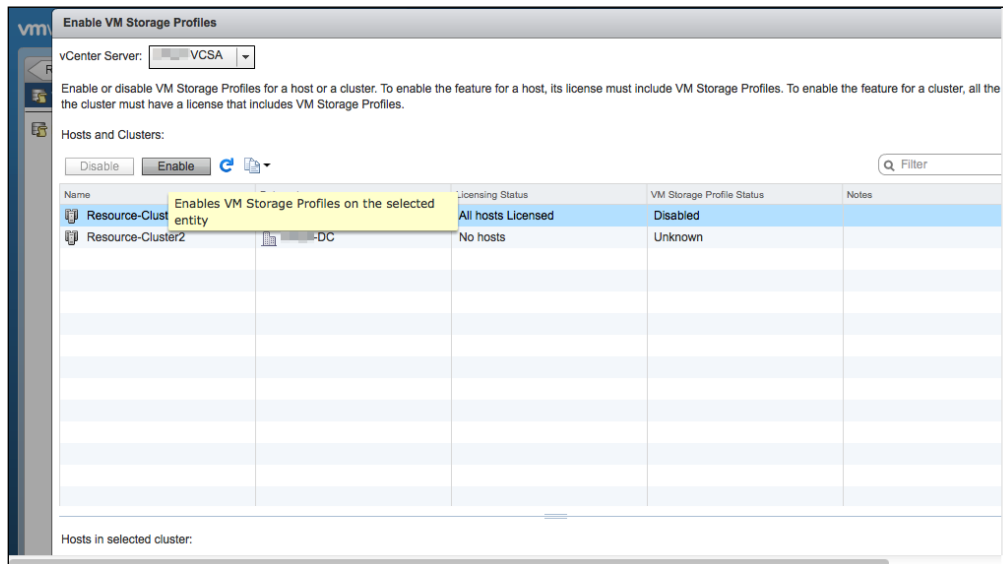


6. Click on **OK**.

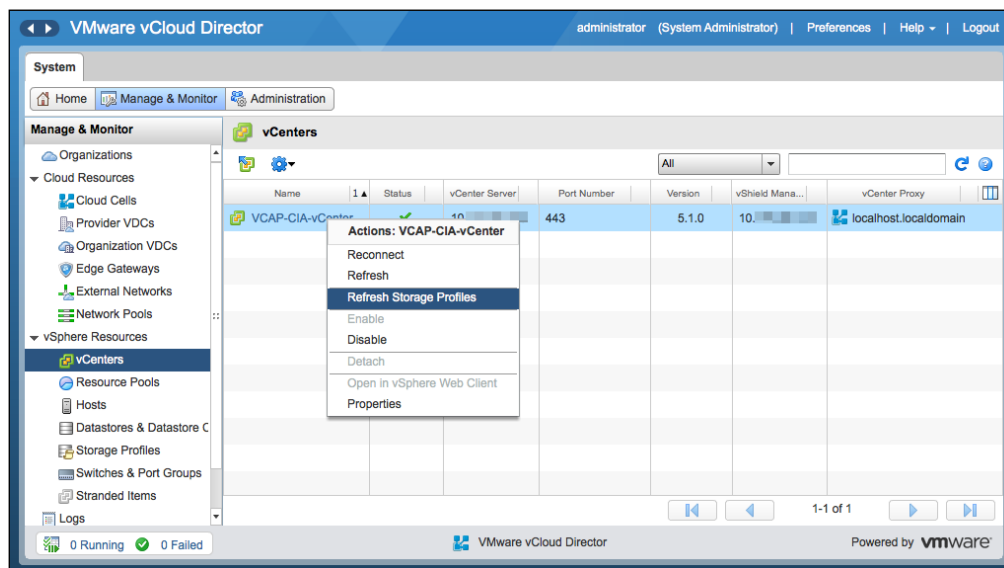
- Now enable VM storage profiles for your vSphere cluster. To do this, click on the **Enable VM Storage Profiles per Compute Resource** icon, as shown in the following screenshot:



- Select the cluster where you want to enable the storage profile and click on the **Enable** button, as shown in the following screenshot:



9. Click on the **Close** button.
10. Open up a web browser. Type the URL of the vCD server, for example, `https://serverFQDN/cloud`.
11. Log in to vCD by using the administrator user ID and password.
12. Click on the **Manage & Monitor** tab.
13. Select the vCenter section.
14. Right-click on the vCenter and select **Refresh Storage Profiles**, as shown in the following screenshot. The storage profile will appear once you create a Provider vDC.



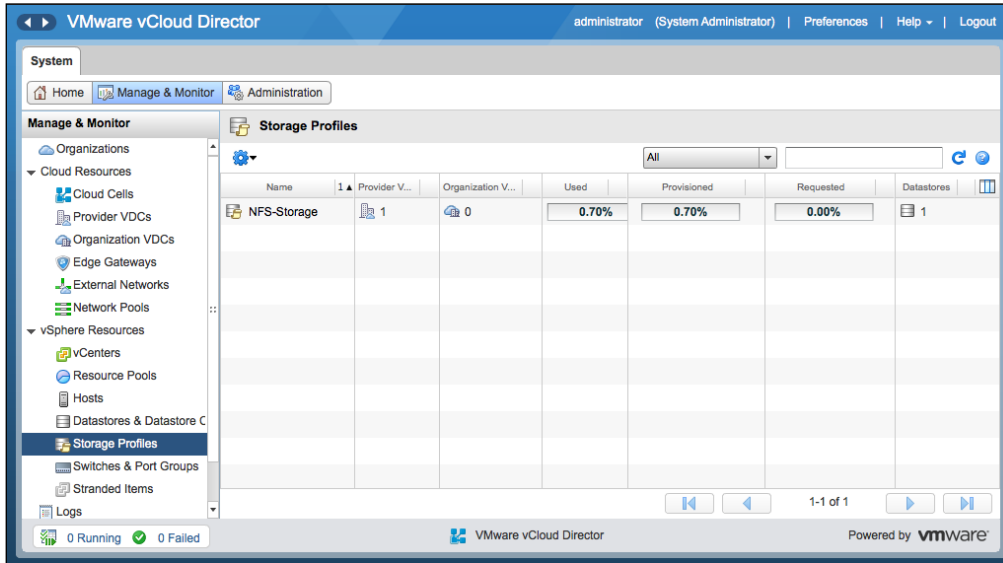
Monitoring storage profiles in vCloud Director

There are a couple of things that you can do with the storage profiles in vCloud Director. For example, it is really easy to identify which storage profile is attached to which datastore. Also, you can determine the vDCs using a specific storage profile. Also, you can find out the number of datastores inside each storage profile and their space metrics.

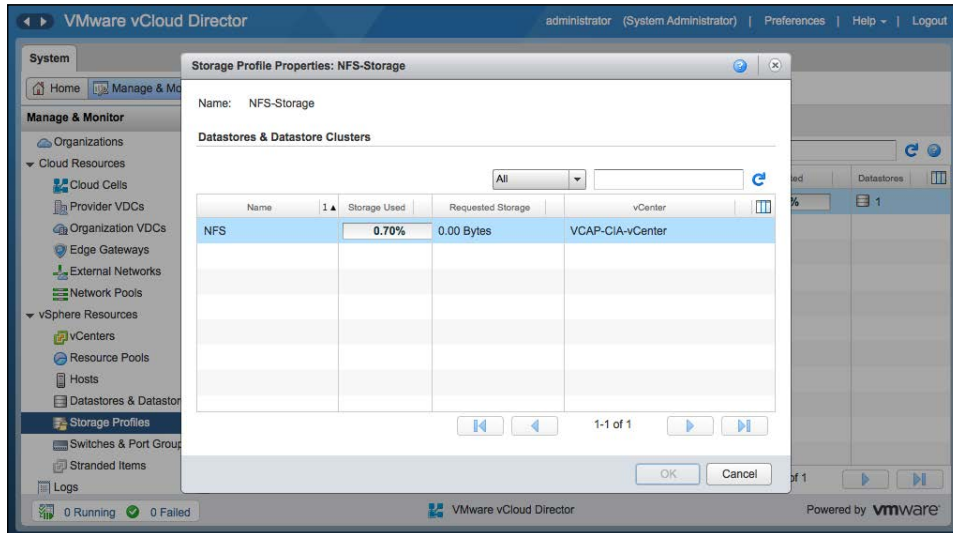
Now, let's take a look at managing and monitoring storage profiles in vCloud Director.

1. Open a web browser and log in to vCD as the administrator.
2. Go to the **Manage & Monitor** tab.

3. Click on the **Storage Profiles** option in the tree list on the left-hand side, which details the storage profiles shown on the right-hand side, as shown in the following screenshot:



4. Right-click on any of the storage profiles and click on **Properties**.
5. This will show you datastores and datastore clusters in the selected storage profile, as shown in the following screenshot:



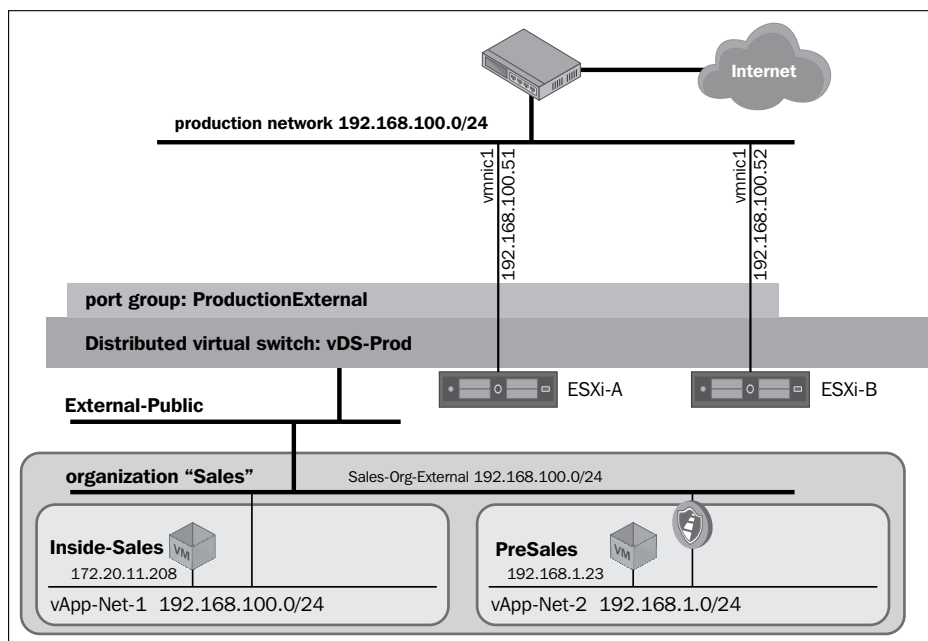
Managing vSphere network resources

vCloud Director has different types of networks; these are external networks. It also has different types of network pools; external networks should be connected to vSphere port groups. Each external network is backed by a single port group. Preferably, use a single distributed virtual switch because it has several port groups in it and each one backs a different external network. Multiple external networks should be traversed through different VLANs.



You can consider external networks as internet facing; however, this is not mandatory.

An important aspect that warrants understanding is how external networks on the provider side are built from vSphere networks. The following diagram shows an example of the external network and the organization network connected to it:

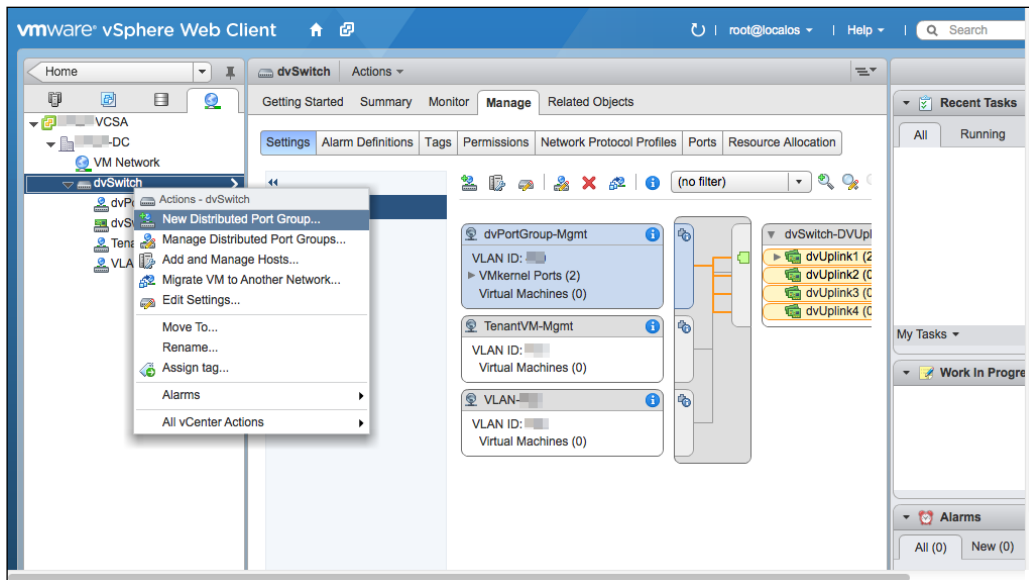


In the preceding diagram, **External-Public**, a provider-level external network, is built from the `ProductionExternal` port group. The `ProductionExternal` port group is located in the **vDS-Prod** distributed virtual switch. The hosts `ESXi01` and `ESXi02` and connected to the `vDS-Prod` distributed virtual switch.

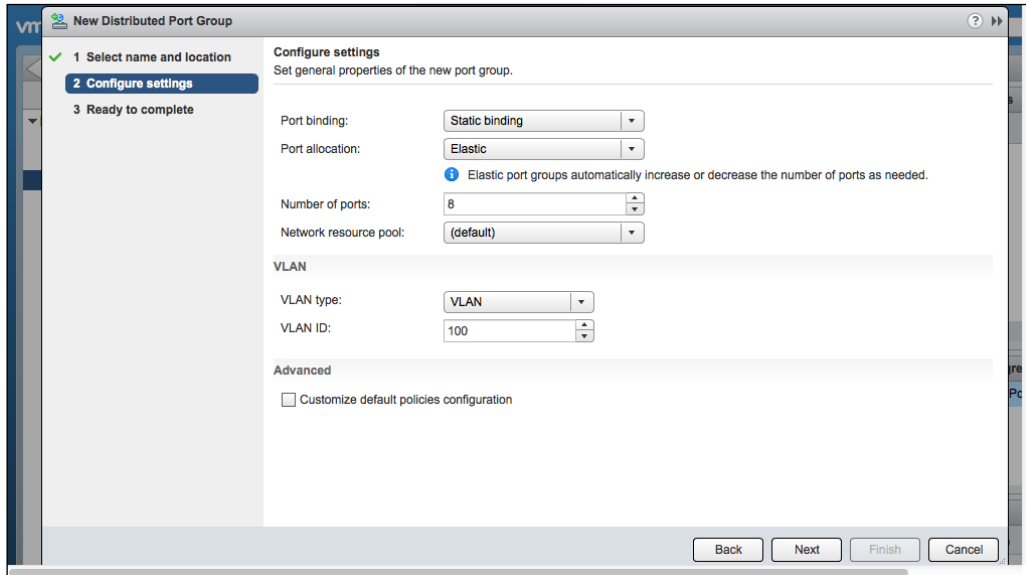
Adding the vSphere network port group

To create and manage vSphere port groups for vCloud Director, follow the given steps:

1. Log in to the vSphere Web Client as the administrator.
2. You will land on the **Home** screen; click on the networking link there.
3. Expand the **dvSwitch** option on the left-hand side of the panel.
4. Right-click on the **dvSwitch** option and click on **New Distributed Port Group**, as shown in the following screenshot:



5. Specify a port group name and click on **Next**.
6. Then, select the VLAN number (optional), as shown in the following screenshot and click on **Next**:

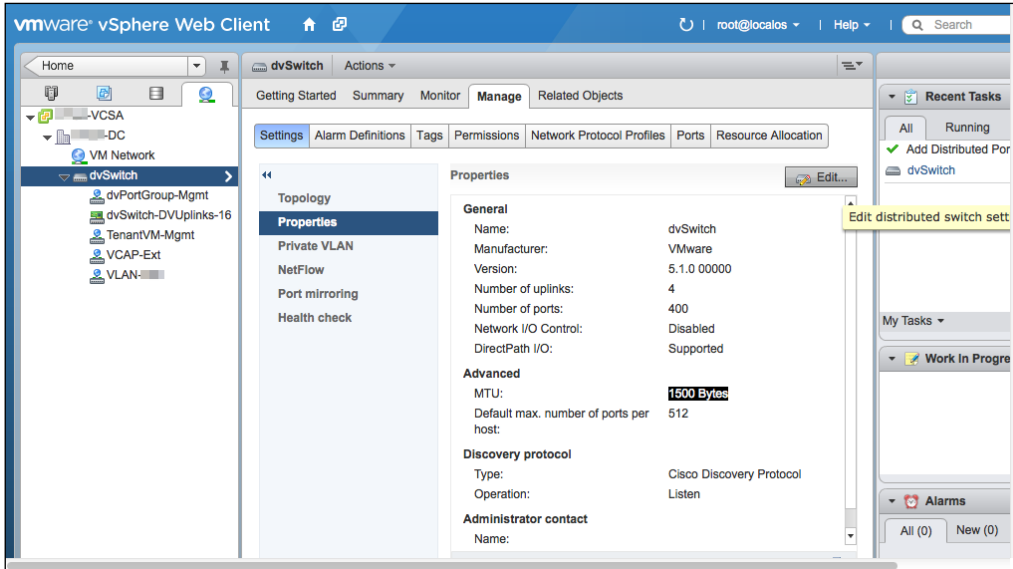


7. Click on **Finish** to create this port group.

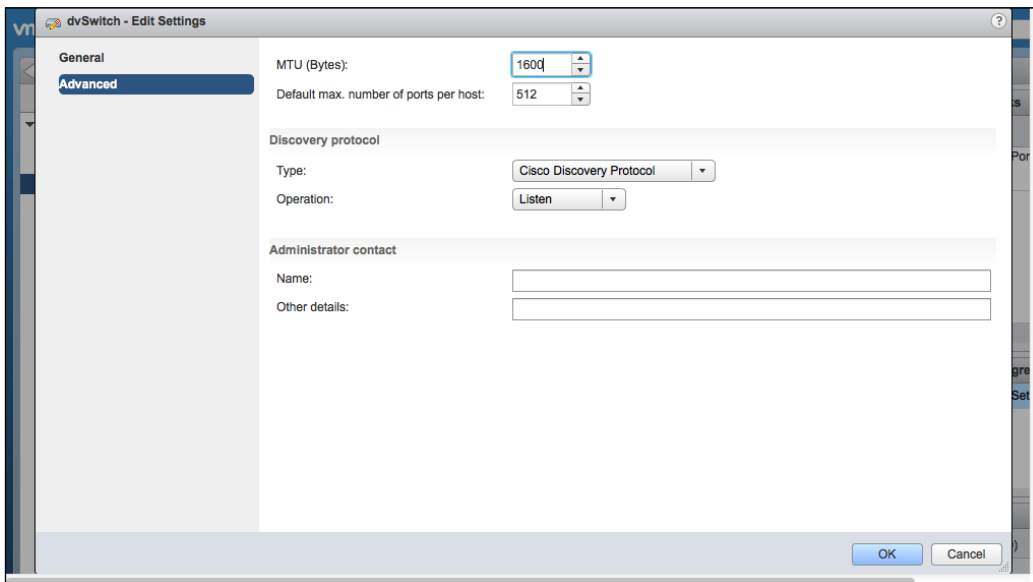
Also, change the MTU settings of the vDS so that you can use the vDS for your VXLAN deployment. (VXLAN deployment is discussed in the next section.) Execute the following steps to change the MTU settings:

1. On the **Networking** page, expand the vDS on the left-hand side.
2. Click on a vDS and on the right-hand side, click on the **Manage** tab.

- Next, click on the **Properties** tab on the left-hand side and under the **Advanced** section, you will see **MTU as 1500 Bytes**, as shown in the following screenshot:



- Click on the **Edit** button and then on the **Advanced** link on the left-hand side.
- Change the **MTU** option from **1500** to **1600** and click on **OK**, as shown in the following screenshot:



Understanding VXLANs

Virtual eXtensible Local Area Network (VXLAN) is a network overlay that encapsulates layer 2 traffic within layer 3. This is a prototype submitted in IETF by Cisco, VMware, Citrix®, Red Hat, Broadcom, and Arista.

VXLAN provides the following features:

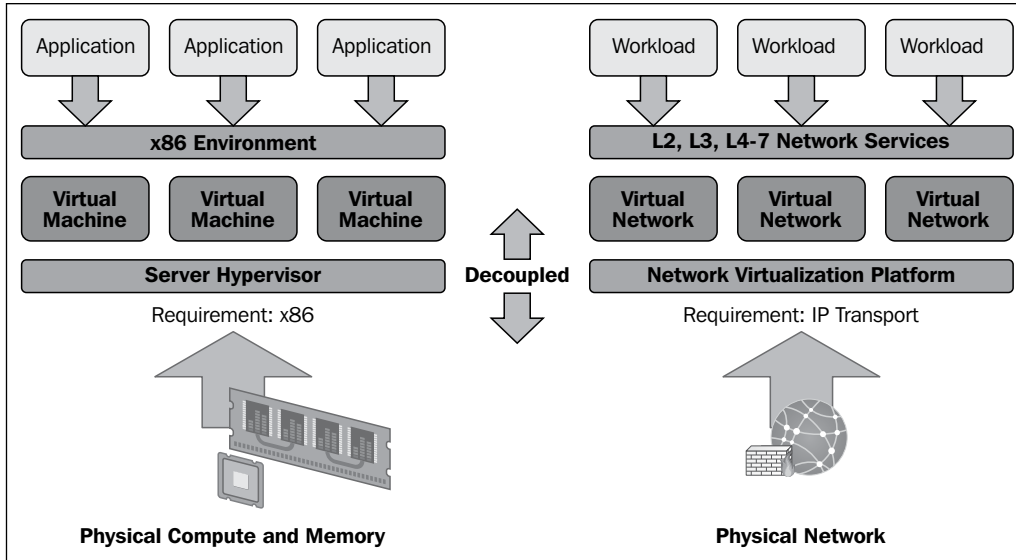
- Ability to manage overlapping addresses between multiple tenants
- Decoupling of the virtual topology provided by tunnels from the network's physical topology
- Support for virtual machine mobility independent of the physical network
- Support for unlimited numbers of virtual networks (in contrast to VLANs for example)
- Decoupling of the network service provided to servers from the technology used in the physical network (for example, providing an L2 service over an L3 fabric)
- Isolating the physical network from the address of the virtual networks, thus avoiding issues such as MAC table size in physical switches
- VXLAN provides up to 16 million virtual networks in contrast to VLAN's limit of 4094
- Since it is application agnostic, all work is performed in the ESXi host

VXLAN across VM traffic is tunneled through a layer 3 network and it is handled by a VXLAN module installed in each ESXi host.

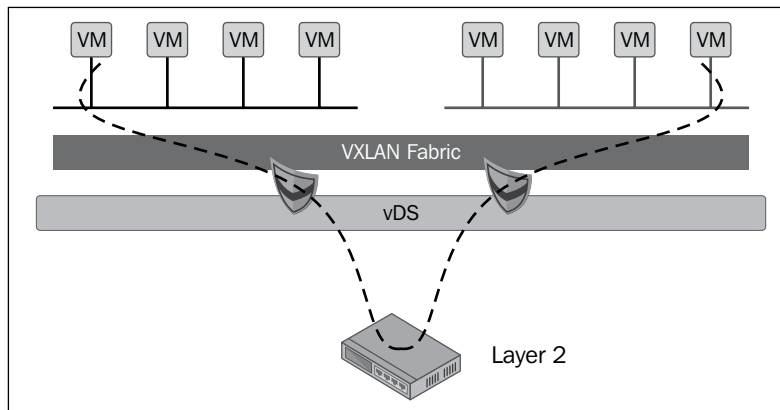
VXLAN requires certain mandatory components as follows:

- vSphere Enterprise Plus Edition license and vCNS licenses
- vShield Manager
- VMware Distributed Switch
- Virtual Tunnel End Point (VTEP)
- VMware vShield Edge

The analogy between computer and network virtualization (overlay transport) is illustrated in the following diagram:

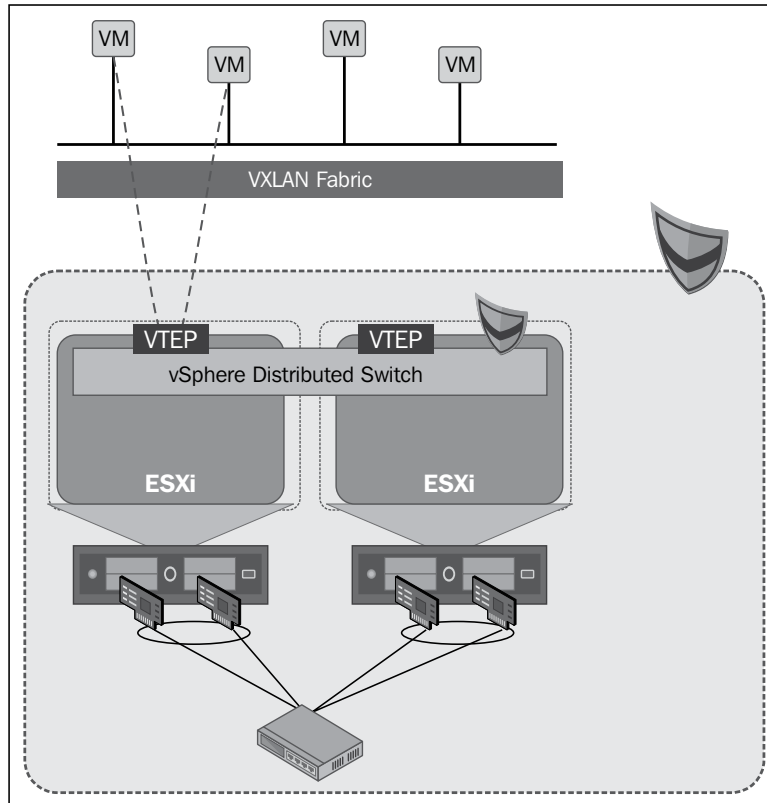


The following diagram shows a packet flow across virtual wires on the same layer 2 VXLAN transport network:

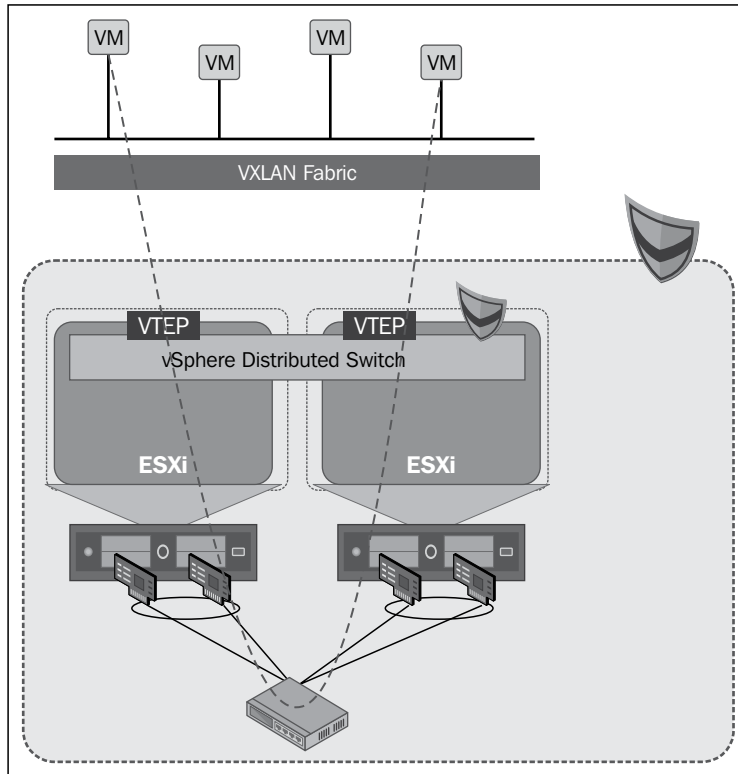


This contrasts the packet flow across virtual wires on different layer 3 VXLAN transport networks. Thus, instead of the L2 network, the packet will traverse through the L3 network.

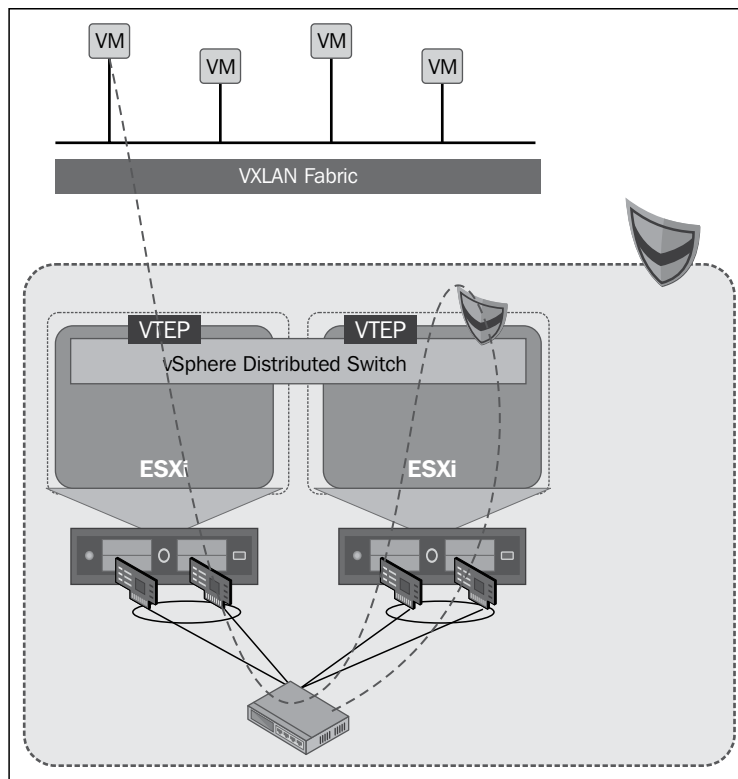
In VXLAN intra-host packet flow, a VM sends the packet to a remote destination on the same virtual wire, and the packet hits vDS and is forwarded to a destination VM. This is illustrated in the following diagram:



Similarly, in an inter-host packet flow, VM sends a packet to a remote destination on the same virtual wire; destination VM is remote and the packet will traverse the VXLAN network. Then the ESXi host encapsulates the packet and transmits it via the VTEP VMkernel adapter. Finally, target the ESXi host running the destination VM receives the packet on the VTEP, and forwards it to VM. This is illustrated in the following diagram:



On the other hand, for a routed packet flow in VXLAN, VM transmits a packet to a remote destination. The VTEP kernel module in the ESXi host encapsulates a packet and transmits it on the VXLAN network. The ESXi host that runs the Edge device receives the packet and processes it through the rule engine. Then, this packet is processed using the firewall/NAT/routing rules and is sent out through the external interface on the Edge device. Finally, the packet hits the physical network infrastructure. This process is illustrated in the following diagram:

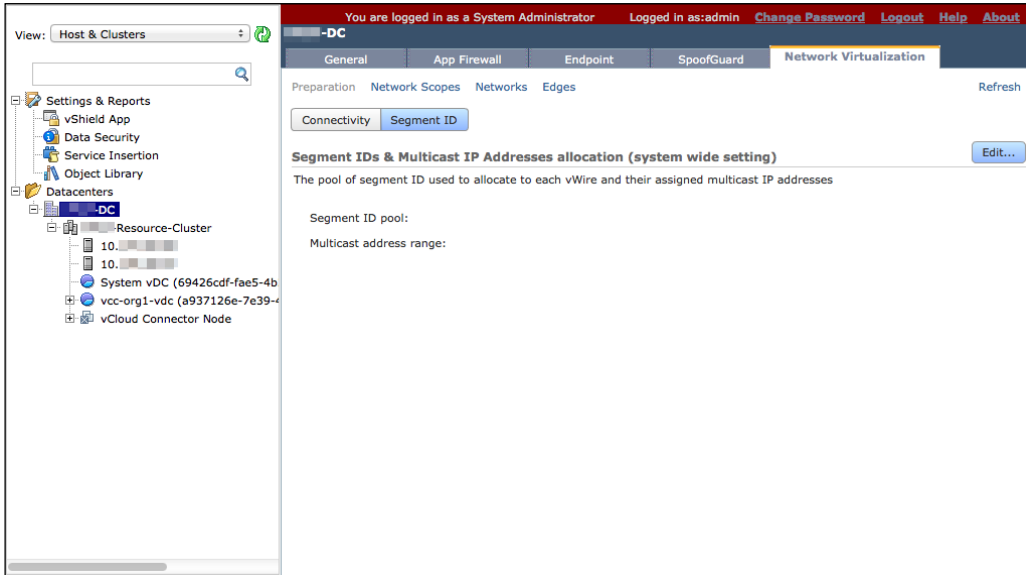


Preparing VXLAN for vCloud Director

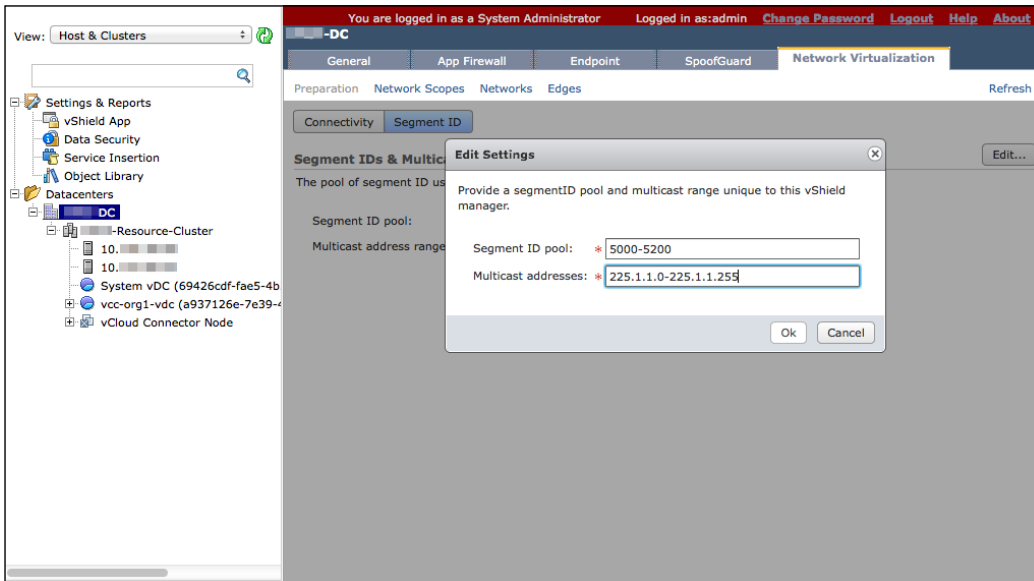
To prepare your vSphere cluster for VXLAN, perform the following steps:

1. Open a web browser and log in to the vShield Manager.
2. Expand the **Datacenters** tree list and click on your datacenter.
3. Click on the **Network Virtualization** tab on the right-hand side.
4. Select the **Preparation** link.
5. Click on the **Segment ID** tab.

6. Then click on the **Edit** button, as shown in the following screenshot:

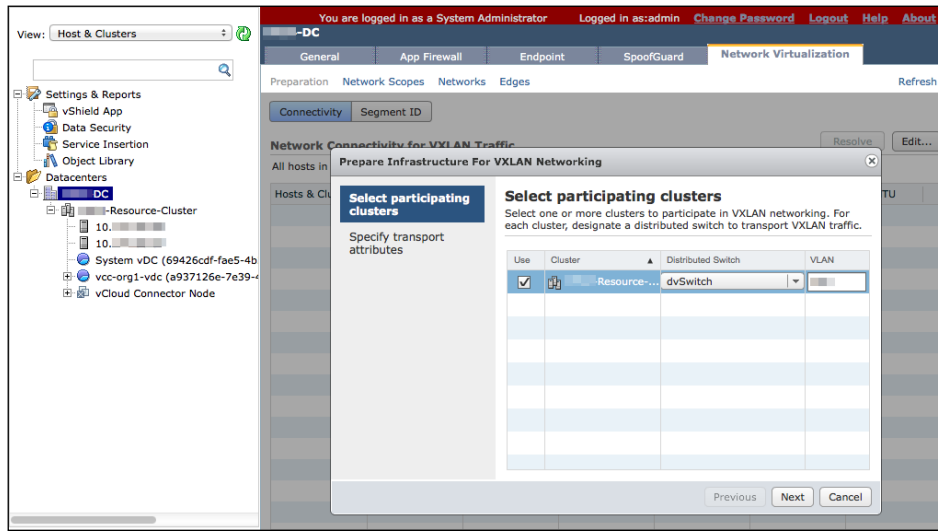


7. Next, insert the segment ID pool and multicast address range, as shown in the following screenshot:



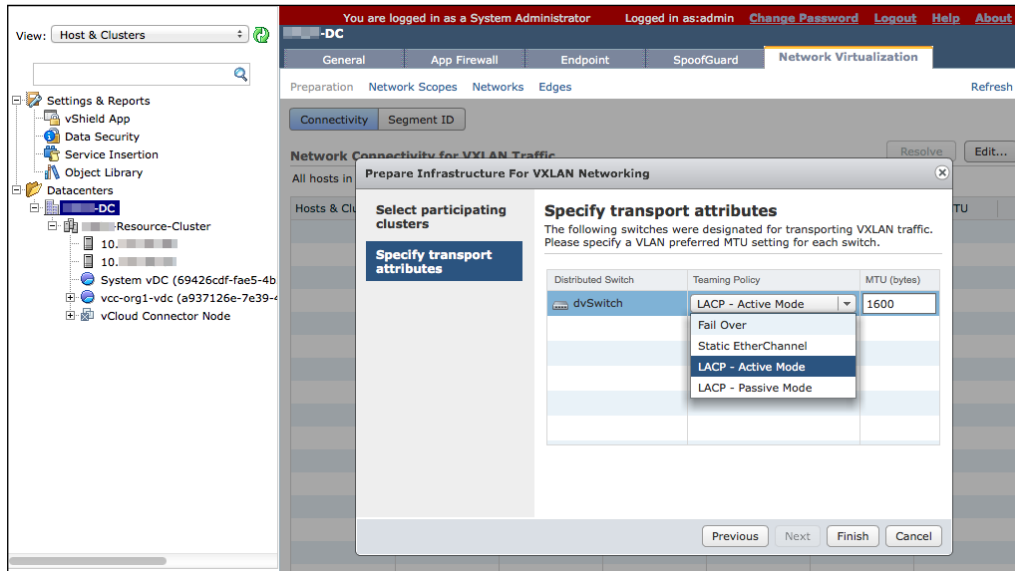
8. Click on **OK**.

9. To configure cluster connectivity, click on the **Connectivity** tab.
10. Then click on the **Edit** button.
11. Select the vSphere cluster and the distributed vSwitch from the drop-down combobox and specify VLAN. Once this is done, click on **Next** as shown in the following screenshot:



12. Doing this will take you to the **Specify transport attributes** page. Here, select **Fail Over** from the drop-down box under the **Teaming Policy** tab.

- As shown in the following screenshot, by default, the **MTU (bytes)** value should be **1600** (leave this as is):



- Click on the **Finish** button.
- Your cluster is now prepared, the ESXi hosts are in the maintenance mode, and the VXLAN agents are installed. Post that and check whether the cluster and host are ready. The status should be **Ready**.
- Expand the cluster and do the following:
 - Make sure that the status of each ESXi host is **Ready**.
 - Make sure that each **virtual machine network interface card (vmnic)** has acquired an appropriate DHCP-assigned address (you can use a static address as well) and is assigned to a unique and automatically created vDS port group. You can identify the new dvPort groups using the unique naming convention, vxw-dvs-xxx-virtualwire-xxxx.

VMkernel modules (VTEP) are pushed and enabled on all of the hosts in the cluster, and all hosts in the cluster are automatically enabled for the purpose of VXLAN networking.

Summary

In this chapter, we discussed vSphere compute resources and how to add or remove these in vCloud Director. We also discussed storage resources and how to propagate storage resources to the vCloud Director. Finally, we explained VXLAN and how to manage vSphere port groups.

In the next chapter, we will learn how to manage network resources, provider vDCs, organization vDCs, and organizations.

3

Managing vCloud Director Resources

VMware vCloud Director has two types of virtual datacenters (vDCs): provider and organization vDCs. A provider vDC is a collection and an abstraction of storage, CPU, and memory resources. Provider vDC allows you to manage and use these resources and organization vDCs are subsets of the provider vDCs.

Provider vDCs are created and managed by the vCloud Director system administrator and provides resources from vSphere resource pools. The resource pool is generally a cluster. You could also have a single resource pool inside a cluster or expand provider vDCs to contain multiple resource pools or clusters.

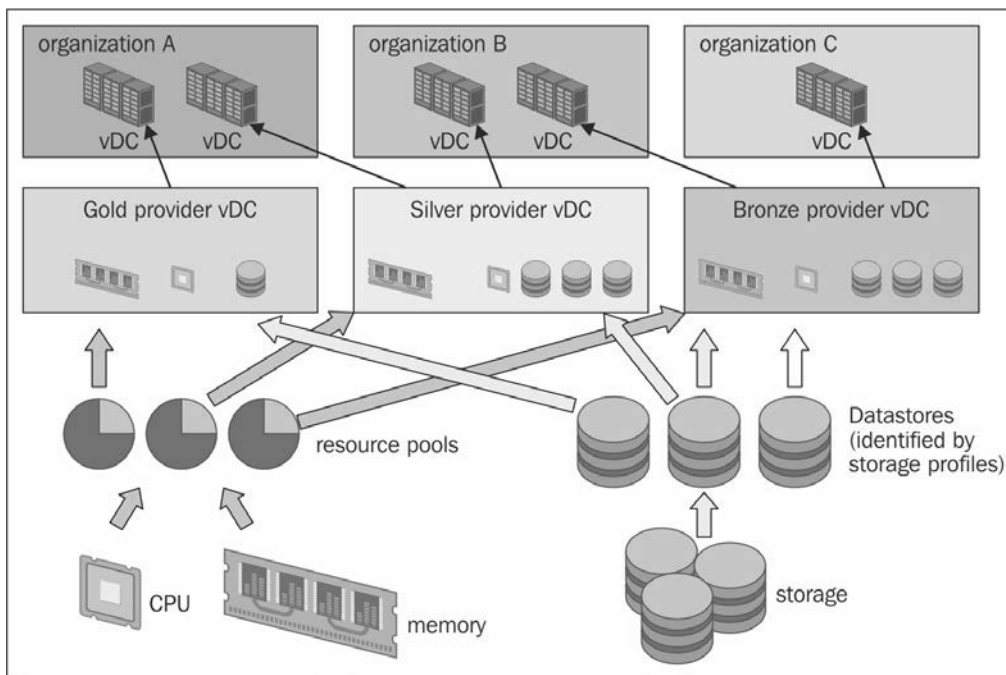
Provider vDC resources include CPU and memory as well as storage, which is discovered using a VMware vSphere storage profile. Storage profiles can be used to identify type, speed, or cost of storage. You can include multiple storage profiles in a single provider vDC. Also, a single provider vDC can provide resources for multiple organizations.

This chapter discusses the management of the following:

- Provider vDCs
- vCloud Director network resources
- a vCloud Director organization
- Organization vDCs

Managing provider vDCs

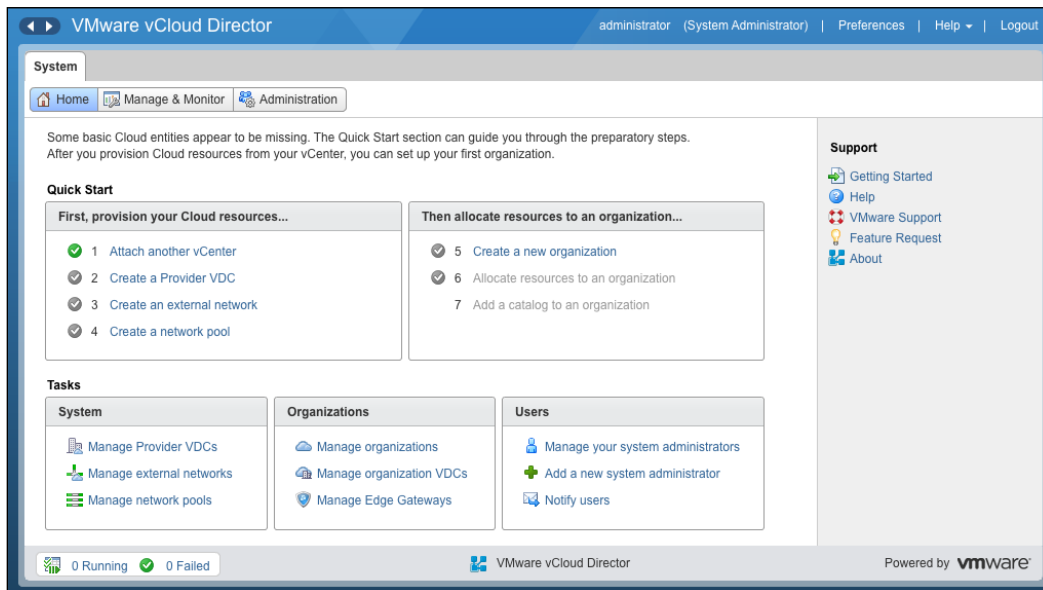
If you design your vCloud Director to have separate purpose into a separate cluster, then you will have vCloud Director resources provided by other clusters. For example, you can segregate clusters by assigning more computing powers or a different set of computing power and storage breed to provide a premium service to a premium customer. Each VMware vCenter Server system can support multiple clusters. However, when you have a separate vCenter Server for different purposes, you might find it simpler to have one vCenter Server system manage only one cluster. While planning the architecture, remember that provider vDCs are based on the resources managed by the vCenter Server. A single provider vDC can encompass more than one vCenter Server system. The following diagram illustrates the abstraction of vSphere resources and mapping of resources to different organizations. However, this diagram does not contain multiple vCenters:



Creating a provider vDC

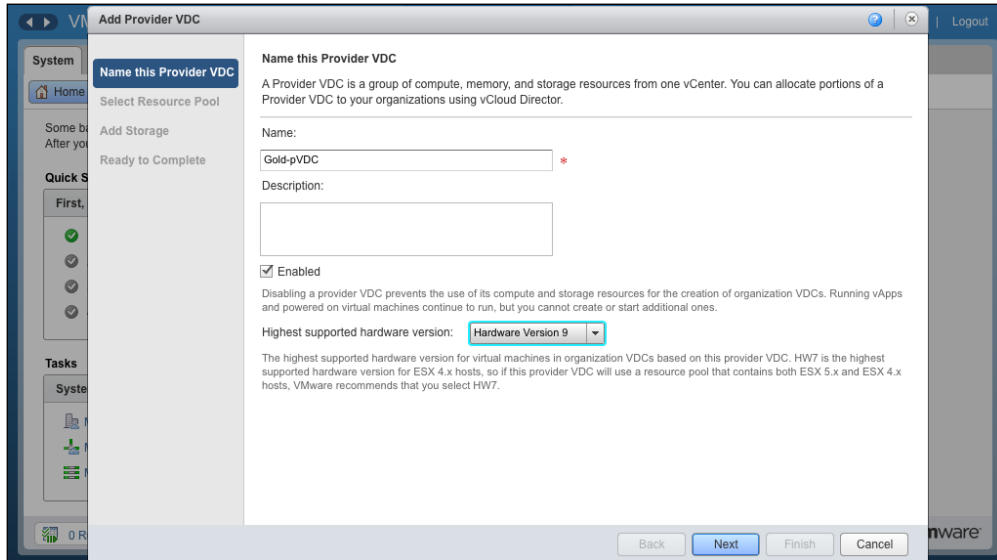
Perform the following steps to create a provider vDC:

1. Start a browser and type in a URL for the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.
3. In the home screen, click on **Create a Provider VDC**, as shown in the following screenshot:

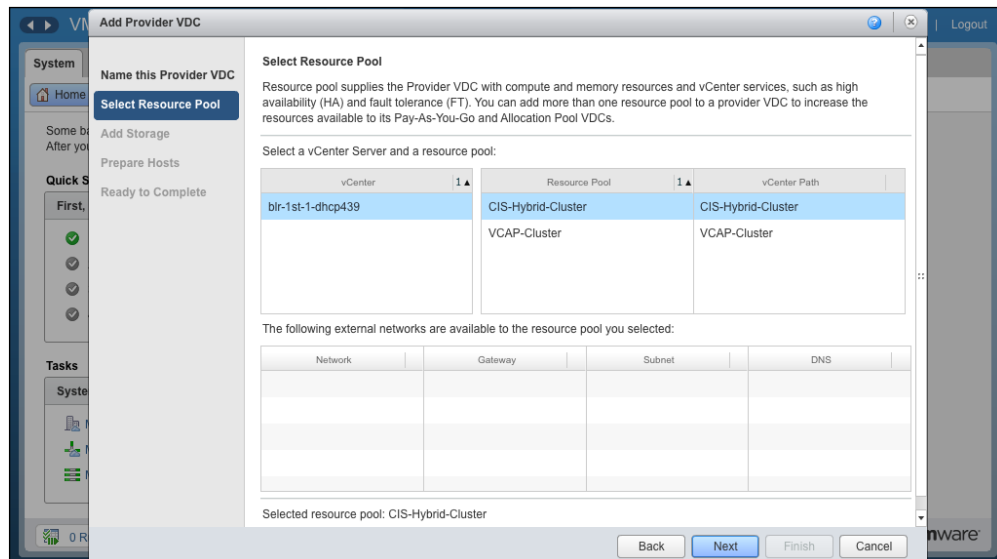


4. Specify a name for the PvDC.
5. Click on the **Enabled** checkbox.

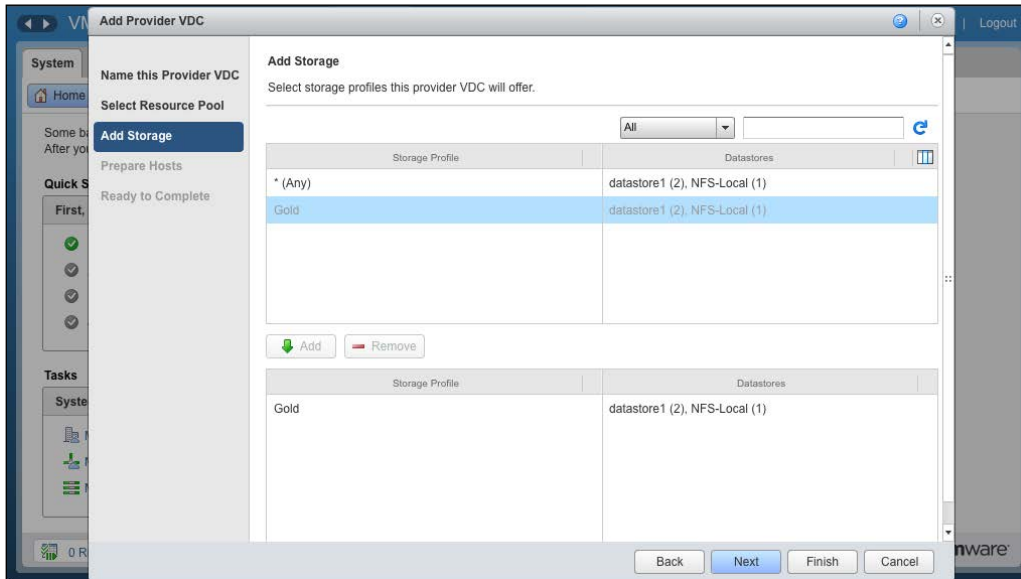
6. Select the highest supported hardware version from the **Highest supported hardware version** drop-down combobox and click on **Next**. This is shown in the following screenshot:



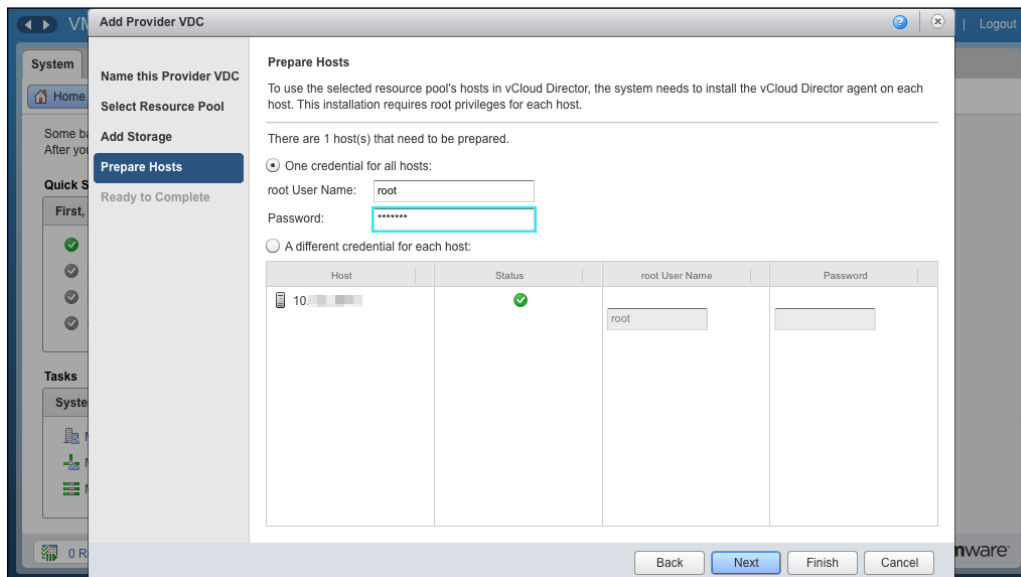
7. Select a vCenter Server.
8. Then, select a resource pool and click on **Next**, as shown in the following screenshot:



9. Select a storage profile and Click on **Add**.
10. Click on **Next**, as shown in the following screenshot:



11. In the **Prepare Hosts** section, specify credentials for the hosts that need preparing.
12. Click on **Next**. This is shown in the following screenshot:





When preparing the hosts for vCloud Director, they switch to the maintenance mode to get the vCD agent VIB installed. So make sure that the ESXi hosts are configured with vMotion. This way, existing VMs that may be registered or running can be evacuated gracefully to other hosts.

13. Finally, review the specified inputs and click on **Finish**.

To expand your provider vDC, merge one or more provider vDCs with an existing one. Once you do so, the combined PvDC will import all the resources from the two provider vDCs. However, a limitation is that only the merged provider remains; all other provider objects are deleted. All dependent objects are also updated. Organization vDCs show as being backed by the merged provider.

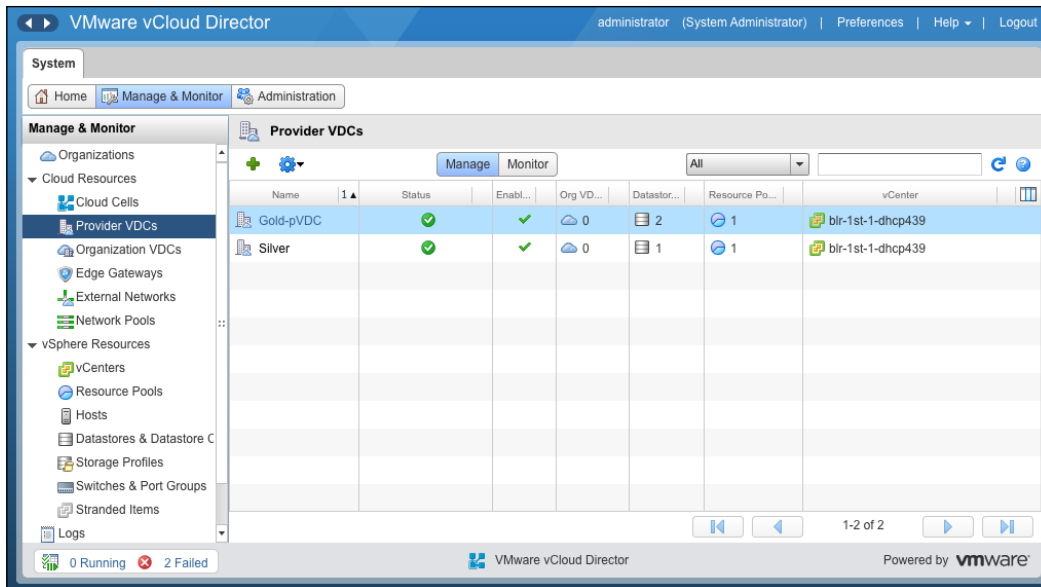
Prior to vCloud Director 5.1, a provider vDC could be supported by no more than one resource pool. Now, however, you can merge existing provider vDCs to create one provider vDC, which is backed by a single or multiple resource pools. When merging, you select one or more provider vDCs as contributors and one provider vDC as the target of the merge.

When you merge two PvDCs, two operations will run in the background. Firstly, the target provider vDC will include networks, network pools, storage profiles, resource pools, and datastores from all the contributor provider vDCs. Secondly, organization vDCs backed by the provider vDCs are now backed by the target.

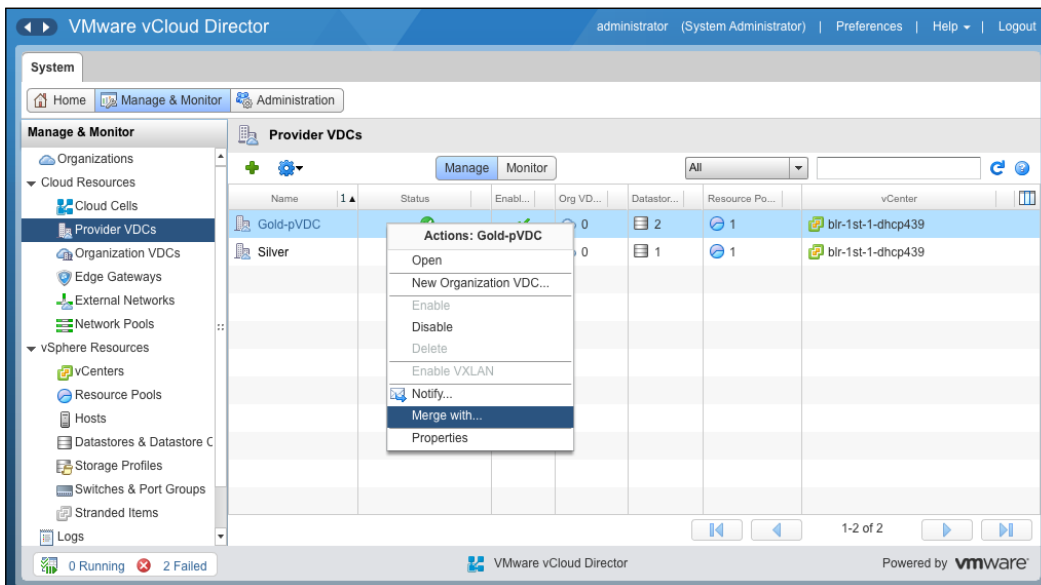
Merging provider vDCs

Let's go through the following steps to merge provider vDCs in vCloud Director:

1. Start a browser and insert the URL of the vCD server; for example, `https://serverFQDN/cloud`.
2. Log in to vCD with an administrator user ID and password.
3. Click on the **Manage & Monitor** tab.
4. Click on **Provider VDCs** in the left panel, as shown in the following screenshot:

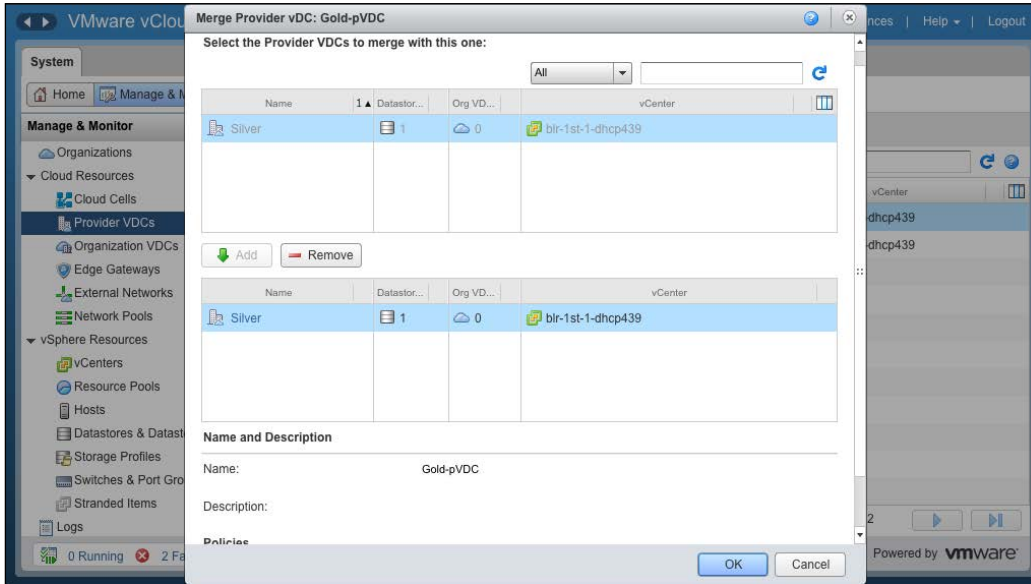


- Right-click on the source PvDC and click on **Merge With...**. This is shown in the following screenshot:



- Select the other provider vDCs to merge with.
- Click on **Add**.

8. Click on **OK**. This is shown in the following screenshot:



So far, we have seen how to manage provider vDCs in vCloud Director. In the next section, we take a look at managing network resources in vCloud Director, which includes creating and managing network pools and provider external networks.

Managing vCloud Director network resources

Network pools are a collection of virtual resources (VLANs, port groups, VXLANs, or isolation-backed networks) that facilitate the virtualization of vApp or organization network virtualization.

Two types of organization vDC networks require network pools. First are the routed organization vDC networks, which connect to an external network through an edge gateway, and second are the isolated organization vDC networks.

All vApp networks are built using resources from network pools. Fencing the vApp requires network resources, although a Direct Connect vApp does not consume network pool resources.

When you assign a network pool to an **organization virtual datacenter (Org vDC)**, specify how much of the resources are dedicated from the pool to the Org vDC.

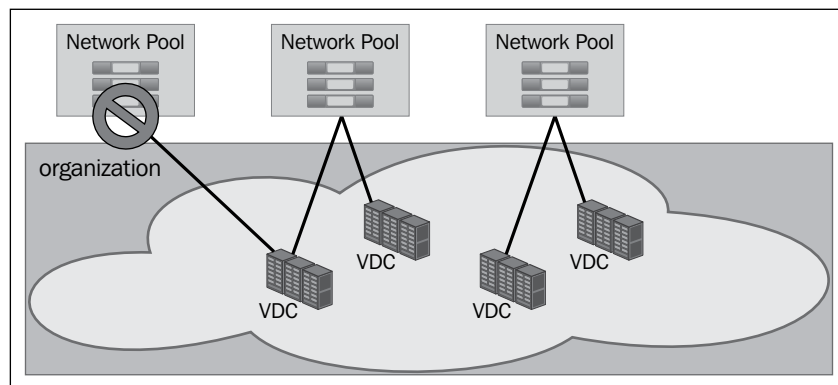
A provider vDC gets its resources from vSphere. CPU and memory are combined into a resource pool, and storage is configured into datastores and then into storage profiles. All of these resources are used by vCloud Director to create a provider vDC. Networks are not included in resource pools or datastores. When you create a provider vDC, vCloud Director analyzes the underlying ESXi hosts and clusters that the resources come from. Based on that analysis, vCloud Director reports the external networks available to organizations and vApps are built on a provider vDC.

Organizations and vApps get their resources from an organization vDC, which is built on the provider vDC. When creating an organization vDC, vCloud Director enables you to directly associate it with a network pool. The network pools are built on vSphere port groups, virtual switches, VLANs, and vCloud Director isolated networks.

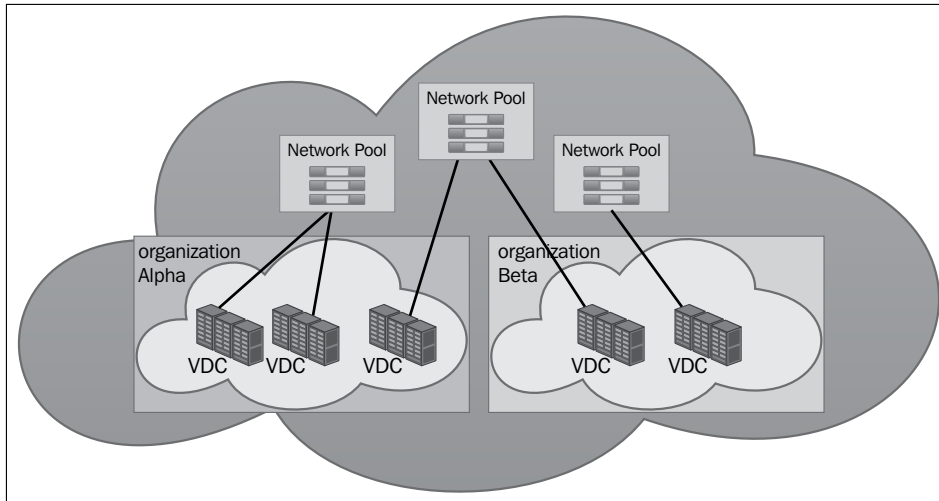
Provider external networks are available to a provider vDC and network pools are directly associated with specific organization vDCs.

Network pools

Each network pool must be backed by a network resource in vSphere. The network resource should be in the vSphere cluster, on which the PvDC is built. Network resources include VLANs, preexisting port groups, and vCloud Director isolated networks. This is shown in the following diagram:



Organization vDCs from different organizations can connect to the same network pool, enabling private enterprise clouds to create one or two network pools that serve an entire company. Using network pools between multiple organizations enables public clouds to create fewer network pools because each cloud tenant does not need their own pool. However, you can overcommit your network pools, as shown in the following diagram:



Each network pool should be backed by a network resource.

The following four types of network pools are possible:

- VLAN-backed network pools
- Network pools backed by vCloud Director network isolation
- Port group-backed network pools
- VXLAN-backed network pools

VLAN-backed network pools

For a VLAN type of network pool, you must specify a VLAN ID range or a group of VLAN IDs. When you specify VLAN ID ranges, do not overlap existing VLANs either in vCenter Server or in attached physical switches.

Caution must be exercised when configuring physical switches. Defining VLANs configured on the ESXi host and ensuring that they are allowed by the switch trunk port are essential tasks when placing a port in trunk mode. The default behavior varies by type of switch and between vendors. You might need to explicitly define all the VLANs used with ESXi on the physical switch.

For each VLAN, specify the VLAN ID, name, type, **maximum transmission unit (MTU)**, **security association identifier (SAID)**, state, ring number, bridge identification number, and so on.

No further steps are required for switches that allow all ports by default. The practice for VMware is to restrict the VLAN ranges to only the required VLAN IDs.

vCDNI-backed network pools

The second type of network pool is one backed by vCloud Director's isolated network. The isolated network is driven by the VSLAD agent that runs on the ESXi hosts in the vSphere cluster. The VSLAD agent is part of the software in the VSLA kernel module.

These networks isolate network traffic. If a packet needs to leave the port group on one ESXi host to move to a different ESXi host, it is tunneled through the VMkernel module. This tunneling uses MAC-in-MAC encapsulation, which puts the isolated network's header in place and sends the packet out to the physical layer. A vCloud Director isolated network adds 24 bytes to the length of the packet. So, when you create a vCDNI pool, change the pool settings and increase the **maximum transmission unit (MTU)** to 1524 at least to accommodate the additional overhead.

Think of the vCloud Director isolated network as a software-based isolated network between two or more ESXi hosts, which uses special packets at layer 2 of the network model (Ethernet layer). The packets are decoded in the VMkernel. Network traffic is isolated at layer 2. The vCloud Director isolated network is used to connect traffic on multiple ESXi hosts.

Creating a network pool backed by the vCloud Director isolated network does not change anything on the vSphere layer. The vShield Edge device is not deployed and no new port groups appear. When the vApp that connects to a network is powered on, the vShield Edge device is deployed and the port group is created.

Port group-backed network pools

The final type is a network pool backed by vSphere port groups. The port groups on virtual switches or distributed virtual switches must be created in advance by the VMware vCenter administrator. These port groups must have VLAN IDs configured to meet the requirements of vCloud security. The network pool based on port groups is the least flexible type. However, this type of network pool backing gives the vCloud administrator total control over the configuration.

You can override the VLAN configuration requirement; however, VMware does not recommend it.

VXLAN-backed network pools

VXLAN is a new type of LAN connection designed to replace the vCloud Director isolated networks. If you have virtual machines running on two different clusters that have different VLAN IDs, these virtual machines cannot communicate with each other unless you set up a router between the clusters.

VXLANs enable you to connect two clusters with a VXLAN wire. The VXLAN wire is a logical connection between the two clusters. Each end of the wire must be anchored with a **VXLAN Tunnel End Point (VTEP)**.

VXLAN is a routable protocol that does not require special configuration within a router. Because VXLAN is an encapsulation protocol, VLANs are not needed to isolate traffic. Each VXLAN wire is isolated.

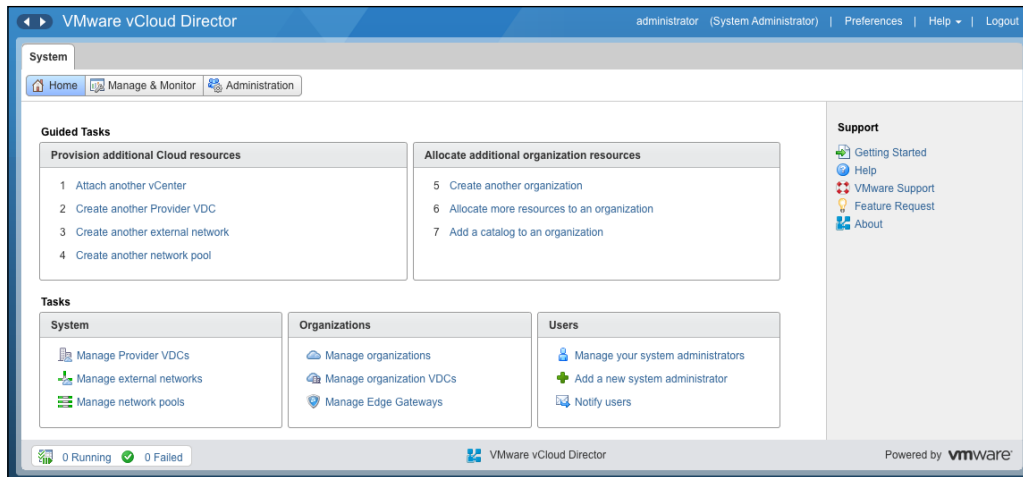
VXLAN is not an encrypted protocol. Traffic is isolated, but it is not secured by encryption.

vCloud Director automatically sets up a network pool backed by a VXLAN pool. The pool is named after the provider vDC. Each provider vDC gets a unique VXLAN pool. Even though a VXLAN pool is available, you are not required to use it. Other types of network pools can still be used with each provider vDC.

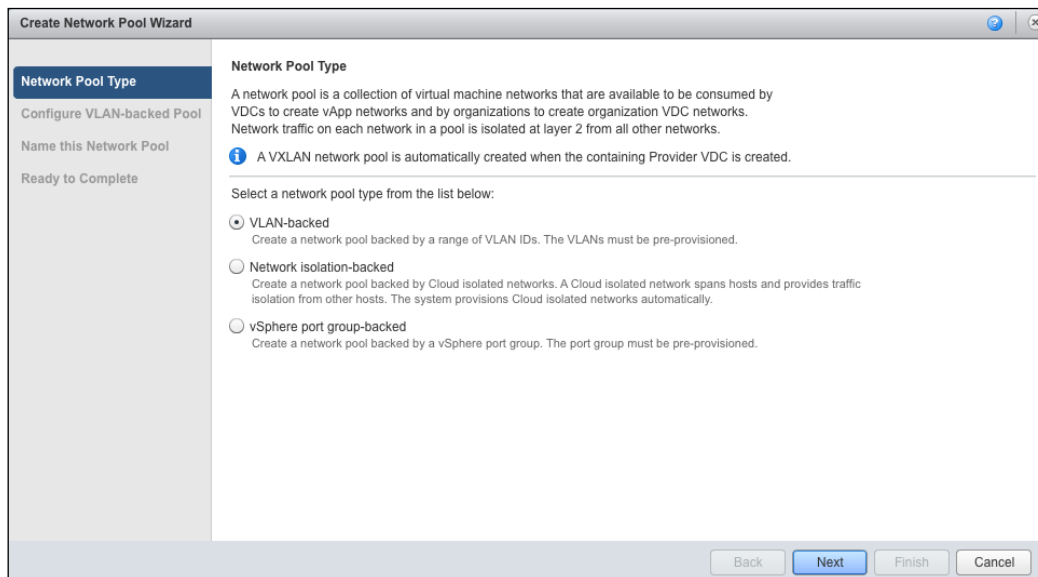
Creating VLAN-backed network pools

Perform the following steps to create a VLAN-backed network pool in vCloud Director:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by using an administrator user ID and password.
3. Click on the **Home** tab.
4. Click on **4 Create another network pool**, as shown in the following screenshot:

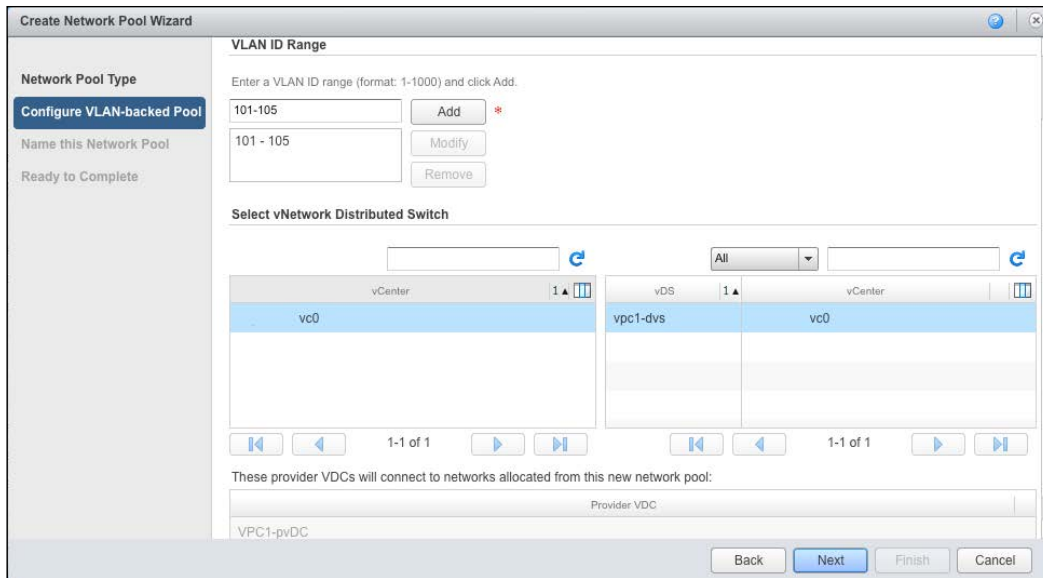


5. In the **Create Network Pool Wizard** window, leave **VLAN-backed** selected and click on **Next**. This is shown in the following diagram:



6. Under the **Configure VLAN-backed Pool** tab, in the **VLAN ID Range** textbox, type the VLAN range want to use. In this example, we use 101-105. Now, click on **Add**.

7. From the **vCenter** list, select the vCenter Server. In the **vDS** list, select your configured vDS.



8. Click on **Next**.
9. Under the **Name this Network Pool** tab, specify a name in the **Name** field.
10. Type a description and click on **Next**. This step is optional.
11. Under **Ready to Complete**, click on **Finish**.

Provider external networks

External networks are logical, differentiated networks based on vSphere port groups. These include distributed switch port groups, standard switch port groups, and Cisco N1000V port groups. Each port group can become a single external network. The best practice is to use port groups on distributed switches. A single distributed switch can have several port groups in it. Each port group can provide a connection point for a different external network. If you plan to create multiple external networks, the port groups should be separated by VLANs. The port groups must be created in vCenter Server and should already exist before vCloud Director can use them for external networks.

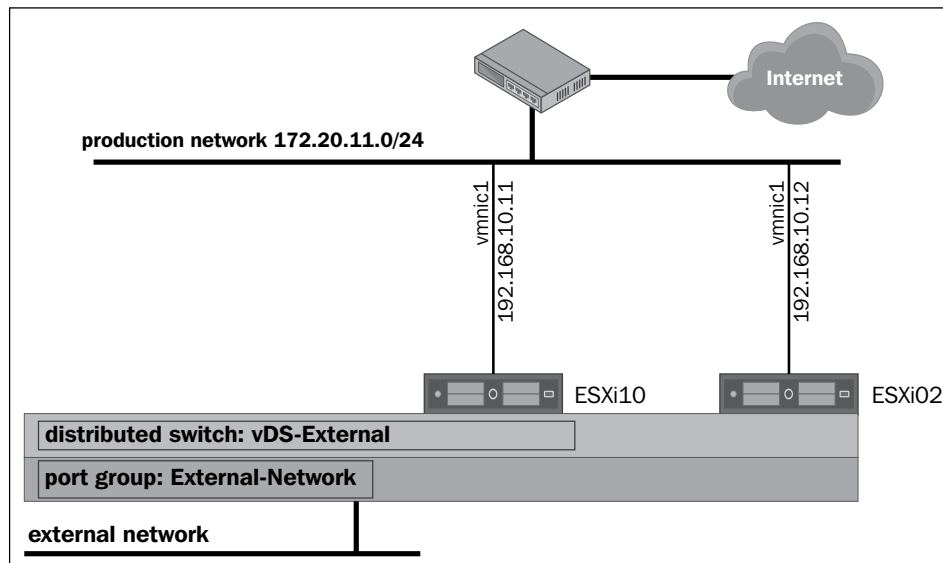
Even though this network is called an external network, a connection to the Internet is not required. An external network is external to vCloud organizations. You can create an external network to connect multiple ESXi hosts to other internal corporate resources without a route to the Internet.

If you wish to provide vApps in the cloud with access to the Internet, create an external network that is connected through a gateway router to the Internet.

All port groups in a VMware cluster are not to be used for external networks. Many of those networks are for purposes outside of vCloud Director. An example of a network that is not used directly by vCloud Director is a network that provides IP storage to ESXi hosts. Another example is a management network used for the internal administration of ESXi hosts and vCenter Server systems.

External networks can also be used to connect organizations either through a common network that both organizations' edge gateways connect to or an upstream router.

Visualizing how external networks at the provider level are built off vSphere networks is important. The following diagram illustrates how an external network, a provider-level external network, is built from a port group named **External-Network**:



The **External-Network** port group is located in the **vDS-External** distributed switch. The **ESXi01** and **ESXi02** hosts are connected to the vDC production distributed switch.

The physical NICs on **ESXi01** and **ESXi02** are both labeled as **vmnic1** on the two hosts. The **vmnic1** NIC on **ESXi01** has been assigned the IP address of **192.168.10.11**. The **vmnic1** NIC on **ESXi02** has been assigned the IP address of **192.168.10.12**. Both of these physical NICs are connected to a physical network known as the production network. The production network has been assigned a **Classless Inter-Domain Routing (CIDR)** network of **192.168.10.0/24**.

External networks connect to port groups that have been defined on vSphere virtual switches. If you plan to use a vSphere port group for a vCloud external network, increase the number of ports from the default value, that is, from 128 to 4096.

The best practice is to use only distributed switches. Distributed switches are automatically consistent in names and port groups on all ESXi hosts in a cluster. vCloud Director can use them with dynamic provisioning.

vCloud Director supports the Cisco Nexus 1000 v. However, this software switch does not work with VLAN or vCDNI-backed network pools. This software switch requires network pools that are backed by port groups or use VXLAN. The port groups must be pre-provisioned in the nexus 1000 v.

The best practice is to use distributed switches with all network pools.

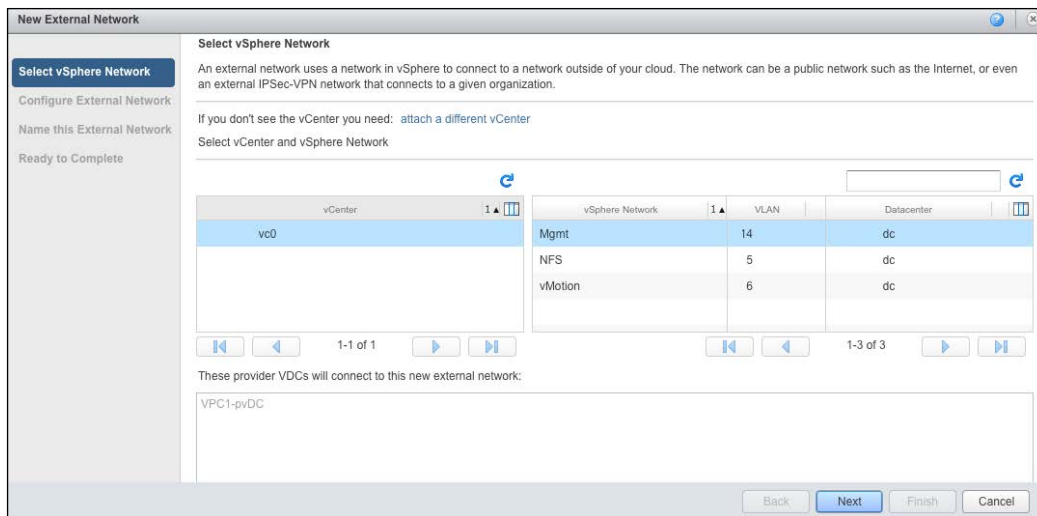
A standard switch can be used with vCloud Director external networks; however, they are not recommended. When using standard switches, all the port groups have to be created accordingly on all the ESXi hosts in advance.

You can use standard switches with network pools that are backed by port groups, but this also is not recommended.

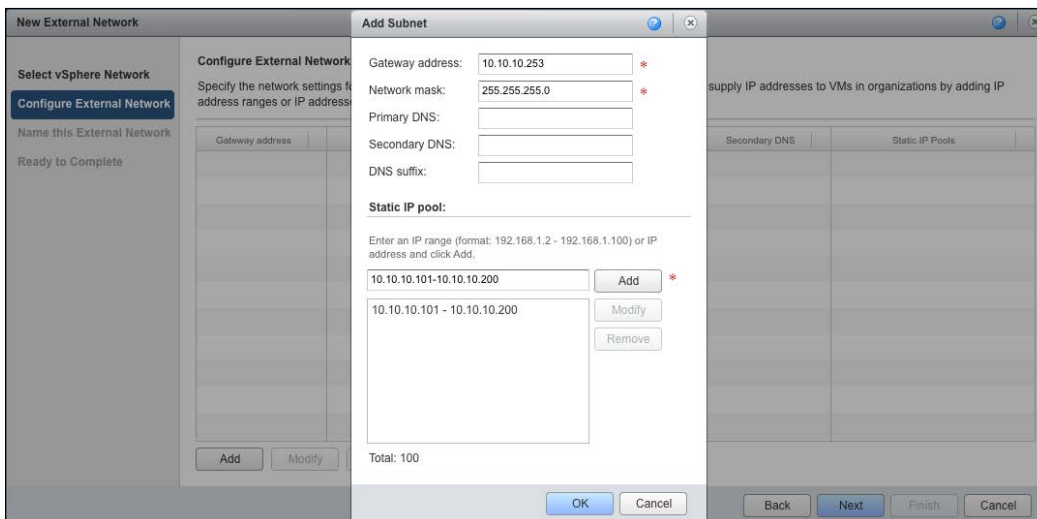
Creating a provider external network

Let's go through the following steps to create an external network in vCloud Director:

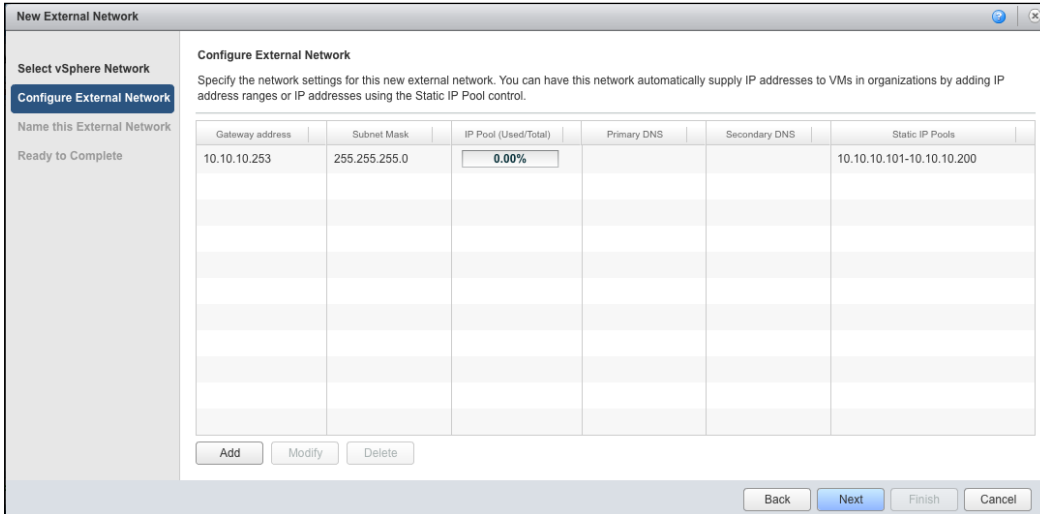
1. Start a browser. Insert the URL of the vCD server in the browser, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Home** tab.
4. Click on **3 Create another external network**.
5. Select vCenter Server and from the right-hand side select which vSphere port group will carry the external network, and click on **Next**. This is shown in the following screenshot:



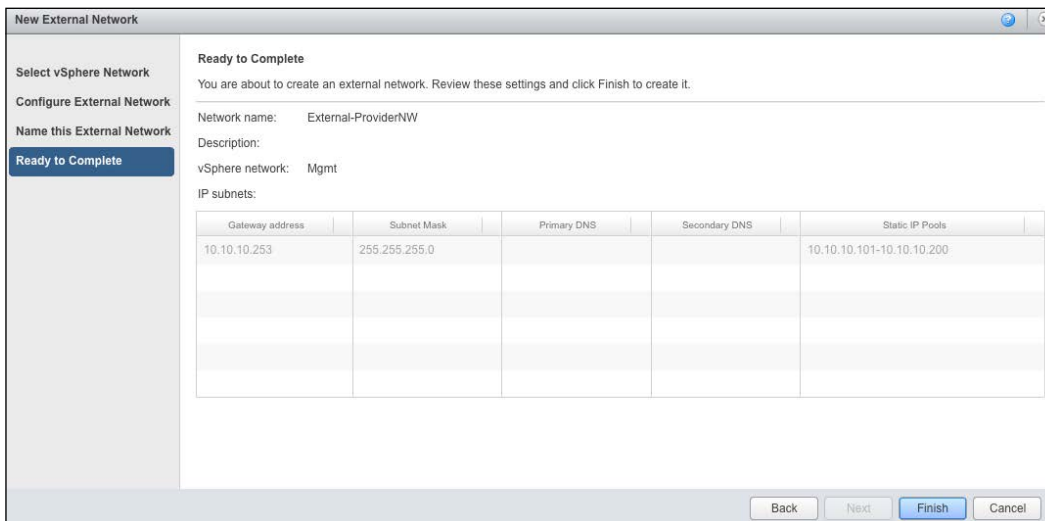
6. In the **Configure External Network** page, click on **Add**.
7. Specify the values for **Gateway address** and **Network mask**.
8. In the **Static IP pool** section, specify the IP address range you want to use and click on **Add**. This is shown in the following screenshot:



- Click on **OK**. The final output will look similar to what is shown in the following screenshot:



- Click on **Next**.
- Click on the **Name this External Network** tab and type a name in the **Network name** field. Again, click on **Next**.
- Review the final information and click on **Finish**, as shown in the following screenshot:



In the previous section, we discussed how to manage network resources in vCloud Director. We learned about the various network pools and external networks.

In the next section, we will discuss about organization and organization vDCs.

Managing a vCloud Director organization

An organization is a logical group of users to which IT services are presented. Organizations provide a security boundary so that appropriate resources and controls can be set up for a given group of users.

Each organization has a unique login URL. Users that are locally created or imported from a **Lightweight Directory Access Protocol (LDAP)** server can operate only in that organization. LDAP settings in each organization are independent from other organizations.

The vCloud Director system administrator creates the organization and provisions resources. After the organization is created, the system administrator distributes the organization URL to the administrator assigned to the organization (called the organization administrator). Using the URL, the organization administrator logs in to the organization portal and sets it up, configures resource use, adds users, and selects organization-specific policies and settings. Organization member users (consumers) can then create, use, and manage IT services packaged as vApps.

When you select the name of the organization, do not worry about the name being visible to other organizations. Multi-tenancy means that users must know the name of their organization before they can provision resources or services. A user in one organization cannot learn the names of other organizations through the vCloud Director user interface. Plan to create an organization for each tenant of the cloud. Only the vCloud Director administrator can create an organization.

The organization name is used in a URL whenever a user navigates to the organization's portal. As a result, the organization name must be suitable as part of a URL. Do not use spaces or special characters in an organization name. Underlines and hyphens are permitted. Because the name is part of a URL, the best practice is to make the name as short as possible.

Each organization has its own organizational policies; these are leases, quotas, and limits.

For instance, to consume storage and processing resources, leases, quotas, and limits hold back the organization users. Predominantly, these settings prevent users from utilizing an organization's resources to the fullest. These settings are described as follows:

- **The lease setting:** This setting equips you with a level of control over the allocated storage and compute resources of an organization. This is done by specifying the maximum amount of time for vApp to run and consume compute resources and vApps and vApp to store templates. The following are the types of lease settings:
 - **The runtime lease setting:** This is applied to prevent inactive vApps, particularly, from consuming compute resources. For example, if a user starts a vApp and does not use or stop it, then vApp continues to consume resources. With a specified runtime lease, when the lease expires, vCloud Director stops the vApp.
 - **The storage lease setting:** This does not allow unused vApps and vApp templates to consume storage resources. The storage lease for vApp initiates once a user stops vApp. However, storage lease does not have an effect on running vApps. If a storage lease expires, vApp or the vApp template is marked as expired by vCloud Director depending on the organizational policy selected.
- **The quota setting:** If you want to set a cap on the number of virtual machines for an organization's user to store and power on in the organization vDCs, then quota is key. An administrator can set a default quota for all new users and these users will inherit that quota by default.
- **The limit setting:** This can help you defend **denial-of-service (DoS)** attacks. Certain vCloud Director operations are more resource intensive than others. An example of such an operation is the copying or moving of vApp. For performance or security reasons, you can also limit the number of simultaneous connections to a virtual machine from the vCloud Director remote console. Limiting the number of simultaneous connections does not limit Virtual Network Computing or Remote Desktop Protocol connections. Unlike other usage policies, limits must be set by system administrators and cannot be set or modified by organization administrators.

Creating a vCloud Director organization

Let's go through the following steps to create an organization in vCloud Director:

1. Start a browser. Insert the URL of the vCD server into the browser, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by using an administrator user ID and password.
3. Click on the **Home** tab.
4. Click on **5 Create another organization**.
5. Specify the organization's name in the **Organization name** field and the organization's full name in the **Organization full name** field, then click on **Next**, as shown in the following screenshot:

New Organization

Name this Organization

An Organization is the fundamental VCD grouping. An Organization contains users, the vApps they create and the resources the vApps use. An organization can be a department in your own company or an external customer you're providing Cloud resources to.

Organization name:
 *

The unique identifier in the full URL with which users log in to this organization. You can only use alphanumeric characters.

Default organization URL:
<https://d1p300v1-vcd-vip.vchslabs.vmware.com:443/cloud/org/vCloud-Essential/>

Organization full name:
 *

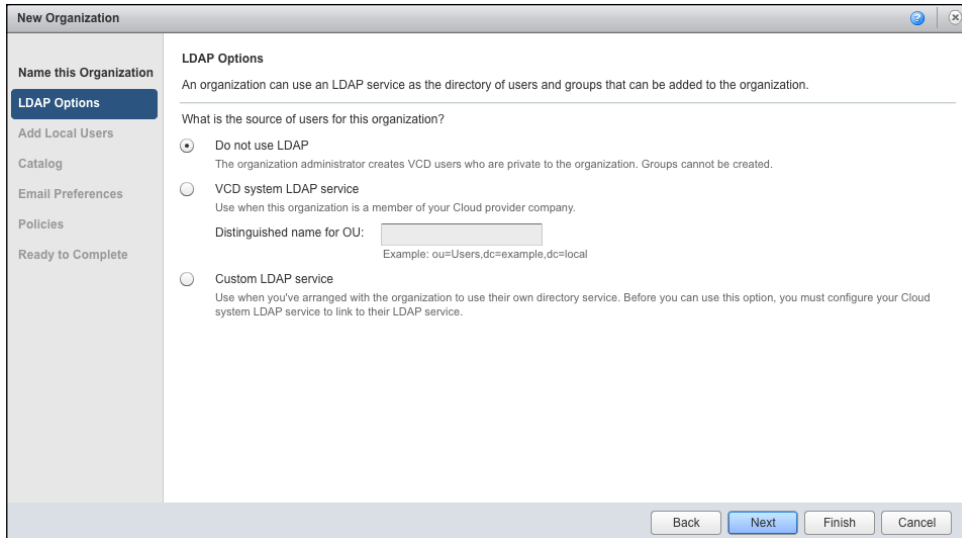
Appears in the Cloud application header when users log in. An organization administrator can change this full name.

Description:

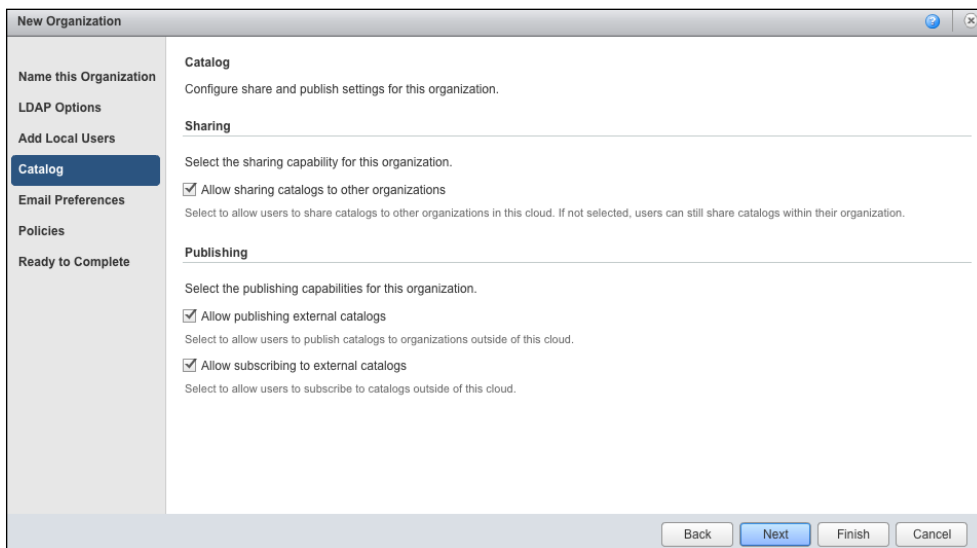
An organization administrator can change this description.

Back Next Finish Cancel

- Under the **LDAP Options** tab, leave **Do not use LDAP** selected and click on **Next**, as shown in the following screenshot:



- Under the **Add Local Users** tab, click on **Next**.
- Under the **Sharing** tab, select **Allow sharing catalogs to other organizations**.
- Under the **Publishing** tab, select **Allow publishing external catalogs** and **Allow subscription to external catalog feeds** and click on **Next**, as shown in the following screenshot:



10. Under the **Email Preferences** tab, click on **Next**.
11. Under the **Policies** tab, select the defaults shown in the following screenshot:

The screenshot shows the 'New Organization' wizard in the 'Policies' tab. The 'Leases' section is active, with the following settings:

- vApp leases:**
 - Maximum runtime lease: 7 Days *
 - Maximum storage lease: 30 Days *
 - Storage cleanup: Move to Expired Items
- vApp template lease:**
 - Maximum storage lease: 90 Days *
 - Storage cleanup: Move to Expired Items

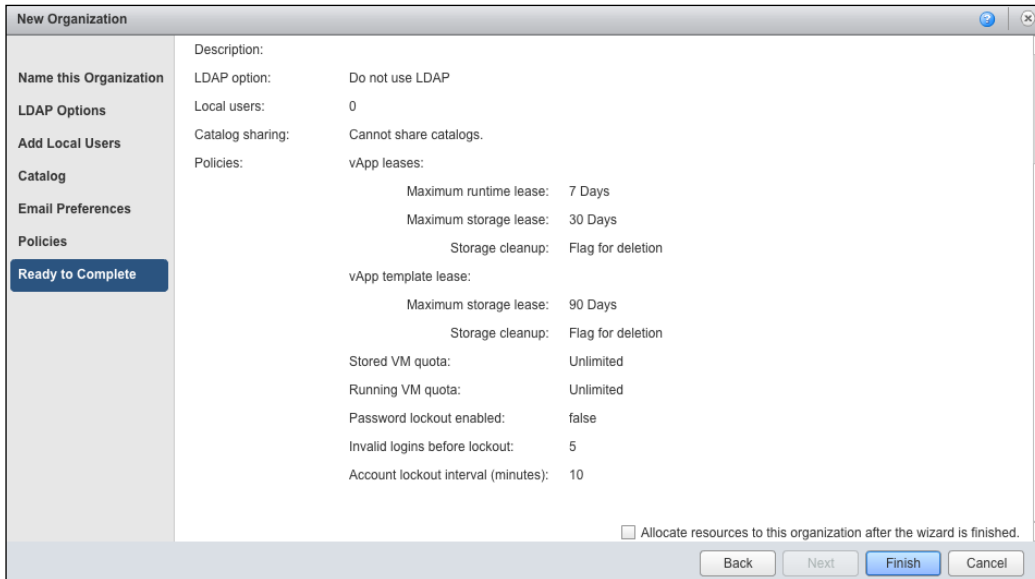
The 'Default Quotas' section is also visible, with the following settings:

- All VMs quota: 1 (radio button selected) / Unlimited
- Running VMs quota: 1 (radio button selected) / Unlimited

At the bottom of the wizard, there are four buttons: Back, Next (highlighted in blue), Finish, and Cancel.

12. Do not change any of the options under **Default Quotas**. Now, click on **Next**.

13. Under the **Ready to Complete** tab, click on **Finish**. This is shown in the following screenshot:



Managing organization vDCs

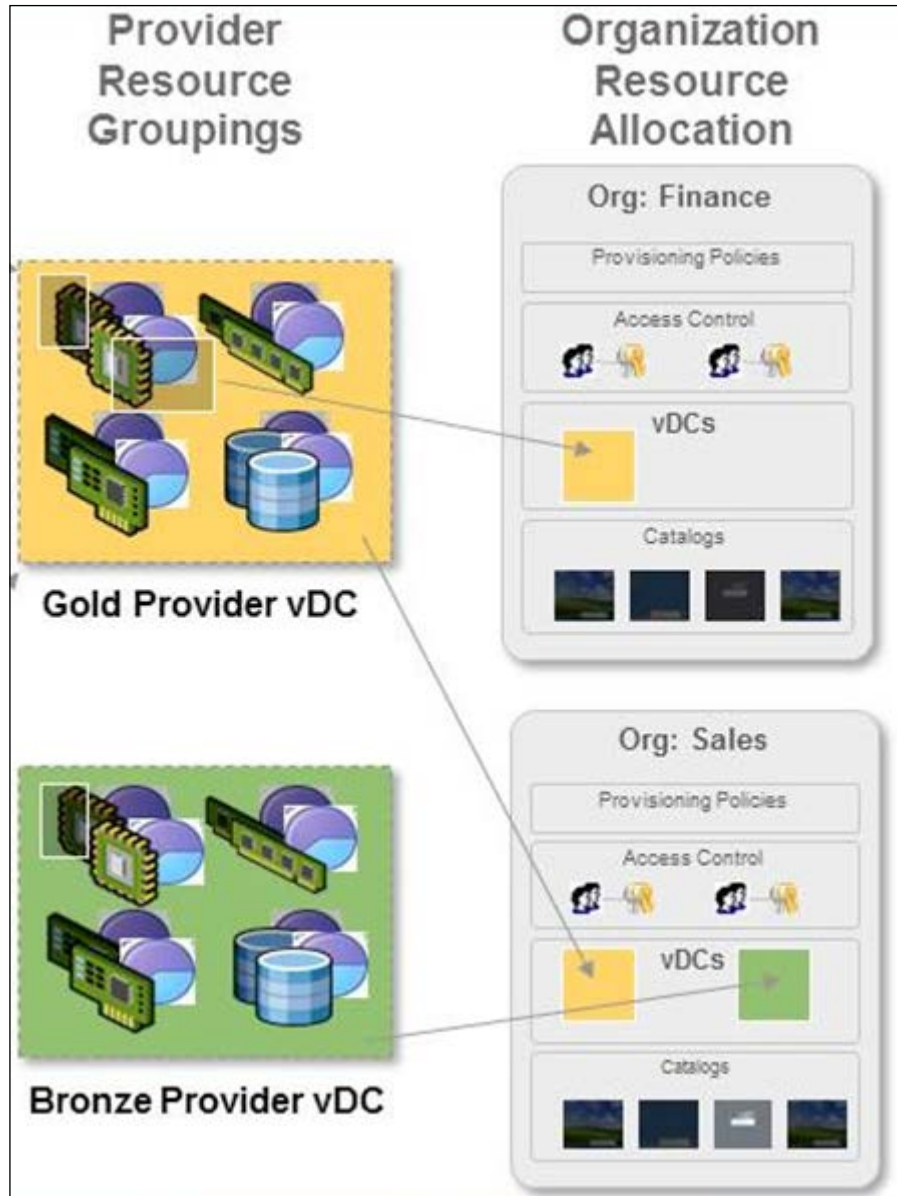
An organization vDC provides resources to an organization and differs from a provider vDC. Organization vDCs provide an environment that allows you to store, deploy, and operate virtual systems. Storage is also provided for virtual media such as floppy disks and CDs.

A single organization can have multiple organization vDCs associated with it. They are used by vCloud Director to divide provider vDCs and allocate resources to an organization. vCloud Director uses resource pools as the basic construct to partition these resources.

It is imperative that you create the organization prior to creating an organization vDC. Each organization can have multiple organization vDCs. But each organization vDC is local to only one organization.

When creating an organization vDC, first select the provider vDC that provides resources. From a vSphere perspective, both provider and organization vDCs are resource pools and have a parent-child relationship.

The organization vDC enables the cloud provider to share provider vDC resources with multiple tenants. Organization vDCs maintain security, enable the provider to set predefined allocations, and ensure that the tenant's performance and capacity requirements can be controlled. This is depicted in the following diagram:



Tenants do not have the ability to see the actual resources in the provider vDC. Their visibility is only into resources that are available in the organization vDC.

Similar to a provider vDC, the organization vDC is a container for resources; however, the manner of allocating resources can be specified. A network pool can be added to an organization vDC with a limited number of networks that can be created. You can also specify the maximum amount of storage that the organization vDC can consume.

You must create your provider vDCs before you create your organization vDCs. Each organization can have multiple organization vDCs. Each organization vDC can be connected to only one provider vDC. However, each provider vDC can serve resources to multiple organization vDCs.

Organization vDC allocation model

When creating an organization vDC, choosing an appropriate allocation model is important. The allocation model determines not only the commitment of provider vDC resources toward organization vDCs, but also how the provider bills the customer for those resources.

You can choose from the following three models:

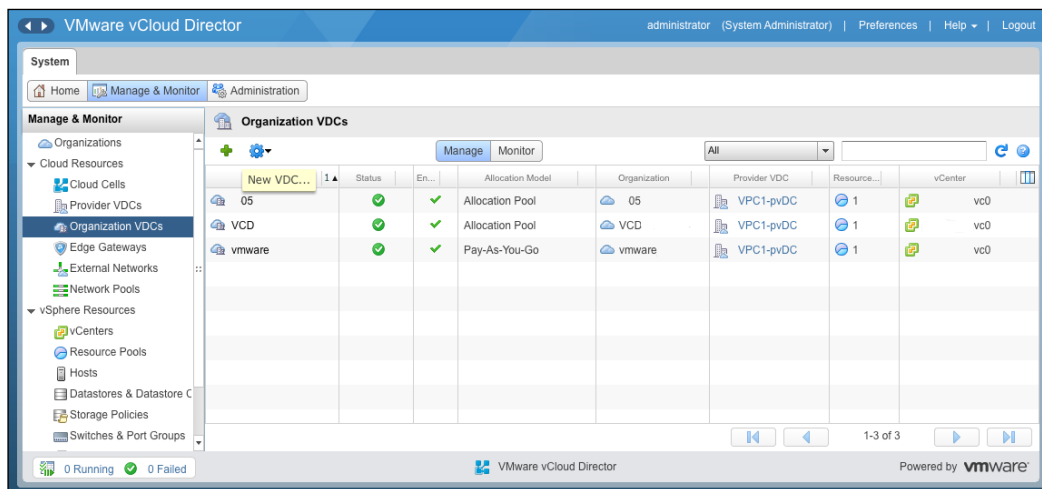
- **The pay-as-you-go model:** This is the easiest model to understand and administer. The simplest way to think of pay-as-you-go is paying for what you get. When vApp powers on, the resources are committed. If vApp is not powered on, then the customer is not billed for resources. Even though the customer is billed as soon as vApp is powered on, only a percentage of the resources are guaranteed. If you want to create a high-tier service offering, the pay-as-you-go model allows the provider to increase the guaranteed resources. The pay-as-you-go model is the only model in which you can specify the speed of virtual CPUs in vApp.
- **The allocation pool model:** This configures a virtual container of resources. The allocation pool model allocates a subset of resources, but it guarantees to a tenant only a percentage of what has been allocated. Thus, the provider has the ability to overcommit resources.

- **The reservation pool model:** This configures a physical container of resources. Think of it as a model in which the customer rents hardware for their exclusive use. The reservation pool model should be the most expensive allocation model offered to customers. The customer is in complete control of the resources that they use, and all resources are guaranteed. The model also offers customers the greatest amount of control. They have the same controls that a vSphere administrator would have over resource pool settings. Thus, over commitment is possible, but it is controlled by the customer.

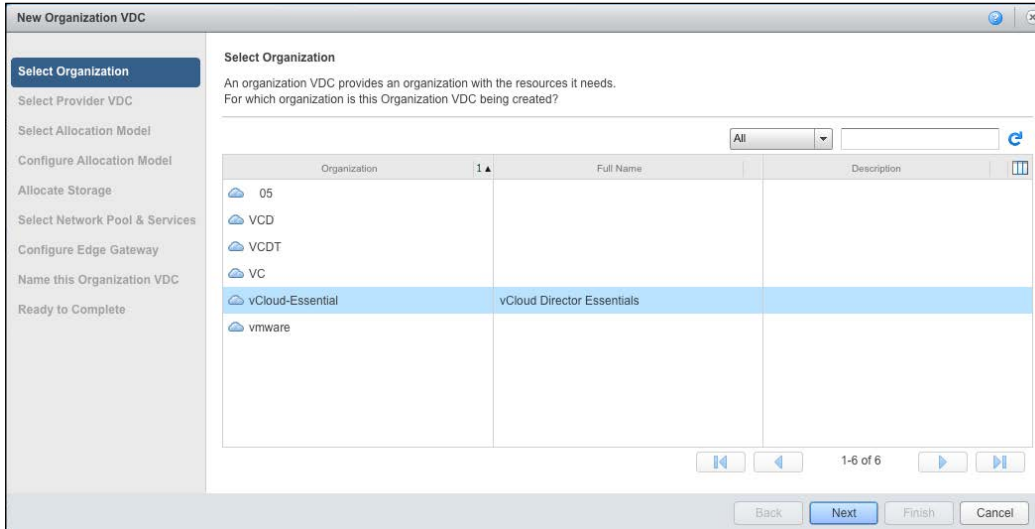
Creating organization vDCs

The following steps create an organization virtual datacenter in vCloud Director:

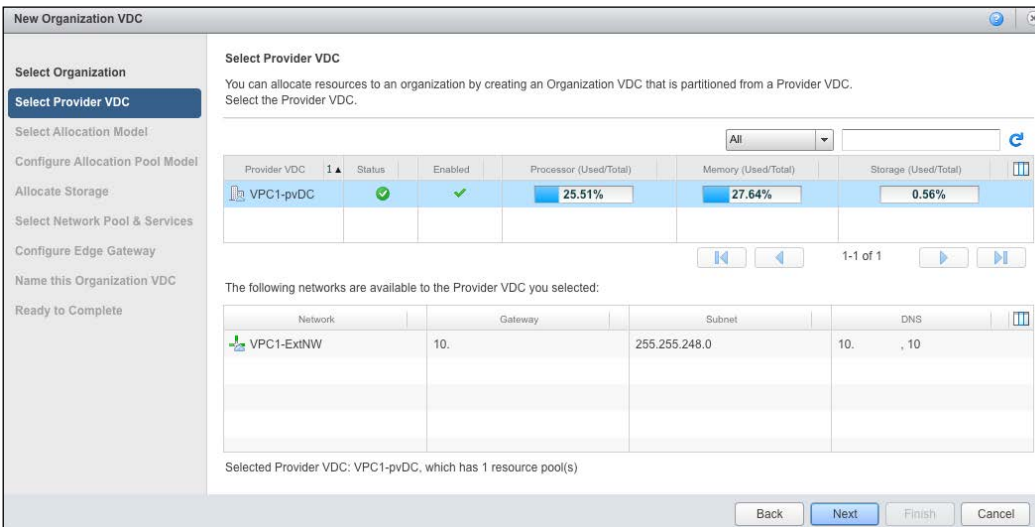
1. Start a browser and insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab.
4. Click on the **Organization VDCs** link in panel on the left-hand side.
5. Click on the + sign to create an Org vDC, as shown in the following screenshot:



- Select the organization that it should belong to and click on **Next**, as shown in the following screenshot:



- Under **Select Provider VDC**, select your already configured provider vDC and click on **Next**. The percentage of available resources for each provider is displayed. External networks, available to each provider vDC, appear after a provider vDC is selected, as shown in the following screenshot:



8. On the **Select Allocation Model** page, select **Allocation Pool** and click on **Next**, as shown in the following screenshot:

New Organization VDC

Select Allocation Model

The Organization VDC's allocation model allows you to control the quality of the service you're providing and the cost of providing these resources.

- Allocation Pool**
Only a percentage of the resources you allocate are committed to the organization VDC. The system administrator controls overcommitment of capacity on the following pages. When backed by a provider VDC that has multiple resource pools, compute resources are Elastic.
- Pay-As-You-Go**
Resources are committed only when vApps are created in the organization VDC. The system administrator controls overcommitment of capacity on the following pages. When backed by a provider VDC that has multiple resource pools, compute resources are Elastic.
- Reservation Pool**
All of the resources you allocate are committed to the organization VDC. Users can control the overcommitment of capacity at any time.

Back Next Finish Cancel

9. On the **Configure Allocation Model Pool** page, select your preferred values in the **CPU allocation**, **CPU resources guaranteed**, **vCPU speed**, **Memory allocation**, **Memory resources guaranteed**, and **Maximum number of VMs** fields. Now, click on **Next**, as shown in the following screenshot:

New Organization VDC

Configure Allocation Model Pool

CPU allocation: 18.71 GHz
The maximum amount of CPU available to the virtual machines running within this organization VDC (taken from the supporting provider VDC, VPC1-pvDC).

CPU resources guaranteed: 50 % (9.36GHz, 10% of available Provider VDC capacity of 93.54GHz)
The percentage of the resources guaranteed to be available to virtual machines running within it.

vCPU speed: 1 GHz
This value defines what a virtual machine with one vCPU will consume at maximum when running within this organization VDC. A virtual machine with two vCPUs would consume a maximum of twice this value.

Memory allocation: 70.26 GB
The maximum amount of memory available to the virtual machines running within this organization VDC (taken from the supporting provider VDC, VPC1-pvDC).

Memory resources guaranteed: 50 % (35.13GB, 10% of available Provider VDC capacity of 351.29GB)
The percentage of the resources guaranteed to be available to virtual machines running within it.

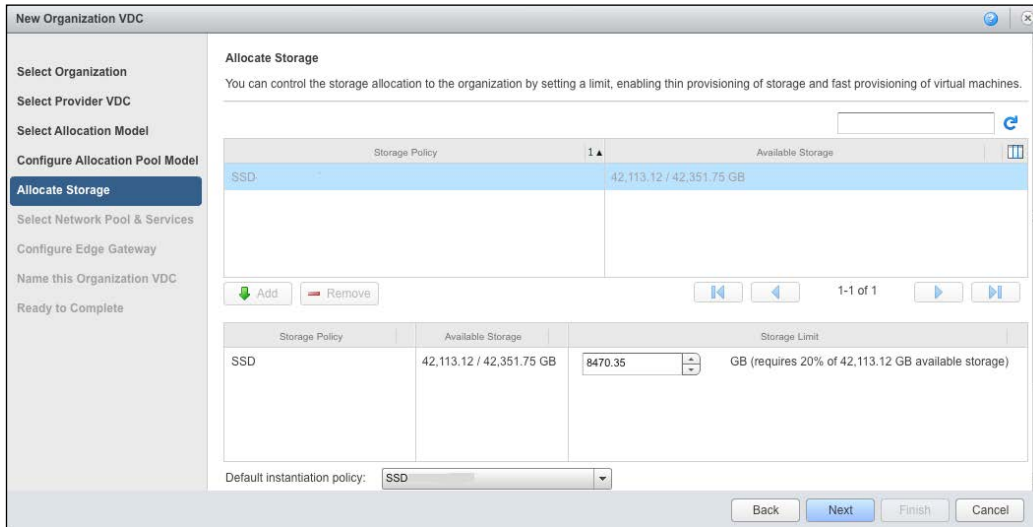
Maximum number of VMs: 100 Unlimited
A safeguard that allows you to control the maximum number of virtual machines in this organization VDC.

The committed resources from Provider VDC, 'VPC1-pvDC' using these allocation settings:

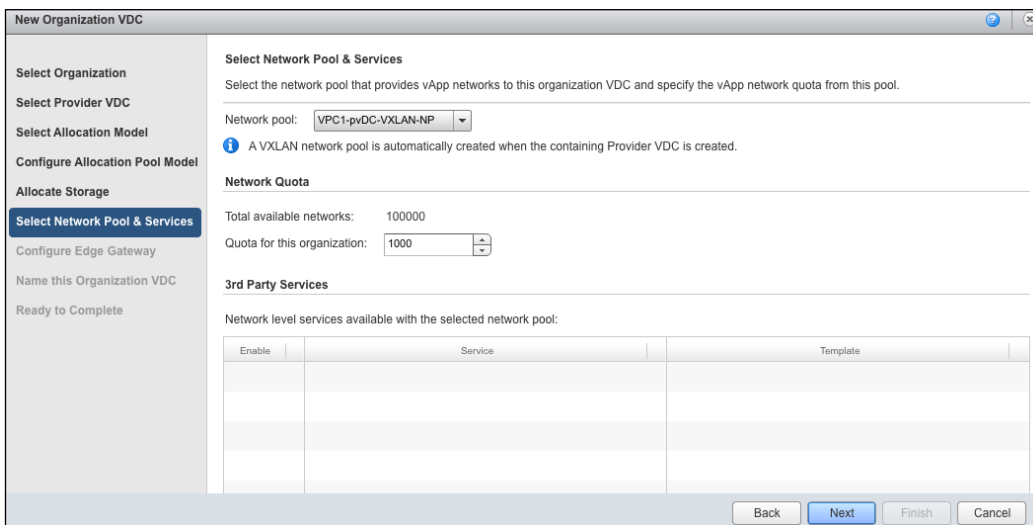
Metric	Total	Allocation	Reservation Committed	Reservation Used
CPU	125.58 GHz	128.71GHz (102.50%)	64.36GHz (51.25%)	32.04GHz (25.51%)
Memory	485.46 GB	490.26GB (100.99%)	455.13GB (93.75%)	134.17GB (27.64%)

Back Next Finish Cancel

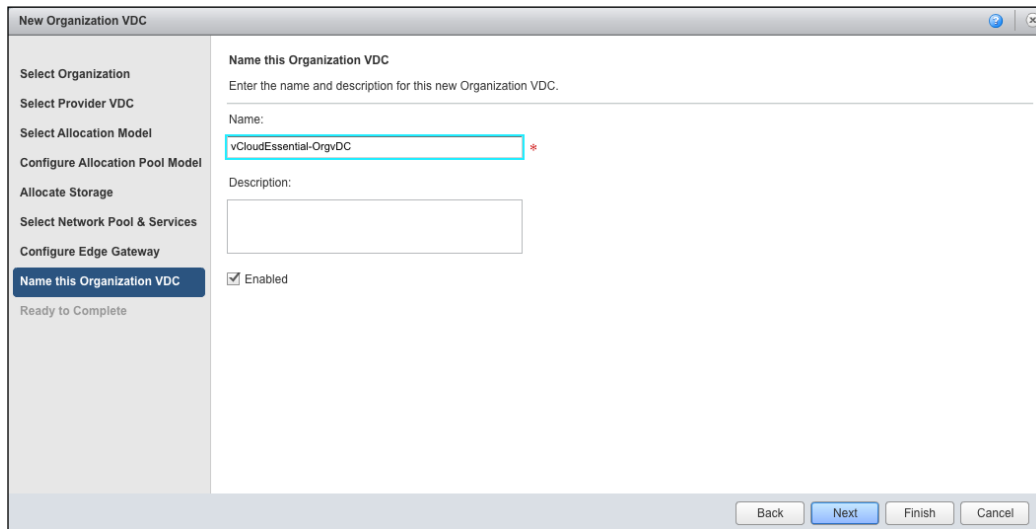
10. In the **Allocate Storage** section, select the storage profile and click on the **Add** button.
11. Change the **Storage Limit** value in the panel on the right-hand side and click on **Next**, as shown in the following screenshot:



12. On the **Select Network Pool & Services** page, select the preferred network pool from the **Network pool** drop-down combobox.
13. Specify a quota in the **Quota for this organization** option and click on **Next**, as shown in the following screenshot:



14. On the **Configure Edge Gateway** section, do not select the checkbox to create an Edge gateway and click on **Next**.
15. In the **Name this Organization VDC** page, specify a name for this Org vDC and click on **Next**, as shown in the following screenshot:



The screenshot shows a window titled "New Organization VDC" with a sidebar on the left containing a list of configuration steps: "Select Organization", "Select Provider VDC", "Select Allocation Model", "Configure Allocation Pool Model", "Allocate Storage", "Select Network Pool & Services", "Configure Edge Gateway", and "Name this Organization VDC" (which is highlighted in blue). Below the sidebar, it says "Ready to Complete". The main area is titled "Name this Organization VDC" and contains the instruction "Enter the name and description for this new Organization VDC." There are two input fields: "Name:" with the value "vCloudEssential-OrgVDC" and a red asterisk indicating a validation error, and "Description:" which is empty. Below the fields is a checkbox labeled "Enabled" which is checked. At the bottom right, there are four buttons: "Back", "Next" (highlighted in blue), "Finish", and "Cancel".

16. On the **Ready to Complete** page, review the entered information to create this organization vDC and click on **Finish**.

Summary

In this chapter, we covered some critical aspects in implementing vCloud Director. We discussed the management of provider vDCs, vCloud Director network resources, and organizations and organization vDCs.

We covered vCloud Director network pools and external networks. We also covered different types of resource allocation models in the organization virtual datacenter.

In the next chapter, we will learn how to configure organization and vApp network. We also show you how to create and maintain cloud networks.

4

Managing Complex vCloud Director Networks

Deploying and managing VMware vCloud Director is not an easy task and requires a thorough understanding of the complex vCloud Director networking and its rich configuration options. In this chapter, we cover some key aspects of vCloud networks.

We will cover the following topics in this chapter:

- Configuring organization network services
 - Configuring DNS relay
 - DHCP service in vCloud Director
 - VPN tunnels in vCloud Director
 - Static routes in vCloud Director
 - Firewall services in vCloud Director
 - SNAT and DNAT rules in vCloud Director
- Creating and managing vShield edge and vCloud networks

In addition, we discuss the different ways to configure organization networks.

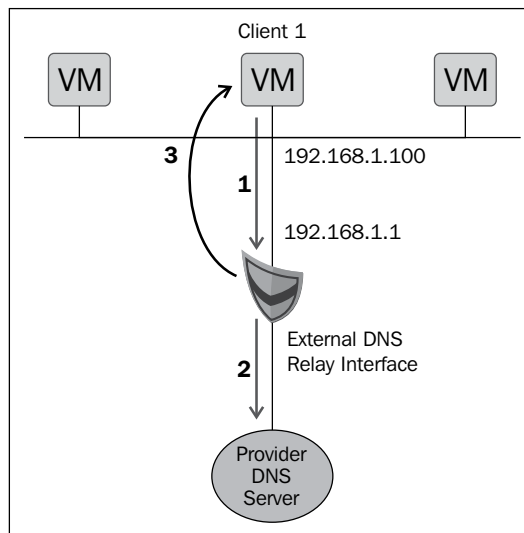
Configuring organization network services

Edge devices can be used as DNS relay hosts owing to the release of vCloud Networking and Security suite 5.1. However, before we jump onto how to do it and why you should do it, let us discuss the DNS relay host technology itself.

If your client machines want to send their DNS queries, they contact DNS relay, which is nothing but a host. The queries are sent by the relay host to the provider's DNS server or any other entity specified using the Edge device settings.

The answer received by the Edge device is then sent back to the machines. The Edge device also stores the answer for a short period of time, so any other machine in your network searching for the same address receives the answer directly from the Edge device without having to ask internet servers again. In other words, the Edge device has this tiny memory called DNS cache that remembers the queries.

The following diagram illustrates one of the setups and its workings:



In this example, you see an external interface configured on Edge to act as a DNS relay interface.

On the client side, we configured **Client1 VM** such that it uses the internal IP of the Edge device (**192.168.1.1**) as a DNS server entry.

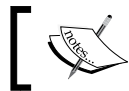
In this setup, **Client1** requests DNS resolution (step 1) for the external host, `google.com`, from Edge's gateway internal IP. To resolve `google.com`, the Edge device will query its configured DNS servers (step 2) and return that resolution to **Client1** (step 3).

Typical uses of this feature are as follows:

- DMZ environment
- Multi-tenant environment
- Accelerated resolution time

Configuring DNS relay

To configure DNS relay in a vShield Edge device, perform the following steps. Configure DNS relay when creating an Edge device or when there is an Edge device available.

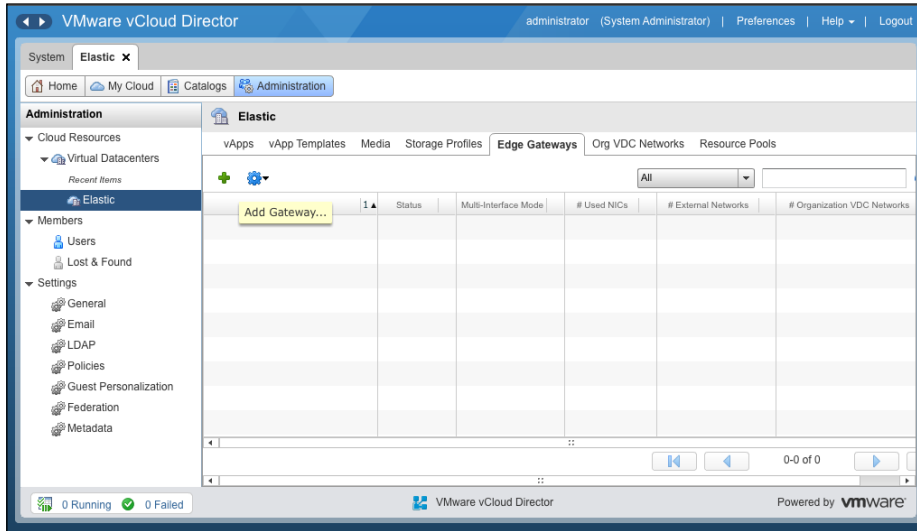


This is an option for an organization gateway and not for a vApp or Org network.

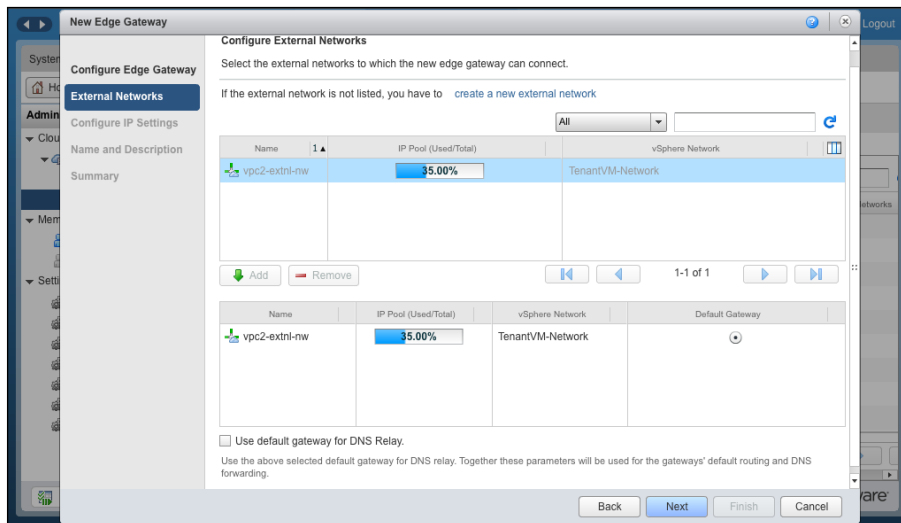
Now, let's develop an Edge gateway in an organization vDC while enabling DNS relay by executing the following steps:

1. Open the vCloud Director URL in a supported browser, for example, `https://serverFQDN/cloud`.
2. Log in to the cloud as the administrator. You will be presented with the **Home** screen.
3. Click on the **Organization VDCs** link and on the right-hand side, you will see some organization vDCs created.
4. Click on any organization vDC. Doing this will take you to the vDC page.
5. Click on the **Administration** page and double-click on **Virtual Datacenter**.
6. Then click on the **Edge Gateways** tab.

- Click on the green-colored + sign as shown in the following screenshot:



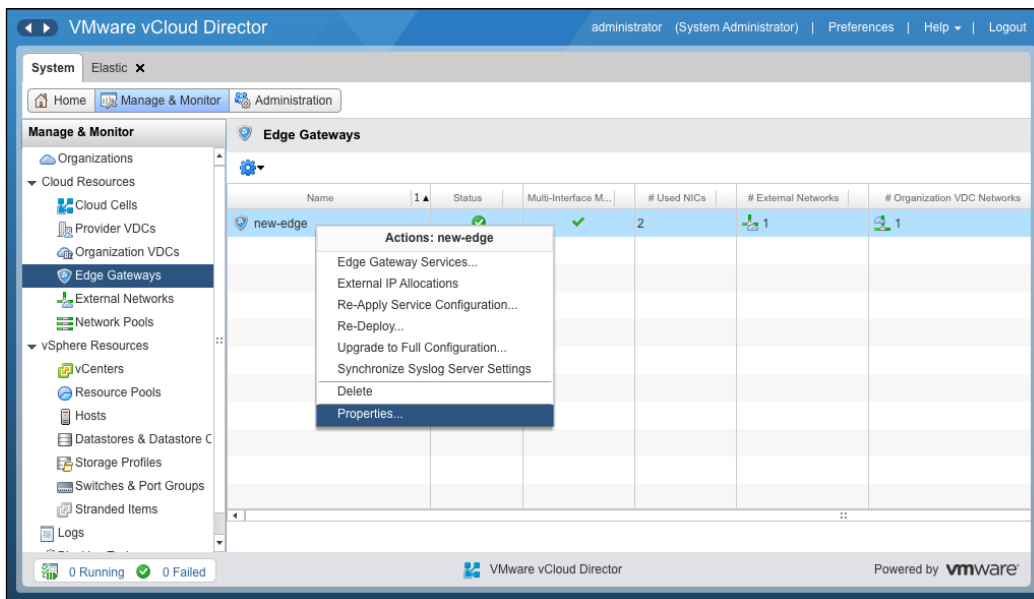
- On the **Configure Edge Gateway** screen, click on the **Configure IP Settings** section. Use the other default settings and click on **Next**.
- On the **Configure External Networks** screen, select the external network and click on **Add**.
- You will see a checkbox on this same screen. Use the default gateway for DNS relay. Once you do, select it and click on **Next**, as shown in the following screenshot:



11. Select the default value on the **Configure IP Settings** page and click on **Next**.
12. Specify a name for this Edge gateway and click on **Next**.
13. Review the information and click on **Finish**.

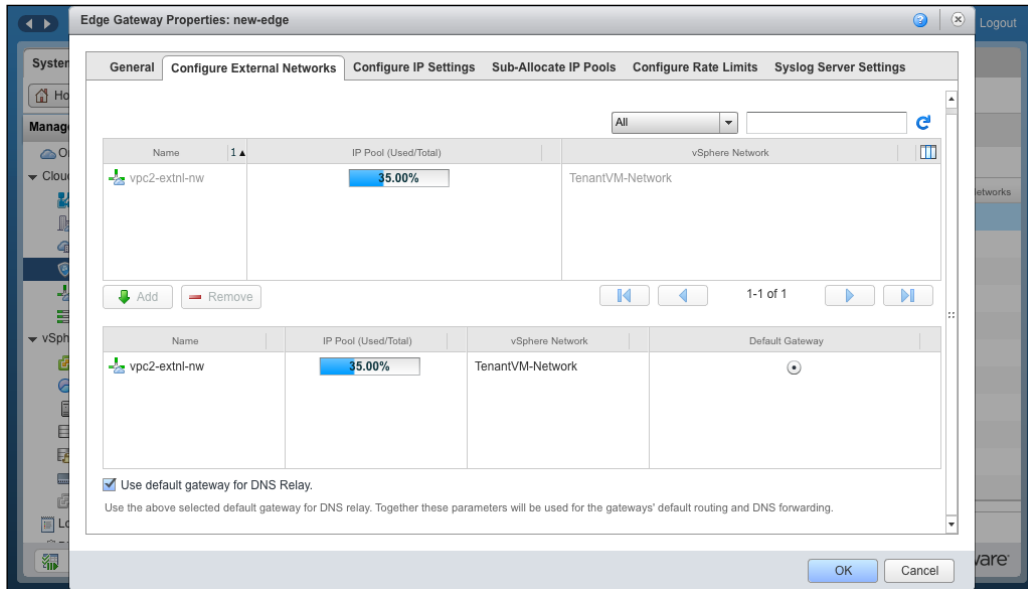
Let's look an alternative way to configure this, assuming you already have an Edge gateway and are trying to configure DNS Relay. Execute the following steps to configure it:

1. Open the vCloud Director URL in a supported browser, for example, `https://serverFQDN/cloud`.
2. Log in to the cloud as the administrator. You will be presented with the **Home** screen.
3. On the **Home** screen, click on **Edge Gateways**.
4. Select an appropriate Edge gateway, right-click, and select **Properties**, as shown in the following screenshot:



5. Click on the **Configure External Networks** tab.

6. Scroll down and select the **Use default gateway for DNS Relay** checkbox, as shown in the following screenshot:



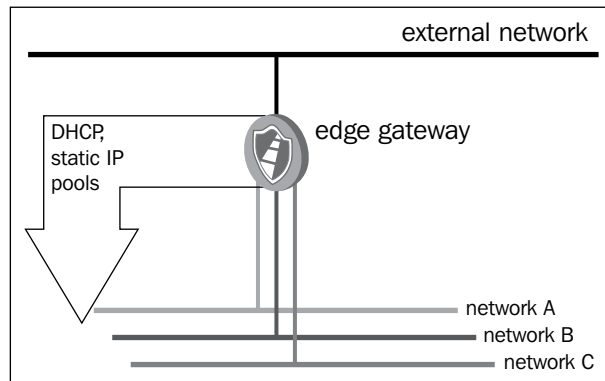
7. Click on **OK**.

In this section, we learned to configure DNS relay. In the next section, we discuss the configuration of a DHCP service in vCloud Director.

DHCP services in vCloud Director

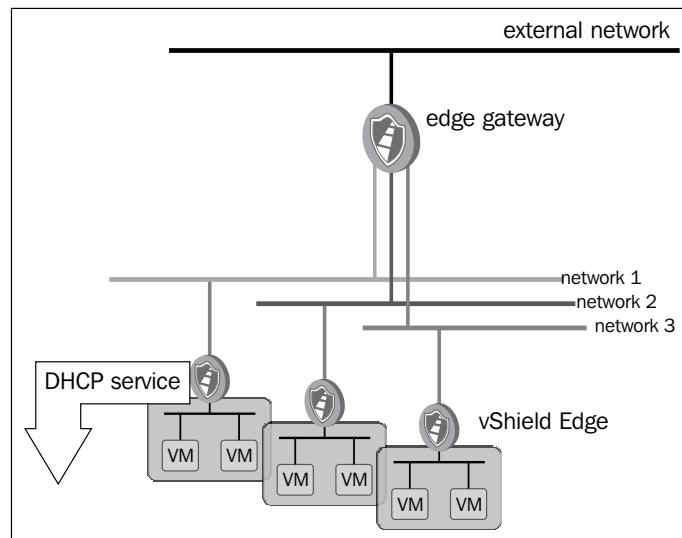
vShield Edge devices support IP address pooling using the DHCP service. vShield Edge DHCP service listens on the vShield Edge internal interface for DHCP discovery. It uses the internal interface's IP address on vShield Edge as the default gateway address for all clients. The broadcast and subnet mask values of the internal interface are used for the container network.

However, when you translate this with vCloud, not all types of networks support DHCP. That said, the Direct Connect network does not support DHCP. So, only routed and isolated networks support the vCNS DHCP service. The following diagram illustrates a routed organization vCD network:

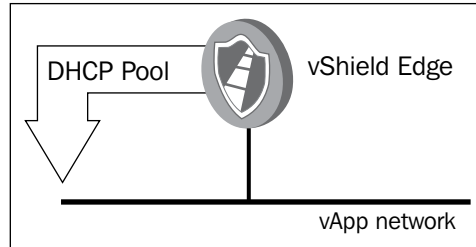


In the preceding diagram, the **DHCP** service provides an IP address from the Edge gateway to the Org networks connected to it.

The following diagram shows how vApp is connected to a routed **external network** and gets a **DHCP service**:



The following diagram shows a vApp network and a vApp connected to it, and DHCP IP address being obtained from the vShield Edge device:



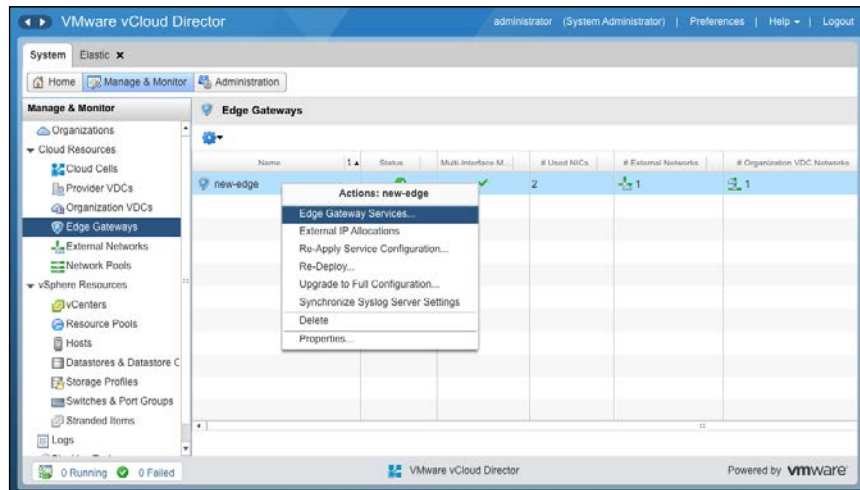
Configuring DHCP pools in vCloud Director

The following actions are required to set up Edge DHCP:

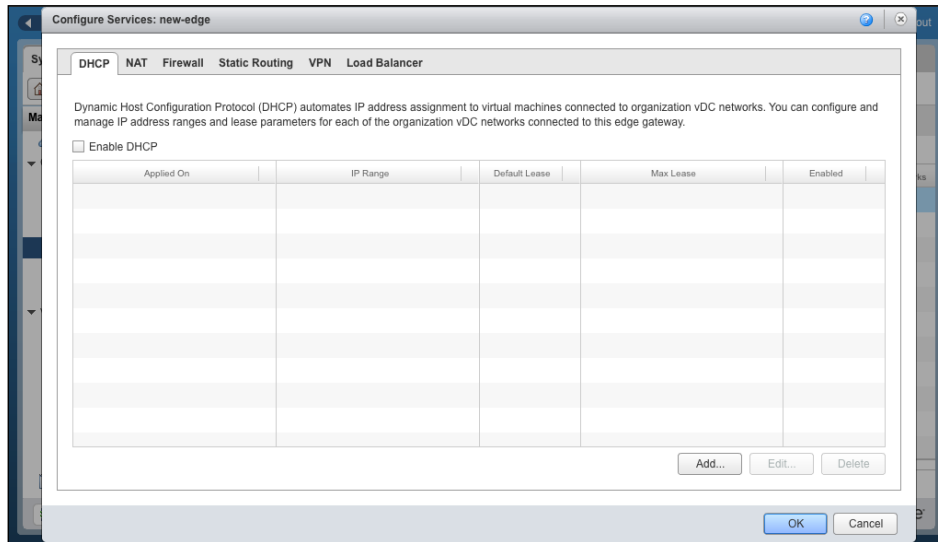
- Add DHCP IP pools
- Enable Edge DHCP services

As a prerequisite, you should know which Edge device is connected to which Org vDC network. Execute the following steps to configure DHCP pool:

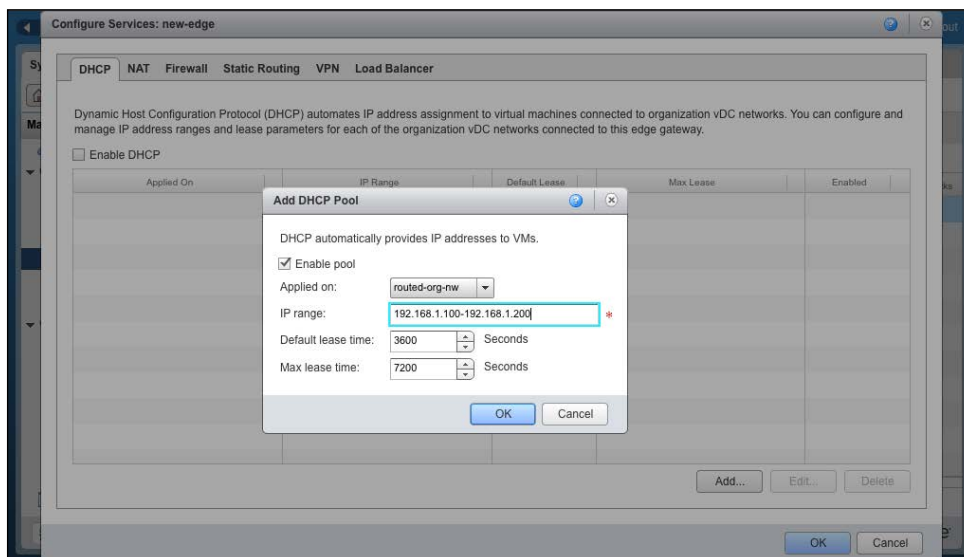
1. Open up a supported browser. Go to the URL of the vCD server; for example, <https://serverFQDN/cloud>.
2. Log in to vCD by typing an administrator user ID and password.
3. Click on the **Edge Gateways** link.
4. Select the appropriate gateway, right-click on it, and select **Edge Gateway Services**, as shown in the following screenshot:



- The first service is **DHCP**, as shown in the following screenshot:



- Click on **Add**.
- From the drop-down combobox, select the network that you want the DHCP to applied be on.
- Specify the IP range.
- Select **Enable Pool** and click on **OK**, as shown in the following screenshot:



10. Click on the **Enable DHCP** checkbox and then on **OK**.

In this section, we learned about the DHCP pool, its functionality, and how to configure it.

Understanding VPN tunnels in vCloud Director

It's imperative that we first understand the basics of CloudVPN tunnels and then move on to a use case. We can then learn to configure a VPN tunnel.

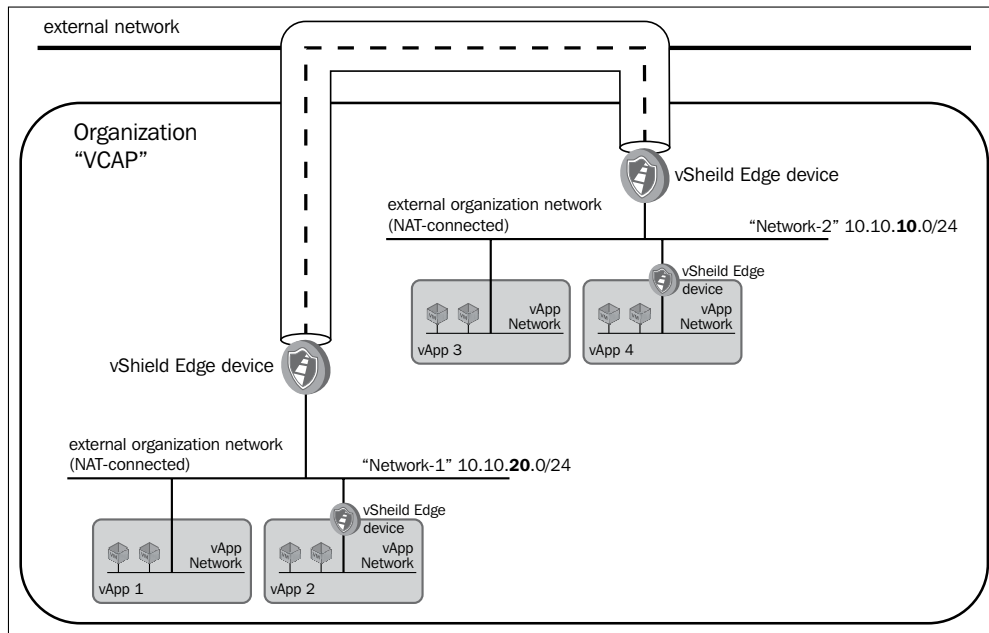
A VPN tunnel is an encrypted or more precisely, encapsulated network path on a public network. This is often used to connect two different corporate sites via the Internet. In vCloud Director, you can connect two organizations through an external network, which can also be used by other organizations. The VPN tunnel prevents users in other organizations from being able to monitor or intercept communications. VPNs must be anchored at both ends by some kind of firewall or VPN device. In vCD, the VPNs are facilitated by vShield Edge devices. When two systems are connected by a VPN tunnel, they communicate like they are on the same network.

Let's have a look at the different types of VPN tunnels you can create in vCloud Director:

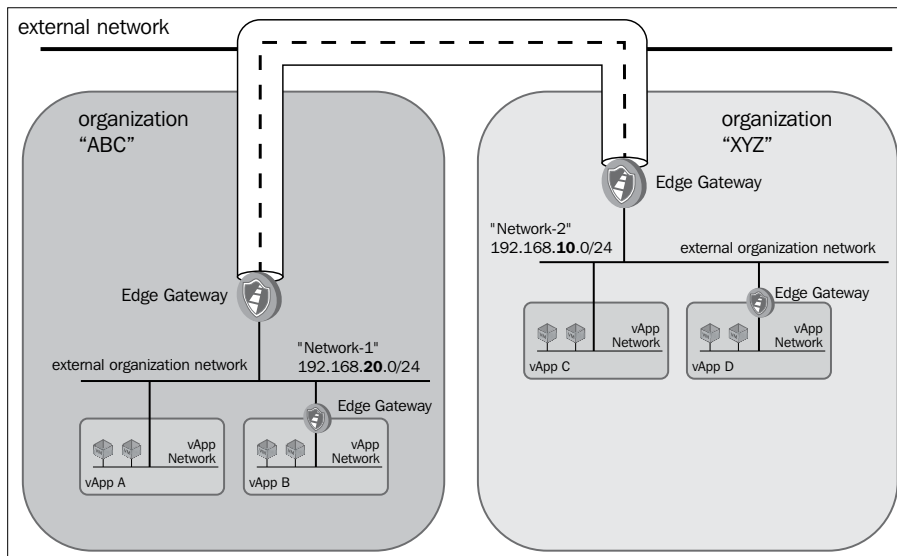
- VPN tunnels between two organization networks in the same organization
- VPN tunnels between two organization networks in two different organizations
- VPN tunnels between an organization network and a remote network outside of VMware vCloud

While only a system administrator can create an organization network, organization administrators have the ability to connect organization networks using VPN tunnels. If the VPN tunnel connects two different organizations, then the organization administrator from each organization must enable the connection. A VPN cannot be established between two different organizations without the authorization of either both organization administrators or the system administrator. It is possible to connect VPN tunnels between two different organizations in two different instances of vCloud Director.

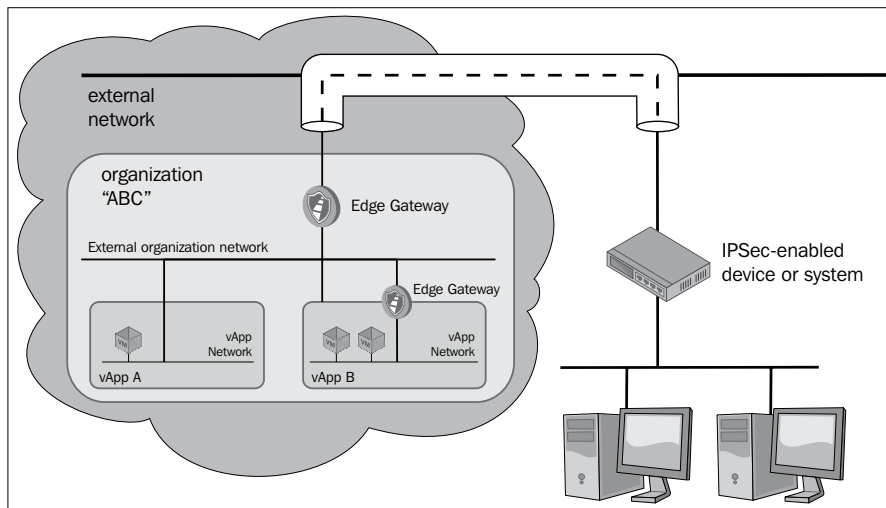
The following is a diagram of a VPN connection between two different organization networks in a single organization:



The following diagram shows a VPN tunnel between two organizations. The basic principles are exactly the same.



vCloud Director can also connect VPN tunnels to remote devices outside of vCloud. These devices must be IPSec-enabled and can be network switches, routers, firewalls, or individual computer systems. This ability to establish a VPN tunnel to a device outside of vCD can significantly increase the flexibility of vCloud communications. The following diagram illustrates a VPN tunnel to a remote network:

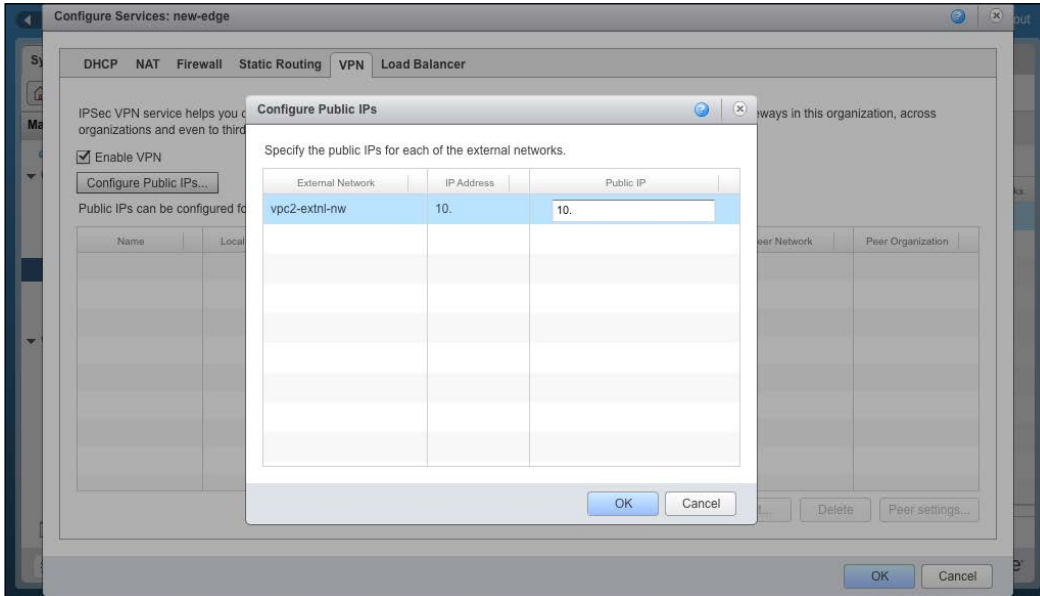


Configuring a virtual private network

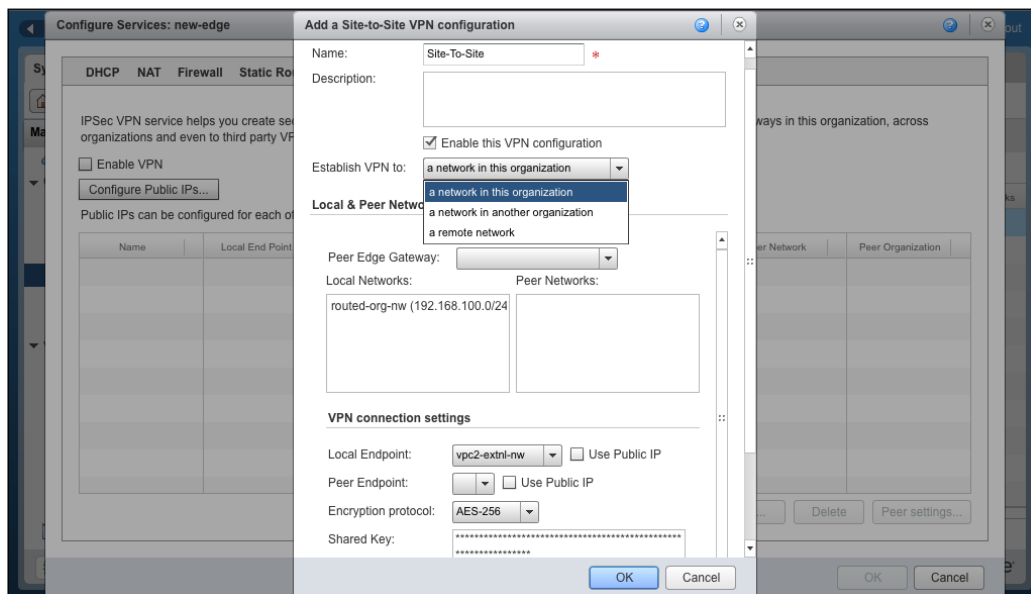
To configure an organization-to-organization VPN tunnel in vCloud Director, execute the following steps:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using the administrator user ID and password.
3. Click on the **Manage & Monitor** tab.
4. Click on the **Edge Gateways** link in the panel on the left-hand side.
5. Select an appropriate gateway, right-click, and select **Edge Gateway Services**.
6. Click on the **VPN** tab.
7. Click on **Configure Public IPs**.

8. Specify a public IP and click on **OK**, as shown in the following screenshot:



9. Click on **Add** to add the VPN endpoint.
10. Click on **Establish VPN to** and specify an appropriate VPN type (in this example, it is the first option), as shown in the following screenshot:



11. If this VPN is within the same organization, then select the **Peer Edge Gateway** option from the dropdown.
12. Then, select the local and peer networks.
13. Select the local and peer endpoints. Now click on **OK**.
14. Click on **Enable VPN** and then on **OK**.



This section assumes that either the firewall service is disabled or the default rule is set to accept all on both sides.

In this section, we learned what VPN is and how to configure it within a vCloud Director environment. In the next section, we discuss static routing and various use cases and implementation.

Understanding static routes in vCloud Director

Although most present network routing is done dynamically, where routers automatically choose the best path between two network endpoints, a static route is still needed. It's specifically required when routers are configured to not create dynamic routes for security reasons. A static route is a preprogrammed path between two networks. Using vCloud Director, you can create static routes between vApp networks and organization networks.

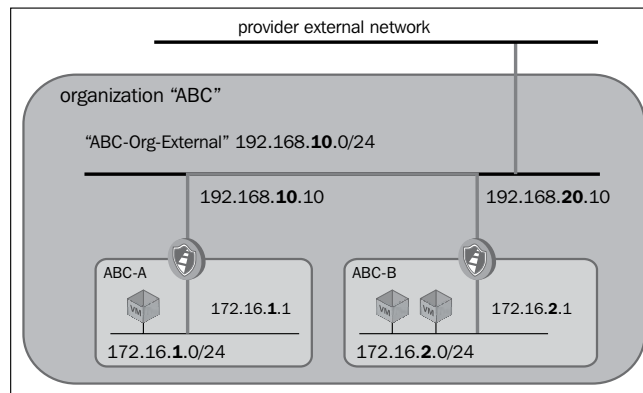
The following are the different types of supported static routes:

- Static routes from one vApp network to another between vApps in the same organization
- Static routes from one vApp network to another between vApps in different organizations

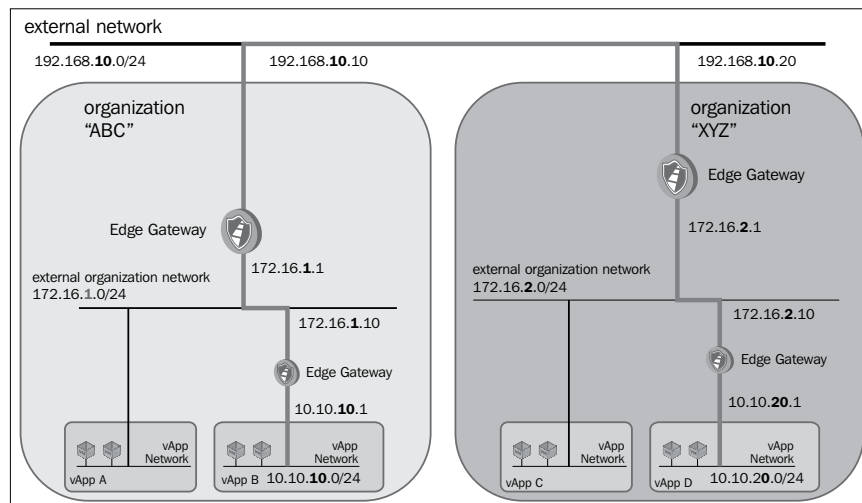
You're probably wondering whether two vApp networks that are connected to the same organization network can be connected with each other using a static route; the answer is yes, it is possible. This enables communications between two vApps; however, these communications are not encrypted. Static routing services must be enabled at the organization network level before creating static routes, which allow traffic between different vApps networks routed to other organization networks. For an organization network, static routing can be enabled only by system administrators. However, at the vApp network level, routes system can be established by administrators and organization administrators.

There are two ways to connect vApp networks with static routes. First is defining the static routes at the organization network level. This can be done by an organization administrator or a system administrator. The second way is the process of creating static routes at the vApp network level. This can be done by vApp administrators. Both vApp administrators must be involved and both vApps must have two routes.

The following diagram illustrates two different vApp networks in the same organization that are connected by a static route:



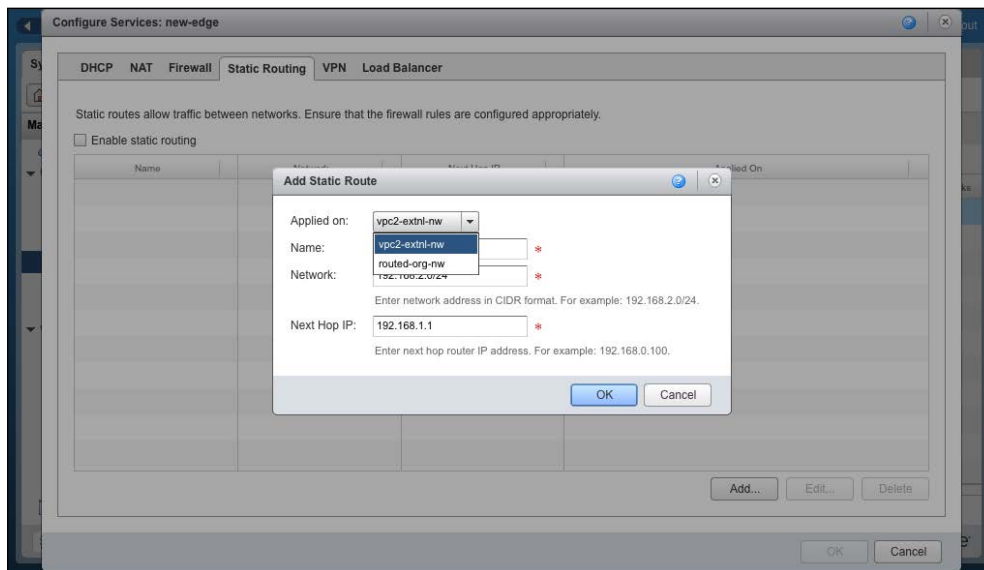
The following diagram shows two vApp networks in two different organizations connected by a static route. Only vApp networks connected to organization networks with a routed connection can be connected with a static route at the vApp level. If the vApp is directly connected, then it does not have a vApp network. vApps that are directly connected can still use static routes defined at the organization network level.



Configuring static routes in an Org Gateway

Execute the following steps to configure a static route:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab.
4. Click on the **Edge Gateways** link in the panel on the left-hand side.
5. Select the appropriate Edge gateway, right-click, and select **Edge Gateway Services**.
6. Click on the **Static Routing** tab.
7. Then click on **Add**.
8. Select the network it needs to be applied on.
9. Specify a route name.
10. Enter the network address that needs to be mapped.
11. Enter the next hop IP in the **Next Hop IP** field, through which it will reach the destination network, and click on **OK** as shown in the following screenshot:



12. Click on **Enable Static Routing** and click on **OK**.

In this section, we learned about static routing, its options, and how to configure it within a vCloud Director environment. In the next section, you'll learn about the firewall's functionalities and its configuration for vCloud Director-based networks.

Understanding the firewall service in vCloud Director

When you create a routed organization or vApp network, vShield manager deploys a vShield Edge device. This device contains a packet filtering firewall that helps control traffic within a vCloud environment.

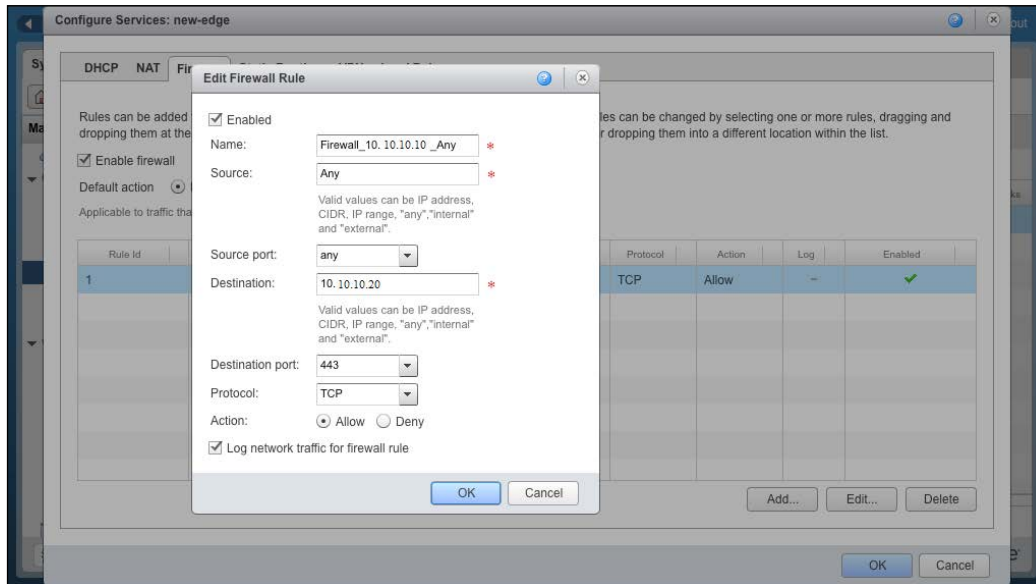
This is a 5-tuple firewall including source IP, source port, destination IP, destination port, and protocol. By default, this is enabled and all traffic is barred due to the implicit deny-all rule. You can place a firewall for incoming or outgoing traffic. If you want to troubleshoot a firewall issue, then your best bet is to disable the firewall service. The rule is retained on the vShield edge for later use. Another feature of this firewall is traffic logging, which you have the option to accept or deny. Your rule logs the traffic in your specified syslog host. This can be extremely useful in debugging firewall rules. vCD system logging has been discussed in *Chapter 1, Configuring and Maintaining vCloud Director*. The firewall rules for vShield Edge devices must be written on the basis of a virtual machine's external IP address for a static route, VPN, and so on.

Configuring the vShield Edge device firewall

In this activity, we will perform basic configuration tasks with a simple VMware vShield Edge device firewall:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Edge Gateways** link in the panel on the left-hand side.
4. Select the appropriate Edge gateway, right-click, and select **Edge Gateway Services**.
5. Click on the **Firewall** tab.
6. Then on the **Add** button.
7. Specify the name of the firewall rule and the five tuples.
8. Specify a firewall action (**Allow/Deny**).
9. Select the **Log network traffic for firewall rule** checkbox. (This is optional.)

10. Click on **OK** as shown in the following screenshot:

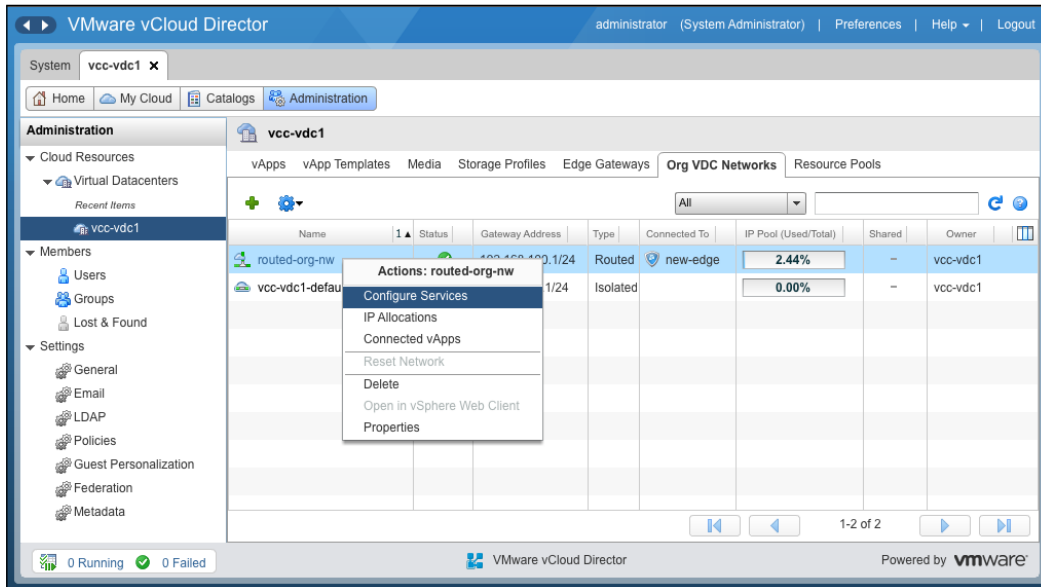


11. Click on the **Enable Firewall** checkbox (if it has not been enabled by default).
12. If you want to log firewall traffic for all the rules, then click on the **Log** checkbox. (This is optional.)
13. Click on **OK**.

If you want to create a firewall rule for a particular organization network, then execute the following steps:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Org vDC Networks** tab.

- Right-click on the organization vDC network name of your choice and select **Configure Services**, as shown in the following screenshot:



- Go to the **Firewall** tab and click on **Add**. Here, specify a name for the firewall rule.
- Specify the source IP address and the source port.
- If you apply this to incoming traffic, then the source has to be the external network. If you are applying this to outgoing traffic, the source has to be the organization vDC network.
- Specify the destination IP address and the destination port.
- If you apply this to incoming traffic, then the destination has to be the organization vDC network. For outgoing traffic, the destination is the external network.
- Specify the protocol and its action.
- A firewall rule can allow or deny traffic that matches the rule. Choose the type of acceptance here.
- Select the **Enabled** checkbox.
- Optionally, you can select the **Log network traffic** checkbox setting. If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.
- Click on **OK** twice.

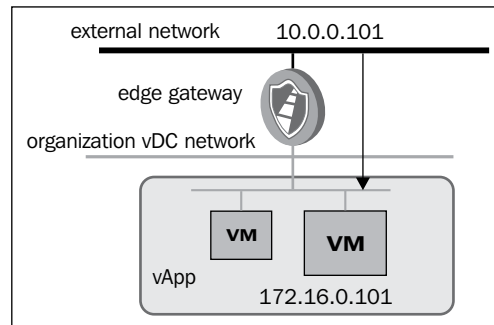
In this section, we discussed firewall management and its configuration on an organization network. In the next section, we discuss **DNAT (destination NAT)** and how to configure DNAT for an organization network.

Understanding DNAT rules in vCloud Director

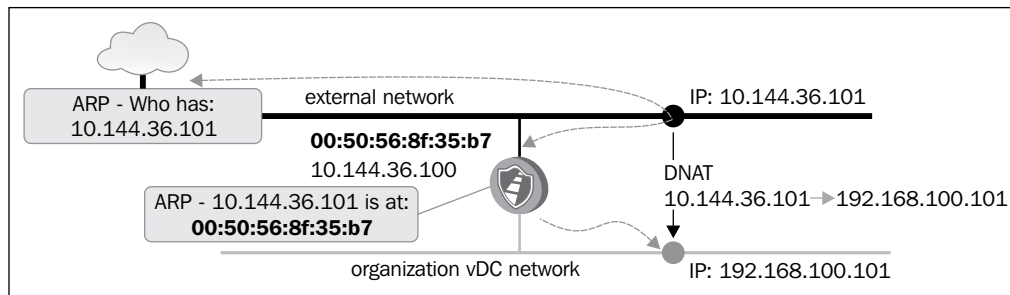
An unregistered IP address is mapped by a **Destination network address translation (DNAT)** to a registered one from a group of registered IP addresses. A 1:1 mapping between unregistered and registered IP addresses is established by DNAT. However, the mapping can vary per registered address available in the pool during communication. Typically, it redirects incoming packets with the destination of a public address/port to private IP one inside your network.

Generally, local area network (LAN), commonly referenced as the stub domain, is the internal network. A stub domain uses IP addresses internally, and most of the network traffic in it is local; it doesn't travel off the internal network. A stub domain can include both registered and unregistered IP addresses. Computers that have unregistered IP addresses must use network address translation to communicate with the rest of the world.

An example design is illustrated in the following diagram, where we map (DNAT) an external IP address to an internal one:



Here, we mapped **10.0.0.101** to an internal VM IP, **172.16.0.101**. This is rather simple and self-explanatory. Next, we show you the packet flow with the help of a diagram and explain how the packet flows.



Let's assume we have a client in the external network who wants to connect to the internal VM. This VM is inside the Org vDC network. It has an internal IP Address (**192.168.100.101**). The client sends an ARP for the external address, **10.144.36.101**. The external interface of your Edge device has an external IP address and will listen and send a reply that ARP is in the client's external MAC. After this, Edge will query the database (routing table) and ensure a 1:1 mapping of its internal IP; it sends the packet to the appropriate VM through the internal interface.

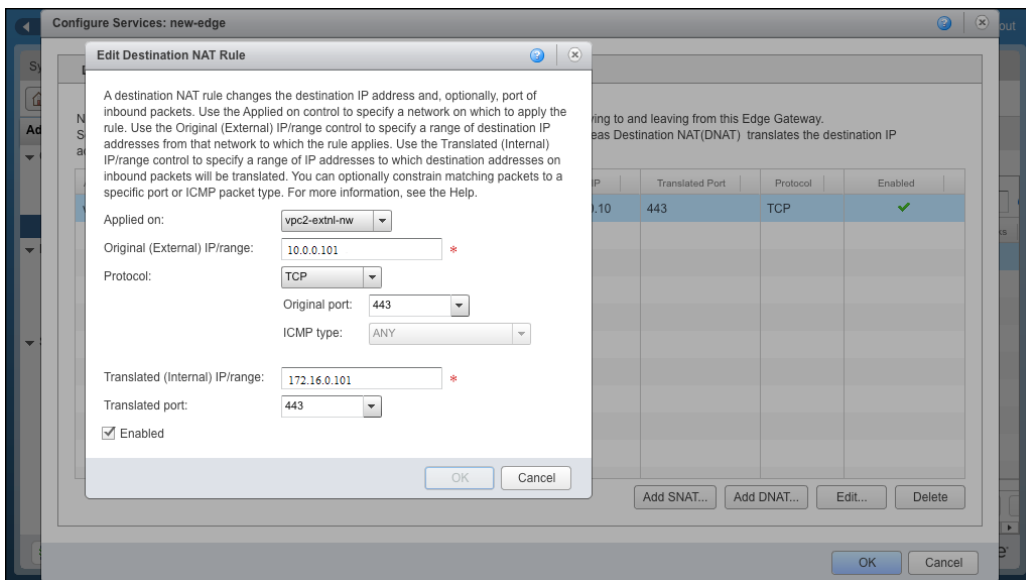
DNAT changes the destination address in the packet's IP header. It might also change the destination port in the TCP/UDP headers.

Configuring a destination NAT

Execute the following steps to configure a DNAT rule:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Edge Gateways** tab, right-click on the Edge gateway name, and select **Edge Gateway Services**.
6. Click on the **NAT** tab and click on **Add DNAT**.
7. Select an external network or another organization vDC network to apply this rule from the **Apply to** drop-down combobox.
8. Type the original IP address or range of IP addresses to apply this rule to the **Original (External) IP/range** textbox.
9. Choose the protocol to apply this rule from the **Protocol** drop-down combobox.
10. Select **Any** to apply this rule on all protocols.

11. Select an original port to apply this rule to. (This is optional.)
12. Next, select an ICMP type to apply this rule, that is, if this rule applies to IMCP. (This is optional.)
13. Type the IP address or range of IP addresses for the purpose of translating the inbound packets' destination addresses, in the **Translated (Internal) IP/range** textbox.
14. From the **Translated port** drop-down menu, select a port for inbound packets to be translated. (This is optional.)
15. Select **Enabled** and click **OK**, as shown in the following screenshot:



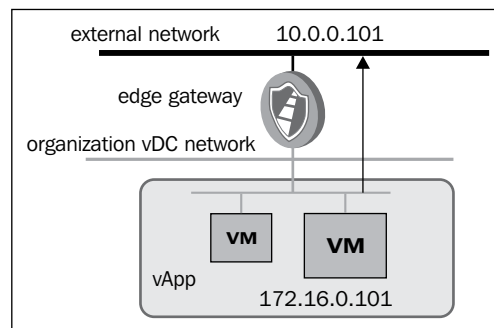
In this section, we discussed DNAT and its configuration over an organization network. In the next section, we learn about **source NAT (SNAT)** and how to configure SNAT for an organization networks.

Understanding SNAT rules in vCloud Director

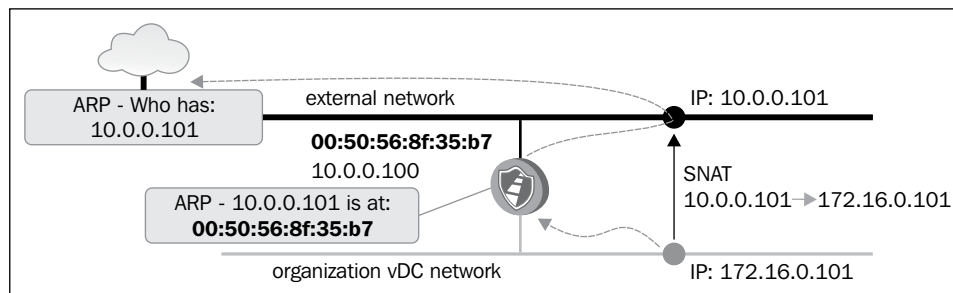
Source network address translation (SNAT) translates the packet's source address. If you want, it can translate the source port to the specified value. SNAT is the reverse DNAT. Traffic leaving a specific IP address or IP range is interpreted as originating from a different IP address or range on an external network connected to the Edge gateway. In the case of IP ranges, each sequential IP pair has a 1:1 correlation.

SNAT mapping is unidirectional. Connections matching the mapping specification are allowed and the resulting solicited responses return using the correct IP addresses and ports. Unsolicited inbound traffic is not allowed. Gateway responds to ARP requests for each SNAT-defined external address. After the packets are received, the Edge gateway transforms the destination IP address, updates checksums, and translates the destination port if needed. The external addresses of SNAT rules must be in the range of a directly attached subnet. The source address can be from a directly attached subnet or a source routed to the gateway.

The following is a logical diagram for SNAT:



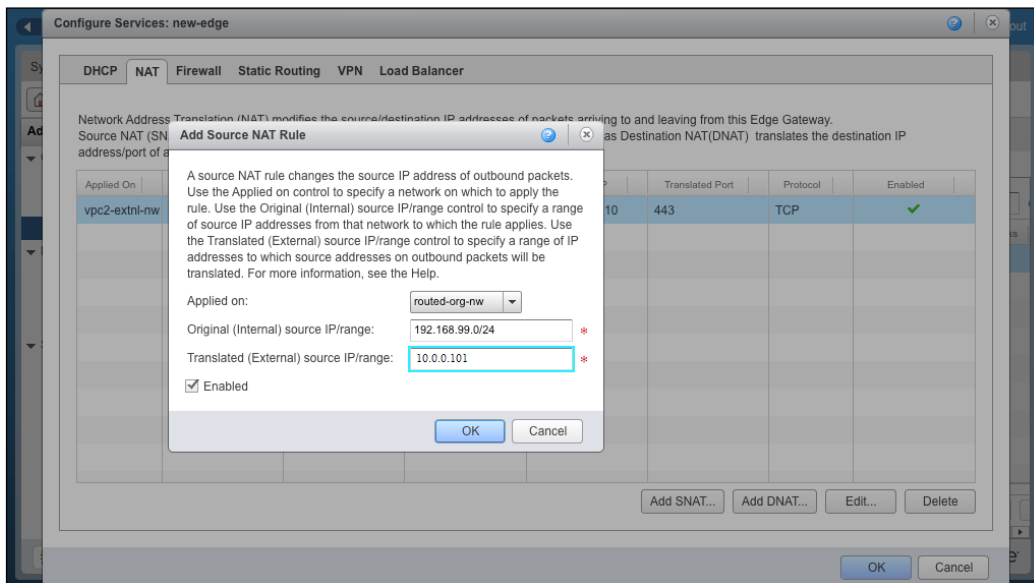
The following diagram illustrates the SNAT packet flow:



Configuring a source NAT

Execute the following steps to configure a DNAT rule:

1. Start the Internet Explorer browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Edge Gateways** tab, right-click on the Edge gateway name, and select **Edge Gateway Services**.
6. Click on the **NAT** tab and click on **Add SNAT**.
7. Select an organization vDC network to apply this rule on from the **Applied on** drop-down menu.
8. Type the original IP address or range of IP addresses to apply this rule in the **Original (Internal) source IP/range** textbox.
9. Type the IP address or range of IP addresses to translate the addresses of outgoing packets, in the **Translated (External) source IP/range** textbox.
10. Select **Enabled** and click on **OK** as shown in the following screenshot:



Creating and managing vShield edge and vCloud networks

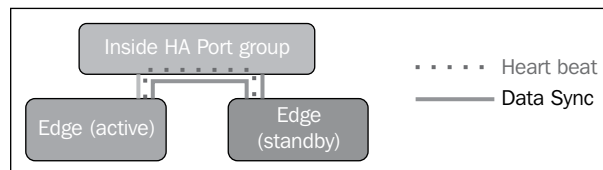
With the release of VMware vShield 5.1, we have seen the high availability of the vShield Manager Service Virtual Machine. In this activity, you will learn how **High Availability (HA)** in an Edge device works and its configuration.

The HA feature in vShield edge deploys two Edge appliances per cluster, which runs in the active-standby mode.

vCenter networking and Security Manager manages the lifecycle of both peers and will simultaneously push user configurations to both edges. The Active Edge device will push run-time state information to standby as well. Edge HA peers communicate with each other using an internal IP address and cannot be used for other purposes except HA. This IP address is allocated to one of the internal interfaces of the Edge device.

The Edge devices must be allowed to communicate without L2 restrictions, meaning there is an auto firewall rule generator that allows the communication. Autorule generation automatically generates service rules to allow the flow of controlled traffic in between peers.

vShield Edge devices in HA mode exchange two types of network traffic, Heartbeat and Data Sync. The following is a logical diagram for these types of traffic:



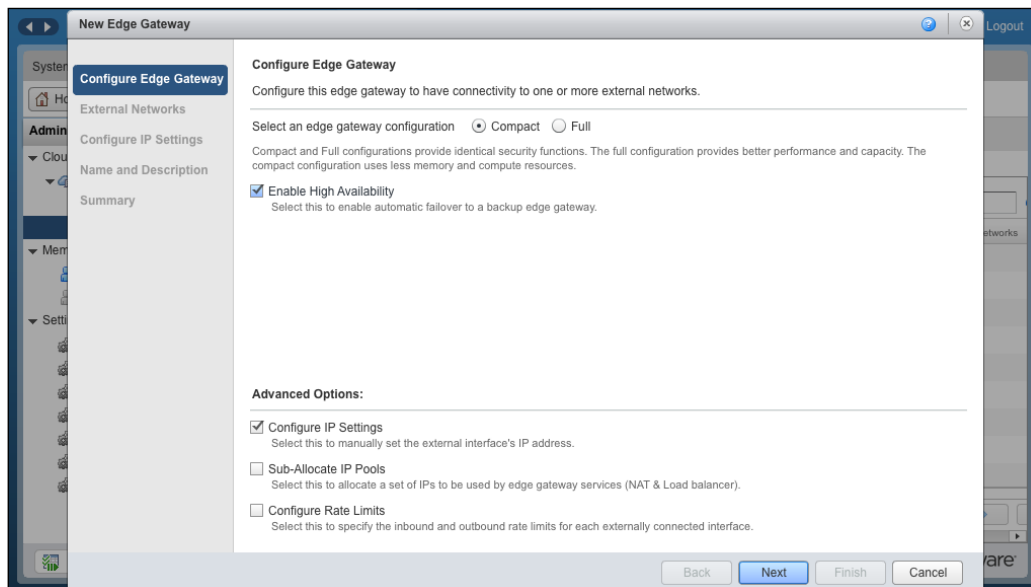
So, when you deploy an Edge appliance in HA mode, in the vSphere level, it creates an anti-affinity rule in the DRS cluster and places them separately in two different hosts within that cluster.

The following events occur when an Edge device experiences a failure:

- Fails over to the passive Edge device statefully for the firewall connections
- Load balancer should sync to the passive Edge device and then fail over to the passive node
- SSL VPN client should automatically reconnect when it fails over
- IPsec VPN tunnel should automatically reconnect when there is a failover
- After the failover edge, the DHCP allocation table state is retained

Execute the following steps to configure a vShield Edge HA:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Edge Gateways** tab and click on the green-color + sign to create an Edge gateway.
6. In the first screen, select the **Enable High Availability** checkbox, as shown in the following screenshot:



7. Click on **Configure IP Settings** and then on **Next**.
8. On the next screen, add the external network and click on **Next**.
9. Check **Configure IP Settings** and click on **Next**.
10. Specify a name and description and click on **Next**.
11. Click on **Finish**.

Configuring vShield Edge devices for compact/full configuration

Create an Edge gateway in either a compact or full configuration. If you choose the full configuration option, it increases capacity and performance. On the other hand, compact configuration requires less memory and fewer compute resources. However, all services are available in either configuration. The following table shows the differences between the two types of configuration:

Resources	Edge (Compact)	Edge (Full)
vCPU	1	2
Memory	256 MB	1 GB
Firewall Performance (Gbps)	3	9.7
Concurrent Sessions	64,000	1,000,000
IPSec VPN throughput (Gbps) – H/W acceleration via AESNI	0.9	2

Execute the following steps to configure a vShield Edge for compact or full configuration:

1. Open up a supported browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and then on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Edge Gateways** tab and then on the green-colored + sign to create an Edge gateway.
6. On this first screen, select the option button for compact or full, depending on your choice of **Edge Gateway** configuration and click on **Next**.
7. Click on **Configure IP Settings** and then on **Next**.
8. On the next screen, add the external network and click on **Next**.
9. Specify a name and its description and click on **Next**.
10. Click on **Finish**.

vCloud Org networks

There are three types of organization vDC networks:

- **Direct Connect organization vDC networks:** This network is created by vCloud Director system administrator and cannot be changed or managed by the organization administrator. As the name suggests, a Direct Connect organization vDC network is a representation of a specific external network. It uses an external network to connect directly to the Internet or to systems outside of the cloud. For example, web servers using an external type of network is the best solution because it does not need internal communication.

If you want to administer this server, with this type of network, you can directly connect to it through SSH or a remote desktop. If vApp is directly connected, either the vApp IP addresses must be statically configured or a DHCP server should be connected to the external network with IP addresses. If vApp addresses are statically configured, they should use the same subnet that the external network is using. Direct Connect vApps should be fenced when connecting to external networks to prevent MAC or IP addresses conflicts.
- **Routed organization vDC networks:** This network connects to a vShield Edge gateway. Only a vCloud Director system administrator can manage external connections to the edge device. Once an Edge gateway has been created for an organization, the organization administrator can create as many routed networks as necessary, within the limitations of the Edge gateway device that have been defined by the vCloud Director administrator; configure NAT features for each network (on the Edge gateway device); manage IP allocation pools and DHCP ranges; and configure firewall rules. An Edge gateway can support 10 networks. Users can attach routed vApp networks or Direct Connect vApps to a routed organization vDC network.
- **Isolated organization vDC networks:** This network does not connect to an edge gateway. An isolated network is backed by an Edge device that can provide DHCP and static IP services to a single organization's network. An organization administrator can create any number of isolated organization vDC networks. An isolated organization vDC network is defined as a single subnet. A use case for an internal organization vDC network could be when customers do not want certain vApps to be connected to the Internet, external networks, or other organization vDC networks. In an isolated organization network, Edge devices do not provide firewall or routing services. If virtual machines in different vApps must communicate with each other, NAT features must be configured on each vApp network edge device.

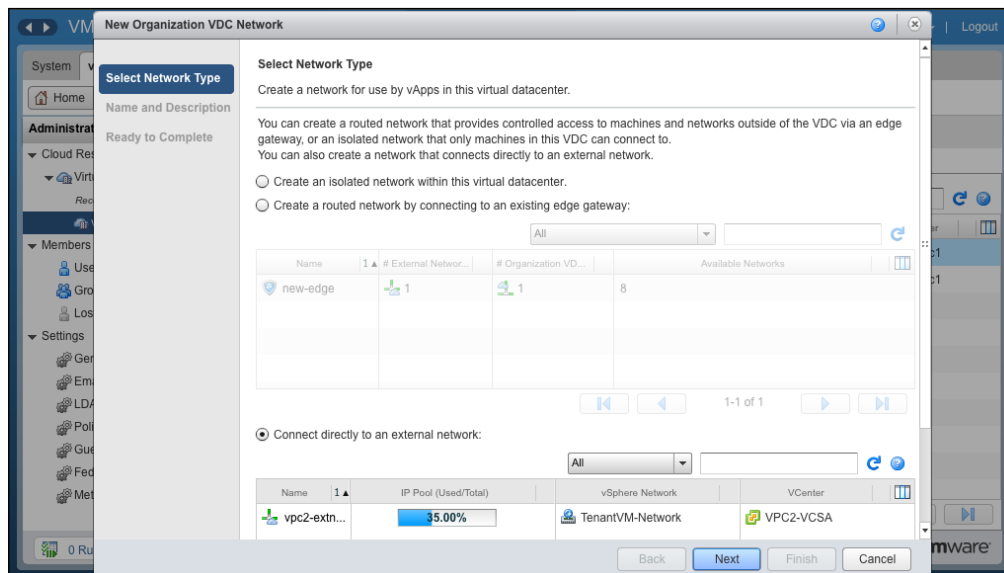
Organization users can attach routed vApp networks to each type of organization vDC network or Direct Connect vApps to each type of network.

Firstly, we learn how to create a Direct Connect network, followed by how to configure a routed organization network and isolated organization network.

Configuring a Direct Connect organization network

Execute the following steps to configure a Direct Connect organization network:

1. Start a browser. Insert the URL of the vCD server into it, for example, example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Org VDC Networks** tab.
6. Click on the green-colored + sign and you will see a screen similar to that shown in the following screenshot:



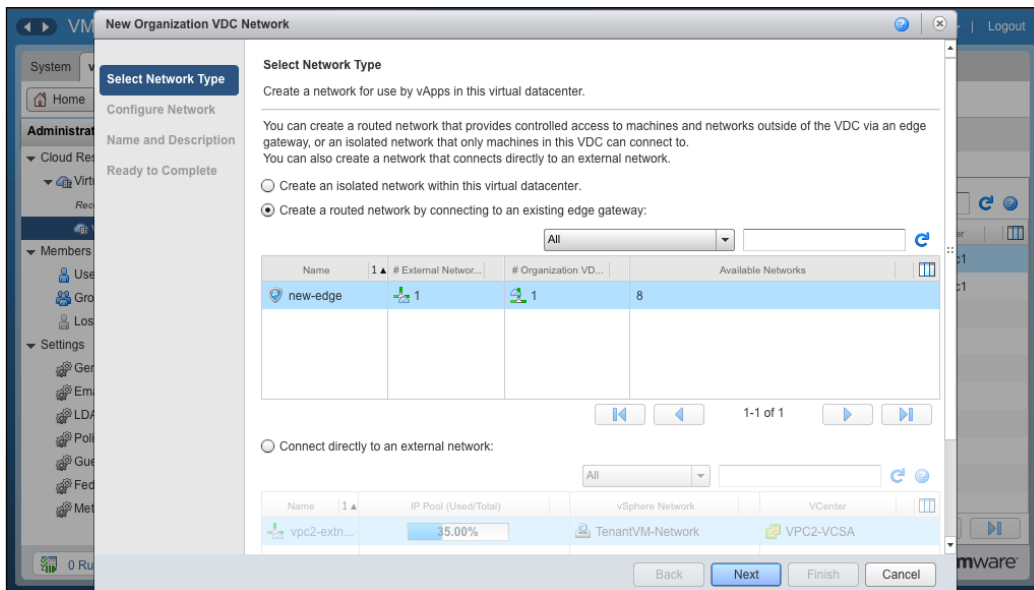
7. Click on **Connect directly to an external network** and select the external network.
8. Click on **Next**.

- Specify a name for the external organization network and description (This is optional.).
- Click on **SHARE this network with other VDCs in the organization** and then on **Next**. This option is optional but will enable you to use the Direct Connect organization network in other organization vDCs as well.
- Review the information and click on **Finish**.

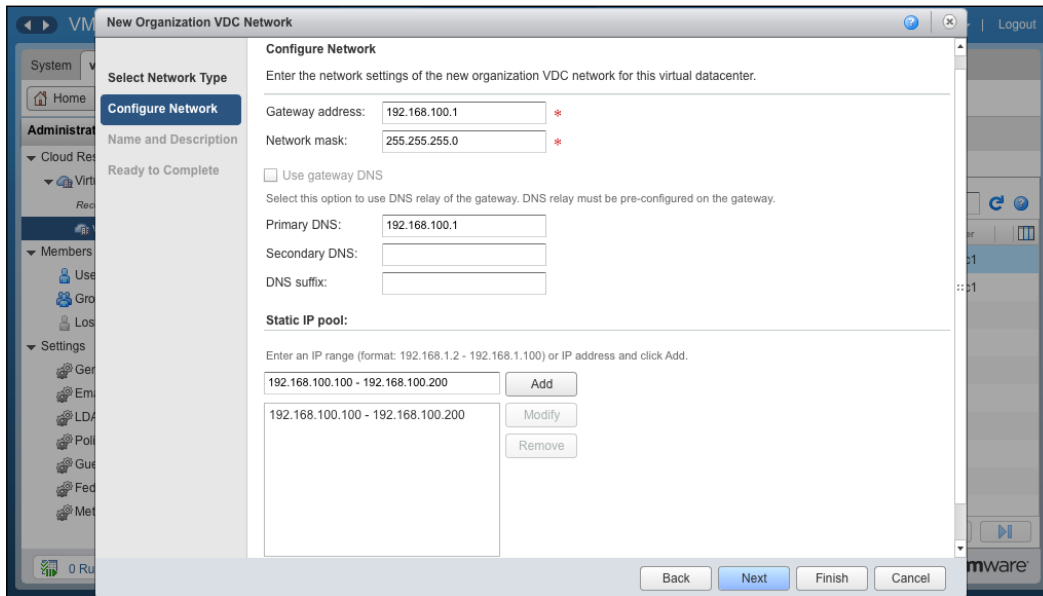
Configuring a routed organization network

Execute the following steps to configure a routed organization network:

- Start a browser. Go to the URL of the vCD server, for example, `https://serverFQDN/cloud`.
- Log in to vCD using an administrator user ID and password.
- Click on the **Manage & Monitor** tab and click on **Organization vDCs** in the pane on the left-hand side.
- Double-click on the organization vDC name to open the organization vDC.
- Click on the **Org VDC networks** tab.
- Click on the green-colored **+** sign. You will see a screen similar to the what's shown in the following screenshot:



7. Click on **Create a routed network by connecting to an existing edge gateway** and select the existing edge device.
8. Click on **Next**.
9. On this screen, specify the gateway address, network mask, DNS, and a static IP pool, as shown in the following screenshot, and click on **Next**:



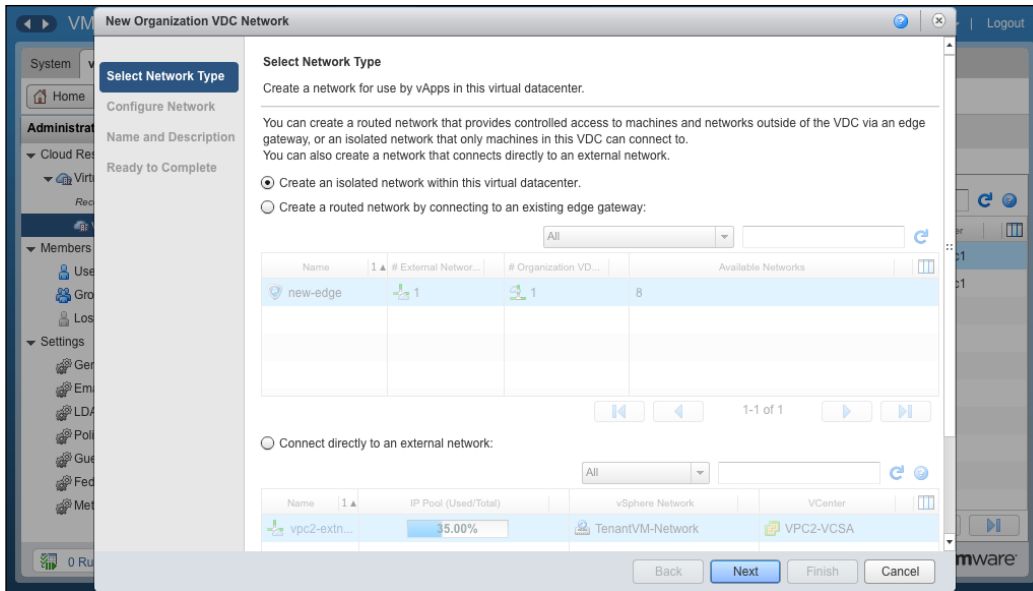
10. Specify a name of the routed organization network and its description. (This is optional)
11. Click on **Share this network with other VDCs in the organization** and click on **Next**. This option is optional but enables you to use this Direct Connect organization network in other organization vDCs as well.
12. Review the information and click on **Finish**.

Configuring an isolated organization network

Perform the following steps to configure an isolated organization network:

1. Start a browser. Insert the URL of the vCD server into it, for example, `https://serverFQDN/cloud`.
2. Log in to vCD using an administrator user ID and password.
3. Click on the **Manage & Monitor** tab and then on **Organization vDCs** in the pane on the left-hand side.

4. Double-click on the organization vDC name to open the organization vDC.
5. Click on the **Org VDC Networks** tab.
6. Click on the green-colored + sign. You will see a screen similar to what is shown in the following screenshot:



7. Click on the **Create an isolated network within this virtual datacenter** option.
8. Click on **Next**.
9. On this screen, specify the gateway address, network mask, DNS, and a static IP pool, and click on **Next**.
10. Specify a name for the internal organization network and its description. (This is optional.)
11. Click on **Share this network with other VDCs in the organization** and then on **Next**. This option is optional and enables you to use this Direct Connect organization network in other organization vDCs as well.
12. Review the information and click on **Finish**.

Summary

In this chapter, we discussed about the configuration of organization and vApp networks, which included configuring DNS Relay, DHCP Service, firewall management, SNAT and DNAT configuration. We also learned how to create and maintain cloud networks that include different types of networks, such as Direct Connect, routed, and isolated organization.

In the next chapter, we focus on managing vApps and catalog. We discuss sharing catalogs and vApps, creating and deploying vApps, creating and configuring catalogs, and managing vApp storage settings.

5

Managing Catalogs and vApps

VMware vCloud Director virtual machines are virtualized hosts. They are called **virtual appliances (vApps)**; however, vApp in vCenter Server is not the same vApp in vCloud director. The management and configuration of these virtual machines control the functionality of vApps. VMware vCloud Director vApps are predefined packages of virtual machines and networks. The configuration of these packages can be a complex task.

A major part of an organization administrator's job is configuring vApps and then using these vApps to create vApp templates. Organization administrators also must assist users in the vApp Author role with the creation and management of vApps.

Similarly, VMware vCloud Director uses catalogs to provide collections of standardized vCloud Director vApp templates and media files to cloud customers. The organization administrator must manage and use these catalogs.

vApp templates allow efficient and rapid deployment of virtual machines in a vCloud environment. Standardized vApp templates can also reduce resource consumption. The creation and management of these templates is a major part of the organization administrator's job.

This chapter covers the following topics:

- Creating and deploying vApps
- Understanding catalogs
- Understanding vApp templates

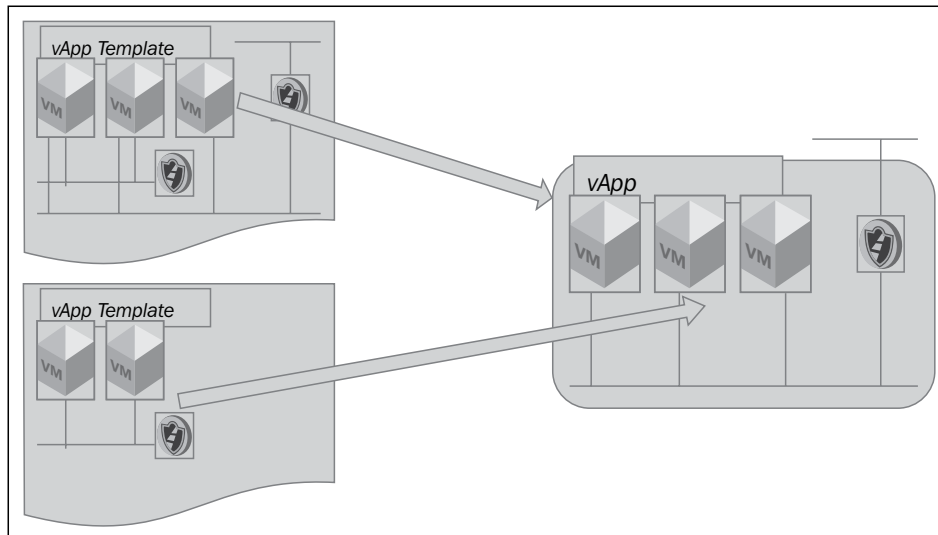
Creating and deploying vApps

vCloud Director delivers IT services in packages called vApps. vApps are composed of one or more virtual machines. These virtual machines communicate over networks included in the package and use resources and services in the deployed environment. The package also includes an OVF descriptor, which provides general application information, hardware requirements, deployment instructions, and policies that are enforced during runtime.

A vCloud vApp is instantiated and consumed differently in vCloud compared to a vSphere environment. A vApp is a container for a distributed software solution and is the standard unit of deployment in vCloud Director. It has power-on operations, consists of one or more virtual machines, and can be imported or exported as an OVF package. A vCloud vApp might have additional vCloud specific constructs such as vApp networks.

Even if you need only one virtual machine, you still must create a vApp for that virtual machine. In vCloud Director 5.1, you can create a vApp by cloning a template in a catalog or by creating a new one. After you have created the vApp, you can add, remove, or modify the virtual machines in it. vApp property settings enable you to control the behavior of virtual machines when you start and stop the vApp. For example, you can set the order in which the virtual machines power on and off.

You can create a vApp based on a vApp template stored in a catalog that you have access to. A vApp in vCloud Director is a logical construct used to describe a set of virtual machines. This is shown in the following diagram:



vApps simplify the deployment and management of a multi-tier application in multiple virtual machines. vApps do this by encapsulating them in a single virtual entity. A vApp has the same basic operations as a virtual machine and can contain one or more virtual machines.

vApps encapsulate not only virtual machines but also their interdependencies and resource allocations, which enables single-step power operations, cloning, deployment, and monitoring of the entire application. If the virtual machine is based on an OVF file that includes OVF properties for customization, these properties are retained in the vApp. If any of those properties are user configurable, you can specify the values in the virtual machines properties pane after you add them to the vApp.

The distribution format for vApps is OVF, which implies that they can be imported and exported as OVF virtual machines.

Custom vApp properties

The vApp custom guest properties feature allows users to pass custom data to the guest operating system of vApps that are deployed in vCloud Director. The custom guest properties feature is useful for an application developer and an application owner. This is because the application can be customized by users in ways beyond guest customization (which are available in earlier versions of vCloud Director).

The steps involved in deploying a custom guest vApp include the following:

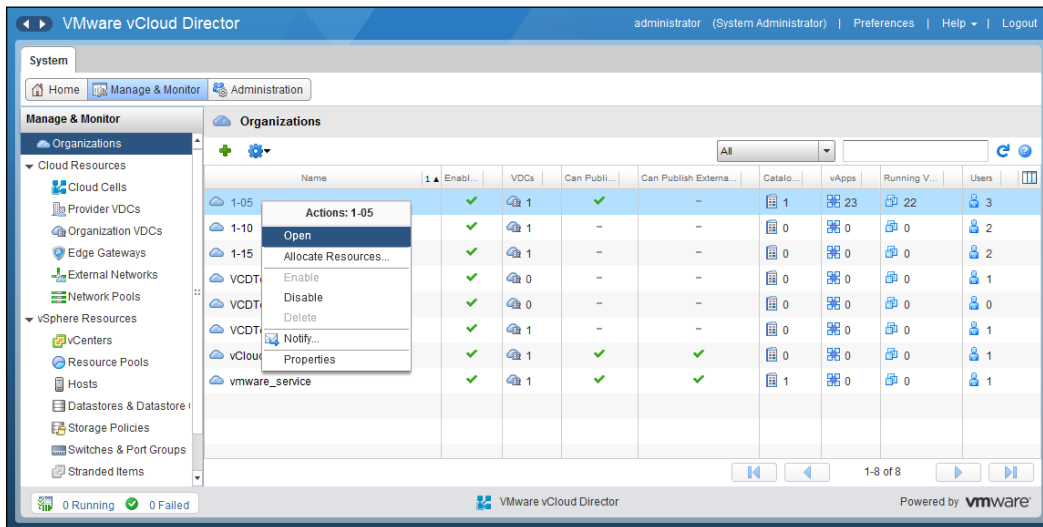
- Template creation by the author:
 - vApp Author creates a vApp and inside it creates a VM
 - vApp Author installs the guest software within that VM
- Deployment by user:
 - Users deploy that vApp
 - Users power on vApp

The deployment works after steps 1 and 2. The OVF environment is generated by vCenter Server, and guest scripts run and customize the software.

Creating a vCloud Director vApp

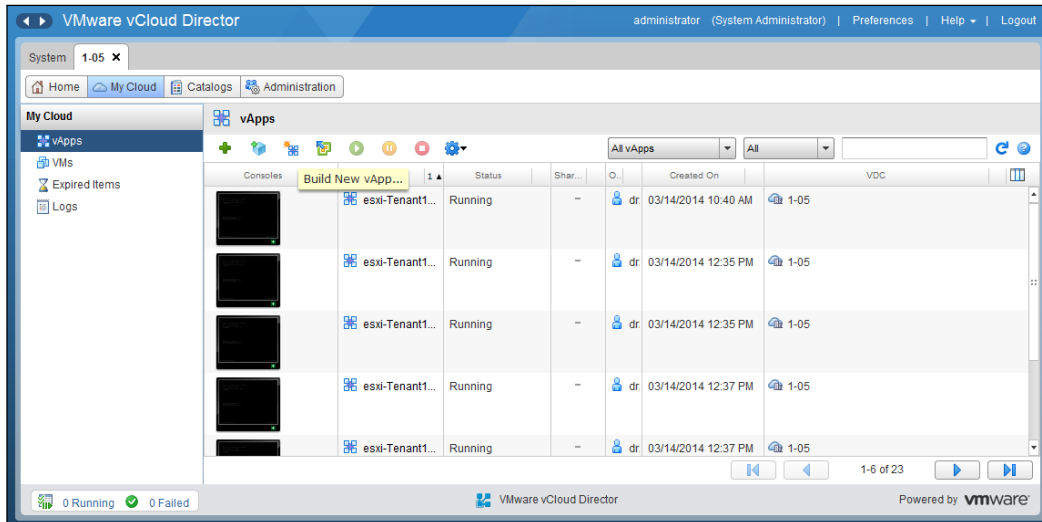
In this section, you will see how to build a vCloud Director vApp:

1. Start a browser. Type in the URL of the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by typing in an administrator user ID and password. Other roles such as org admin can also log in directly to their organization to perform this activity.
3. On the home screen, click on the **Manage & Monitor** tab.
4. In the left pane, click on **Organizations**.
5. In the right pane, right-click on your desired organization and click on **Open**, as shown in the following screenshot:

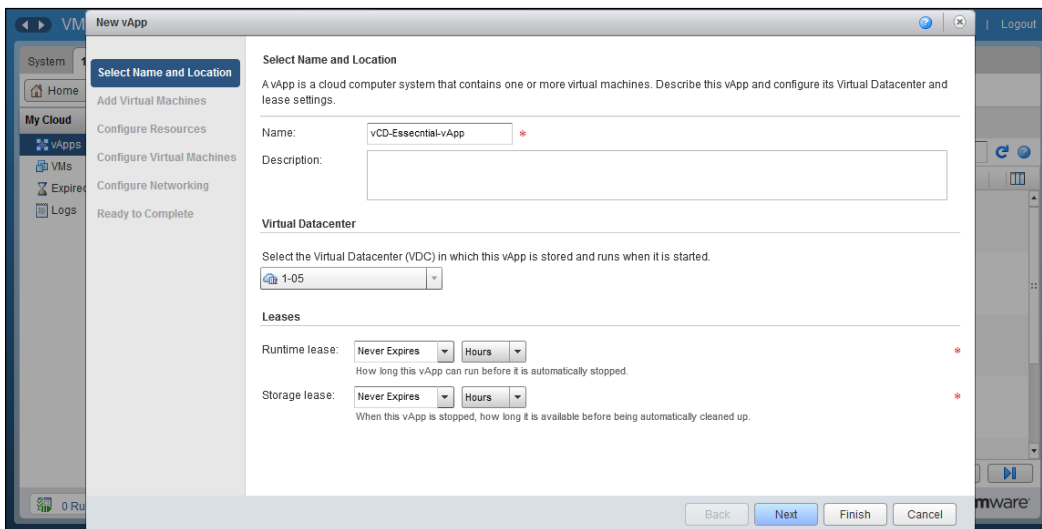


6. Click on the **My Cloud** tab.
7. In the left pane, click on **vApps**.

8. In the right pane, click on the **Build New vApp** icon, as shown in the following screenshot:

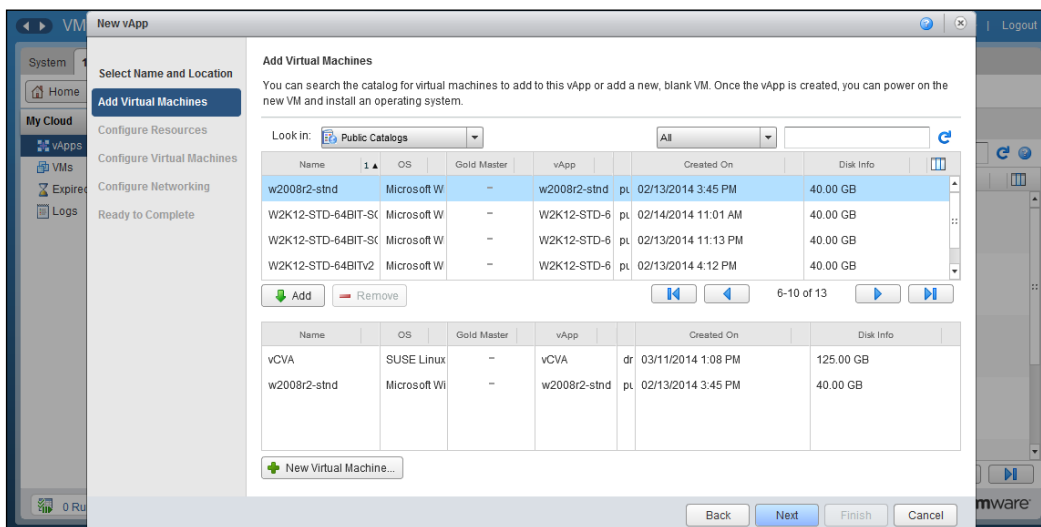


9. In the **New vApp** wizard, under **Name**, specify a name for this vApp, select the virtual data center where you want to create this vApp, and specify your desired runtime lease and storage lease as shown in the following screenshot:

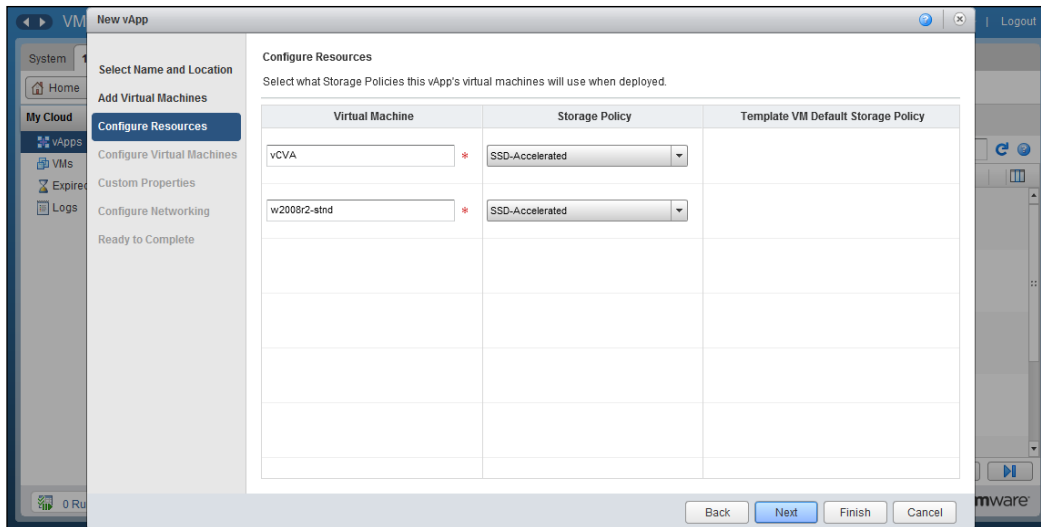


10. Click on **Next**.

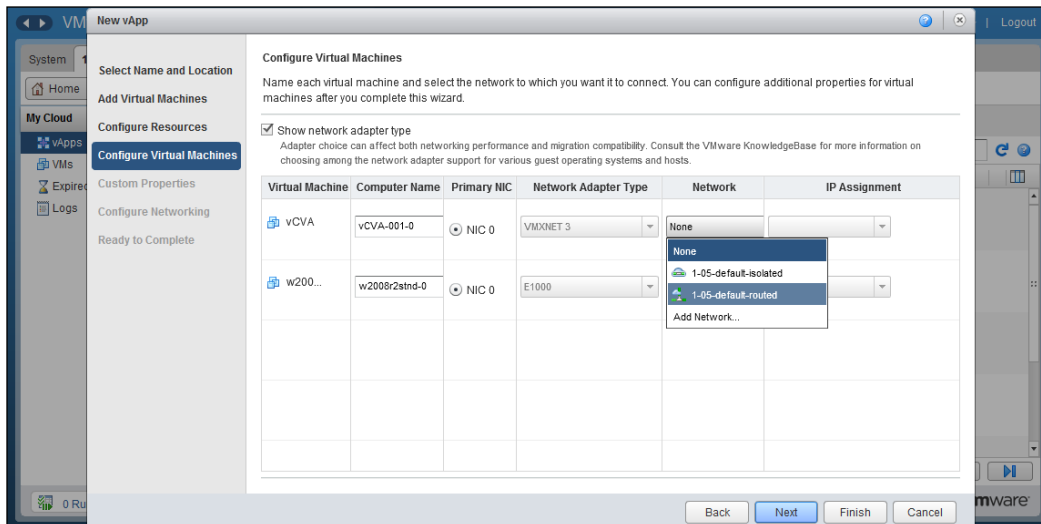
11. Under **Add Virtual Machines**, select **My Organization's Catalogs** from the **Look in** drop-down menu.
12. In the vApp template list, select your preferred vApp template and click on the **Add** button.
13. From the **Look in** drop-down menu, select **Public Catalogs**.
14. In the vApp template list, select your preferred vApp template from the catalog and click on the **Add** button. You can also create a new empty VM by clicking on **New Virtual Machine**, which can be seen in the following screenshot:



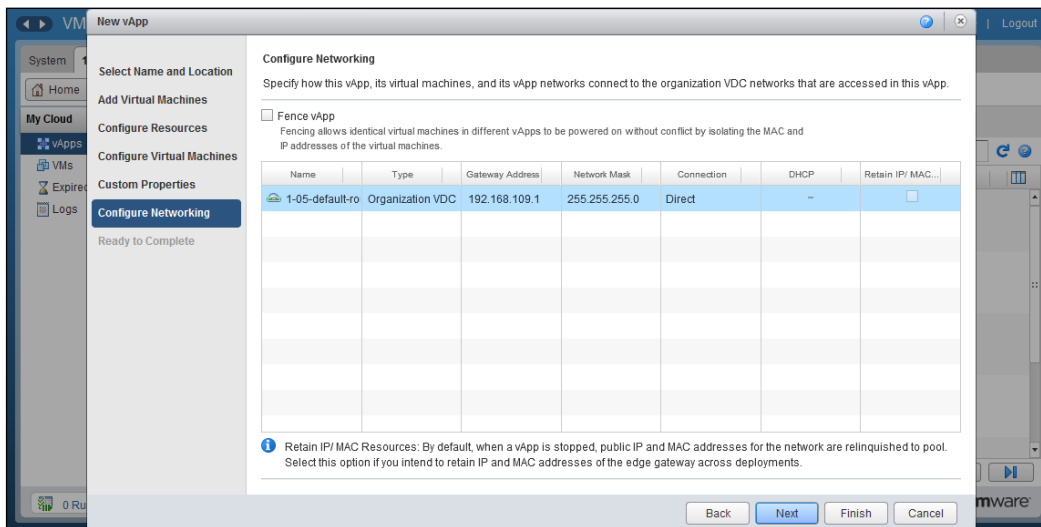
15. Click on **Next**.
16. In the **Configure Resources** section, specify the virtual machine name and choose the storage policy, which is essentially the storage profile attached to the virtual data center, as can be seen in the following screenshot:



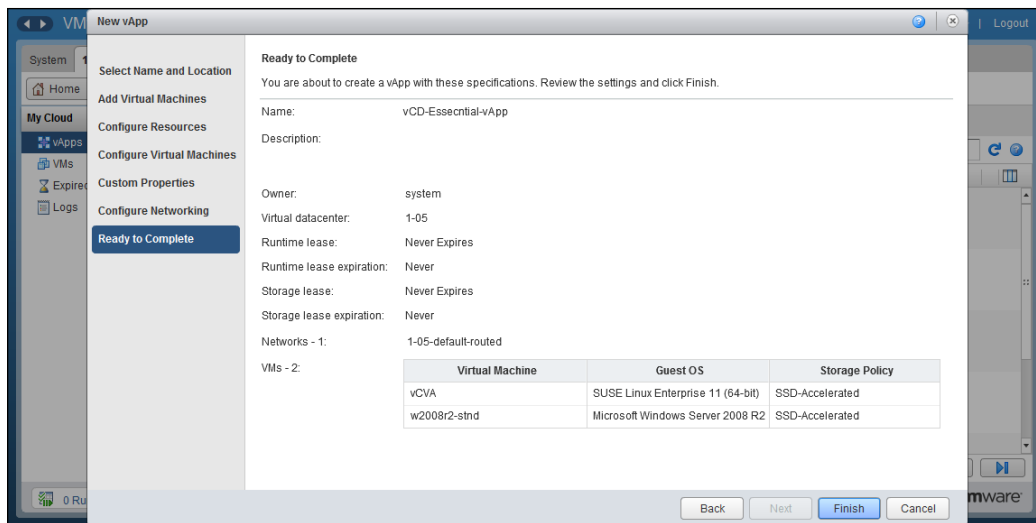
17. Click on **Next**.
18. In the **Configure Virtual Machines** section, specify the computer name under **Computer Name** for each virtual machine.
19. Select **Add Network** from the **Network** drop-down menu for the VM, and select the network where you want them to connect to. The following screenshot shows that we are connecting the VMs to a routed organization vDC network:



20. For both virtual machines, select **Static - IP Pool** from the **IP Assignment** drop-down menu.
21. Click on **Next**.
22. In the **Custom Properties** section, you don't need to specify anything as this is a multimachine vApp, and DNS, Default Gateway, and IP Addresses will be picked up from the routed network automatically. This is a new feature in vCD 5.5.
23. Click on **Next**.
24. Under **Configure Networking**, select the routed organization network, as shown in the following screenshot:

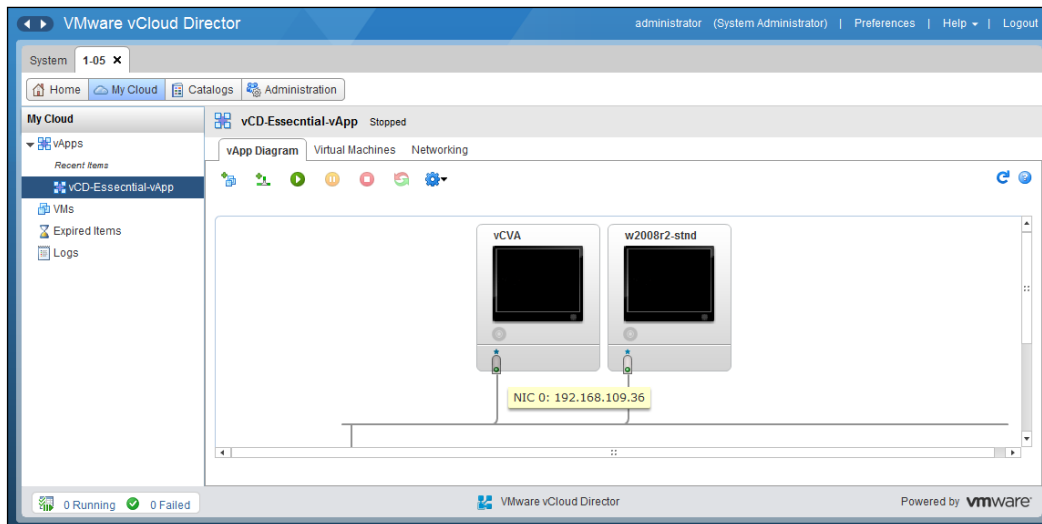


25. Click on **Next**.
26. Under **Ready to Complete**, click on **Finish**, as shown in the following screenshot:



Monitor the vApp status. Wait until the status changes to **Stopped** before continuing.

27. Right-click on this vApp and select **Open**.
28. In the right pane, click on the **vApp Diagram** tab. Scroll down so that all networks are visible.
29. Point to each NIC. Confirm that the IP address to be assigned is in the static IP pool for this network, which can be seen in the following screenshot:



To deploy a vCloud Director vApp in vCD, there are a couple of things you need to have. You need the organization vDC, the associated storage policy, and the leases for each instance of a vApp template deployed from a catalog. The selected vDC provides the compute and memory resources that are necessary to run the vApp and any network edge devices deployed by VMware vCloud Networking and Security. The lease cannot exceed the limit set in the organization's policy.

vApps can be copied between catalogs. While copying a vApp from a public catalog published by another organization, keep the following points in mind:

- The copied vApp networking can be configured for an entirely different topology. Networking settings such as DNS configuration, IP Address assignment, and other networking-related stuff might be inappropriate for running this copied vApp into a new organization.
- The guest customizations applied to the vApp might not meet organization standards. After copying a vApp from a public catalog, you may deploy a copy of the vApp to your My Cloud, then review and update the vApp configuration.
- After updating the configuration based on the organization topology and policies, you can republish the vApp to the catalog.

To ensure that the virtual machines in vApp templates are unique on deployment, vCloud Director includes the ability to customize guests directly from the organization web console. Customization occurs when you power on the virtual machine.

vCloud Director has the ability to customize the network settings of the guest operating system of a virtual machine when you create them from a vApp template. It is done in such a way that when you customize your guest operating system, you can create and deploy multiple unique virtual machines based on the same vApp template without a machine name or network conflicts, specifically the MAC address duplication.

To make it clearer to you, consider this: when you configure a vApp template and add all of the prerequisites for guest customization and add a virtual machine to a vApp based on that template, vCloud Director will create a package with guest customization tools. vCloud Director will copy that package, run the tools, and then delete the package from the VM when you deploy and power on the virtual machine for the first time.

Before vCloud Director can perform guest customization on virtual machines with Windows 2000, XP, or 2003 guest operating systems, a system administrator of VMware vCloud must create a corresponding Microsoft Sysprep deployment package in the vCloud Director deployment environment.

For each virtual machine in a vApp, you can change the hardware settings. You must have vApp author privileges and above to update or change the vApp hardware configuration.

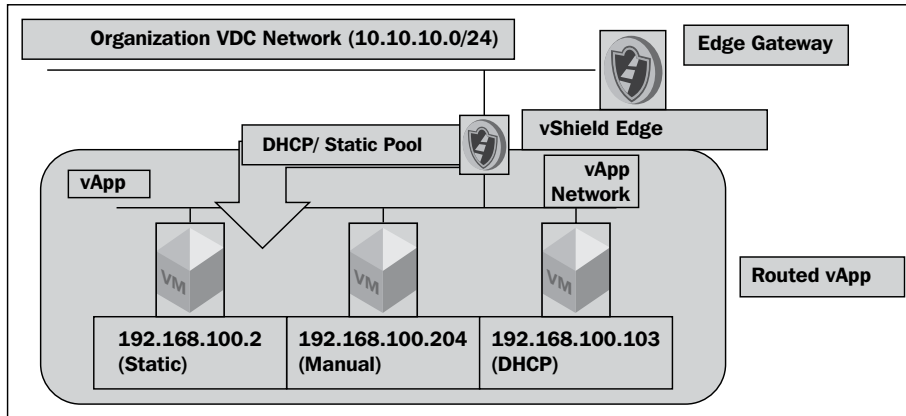
Creating a vApp or customizing a vApp does give you flexibility as to how you want to connect it to organization infrastructure. vApps typically connect to an organization vDC network, either through a routed vApp network edge or directly. To connect a vApp directly to an organization vDC network, you must select the **Add Network** option in the **Network** drop-down menu, and then select one or more existing organization vDC networks to be added to the vApp. After you have created or selected the vApp network configuration, you can configure IP parameters.

vCloud Director uses guest customization when it deploys virtual machines inside vApps to control IP addressing. Three types of IP addressing exist: static, manual, and DHCP.

The virtual machine guest operating system must be configured to receive a DHCP address. vCloud Director does not use guest customization to enforce the configuration of the virtual machine as a DHCP network client. If a virtual machine is set to use DHCP, you must either have the network VMware vShield device configured to support DHCP services, or you must directly attach the vApp network to a higher network that has an external DHCP server.

If a virtual machine has been assigned a DHCP address, you cannot configure an external **network address translation (NAT)** IP address on the organization vDC network.

Let's have a look at a routed organization vDC network, as shown in the following diagram:

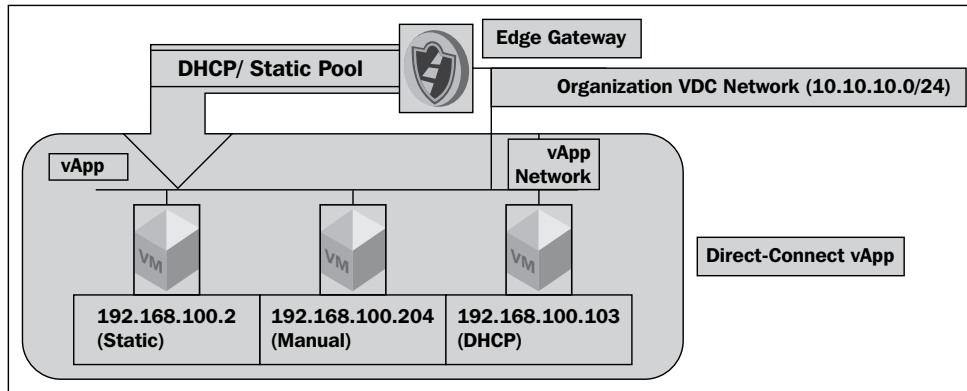


Static addressing is similar in operation to DHCP. When you create the network, you set a static range of IP addresses. vCloud Director pulls IP addresses out of the static range in a sequential order. Then, vCloud Director uses guest customization to manually set the IP address in the virtual machine to the selected static address.

Static addresses have a major advantage over DHCP. If you set a virtual machine to a static IP address, then vCloud Director assigns an external NAT IP address on the organization vDC network that the vApp is attached to. This automatic assignment of external NAT IP addresses greatly simplifies NAT operations.

Manual IP addresses are where vCloud Director uses the address that the administrator manually specifies for a virtual machine. vCloud Director uses guest customization to configure the IP address in the virtual machine. If a virtual machine has a manual IP address assigned, it does not automatically receive an external NAT IP address on the organization vDC network. However, the vCloud Director administrator can manually set the external NAT IP address for a virtual machine with a manual IP address configuration.

Let's have a look at a Direct Connect vApp network, which is shown in the following diagram:

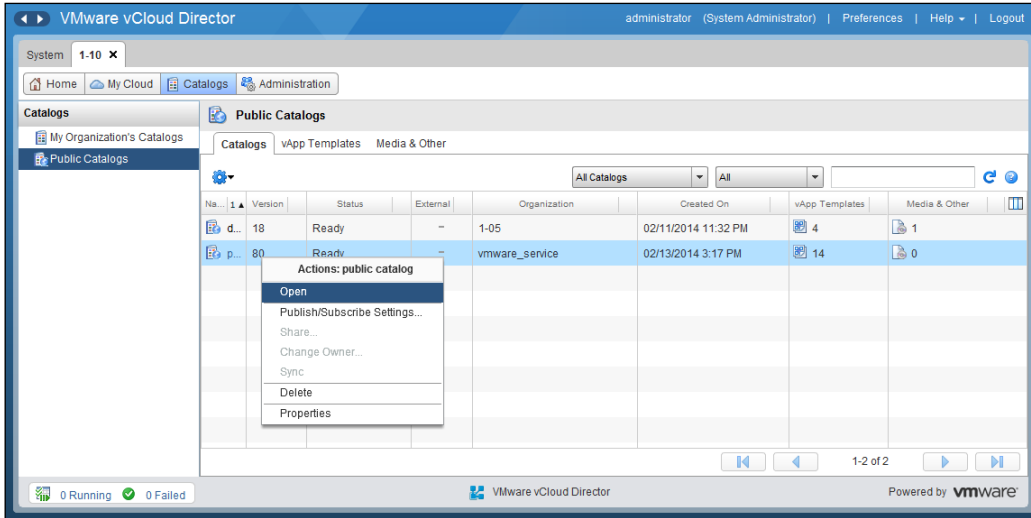


Now let's look at how to deploy a vApp. In this task, we will copy a vApp published by another organization and configure and run the vApp. Usually, in your VMware vCloud Director environment, at least one organization shares a master catalog that is visible to the organization administrators of all organizations.

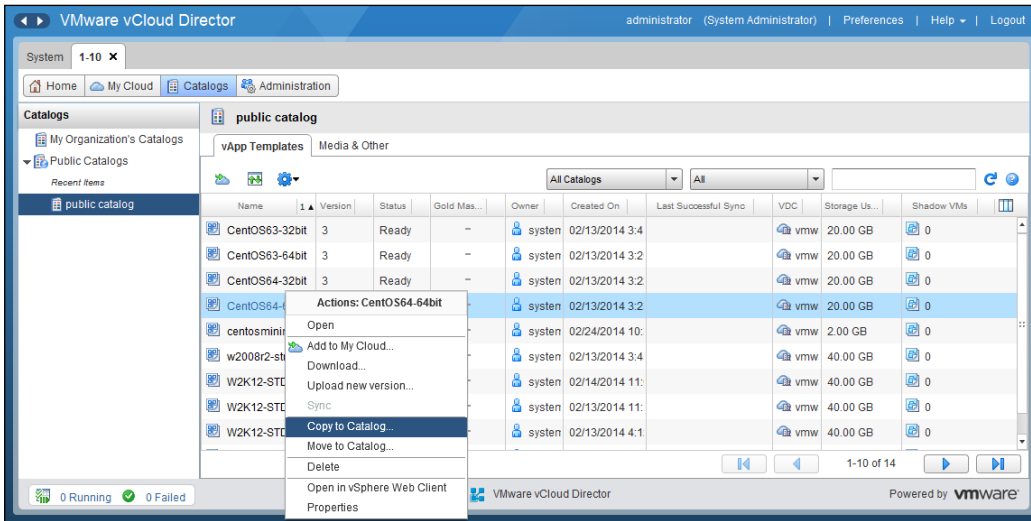
Although you can deploy a vApp to your `My Cloud` folder, the following steps will guide you through copying the vApp to your own catalog before deployment:

1. Start the Internet Explorer browser. Type in the URL of the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.
3. On the home screen, click on the **Manage & Monitor** tab.
4. In the left pane, click on **Organizations**.
5. In the right pane, right-click on your desired organization and click on **Open**. This is shown in the next screenshot.
6. Click on the **Catalogs** tab.
7. In the left pane, click on **Public Catalogs**.
8. In the right pane, click on the **Catalogs** tab.

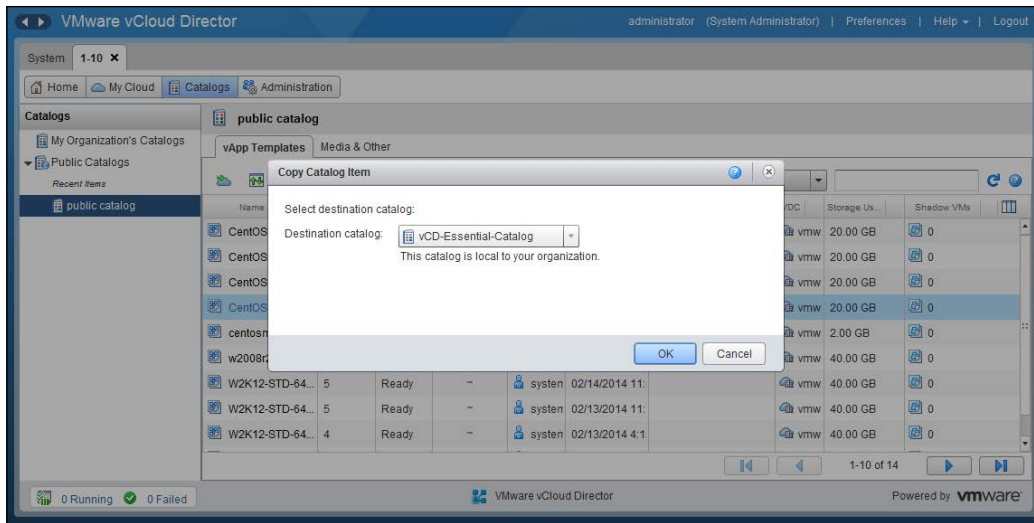
- Right-click on your desired public catalog and click on **Open**, as shown in the following image:



- On the **vApp Templates** tab, right-click on your desired vApp template that you want to copy and click on **Copy to Catalog**, as shown in the following screenshot:

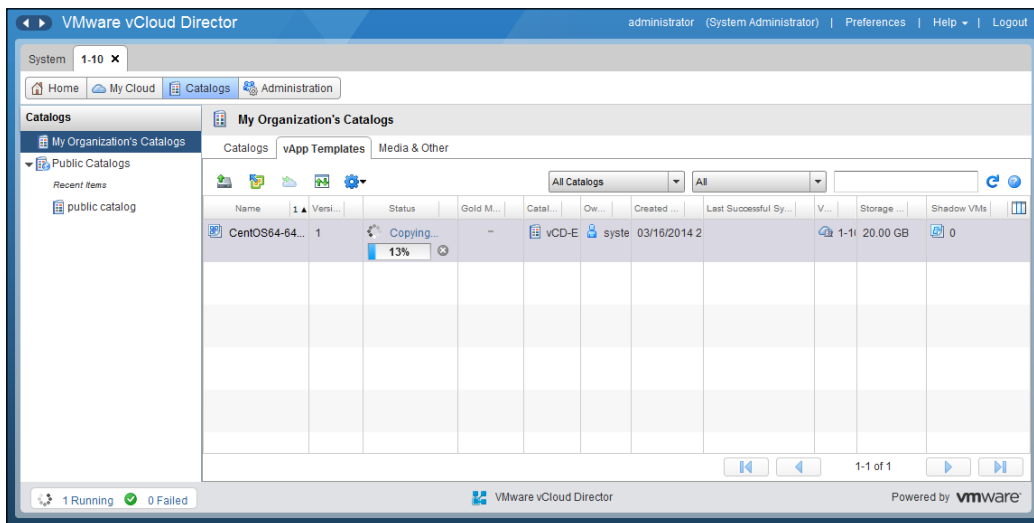


- Select your desired destination catalog as the destination and click on **OK**, as shown in the following screenshot:

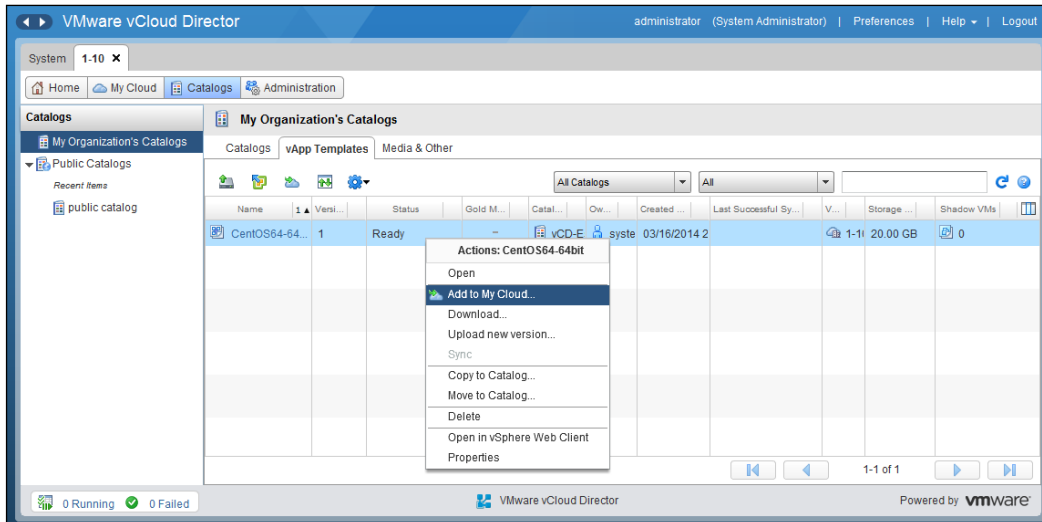


12. In the left pane, click on **My Organization's Catalogs**.

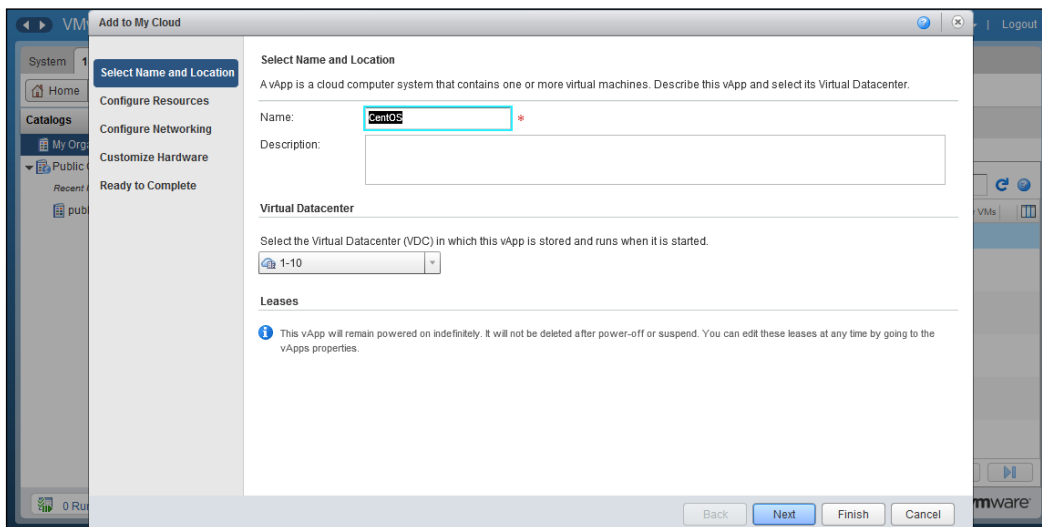
13. In the right pane, monitor the status. Wait until the status changes to **Ready** before continuing, as you can see in the following screenshot:



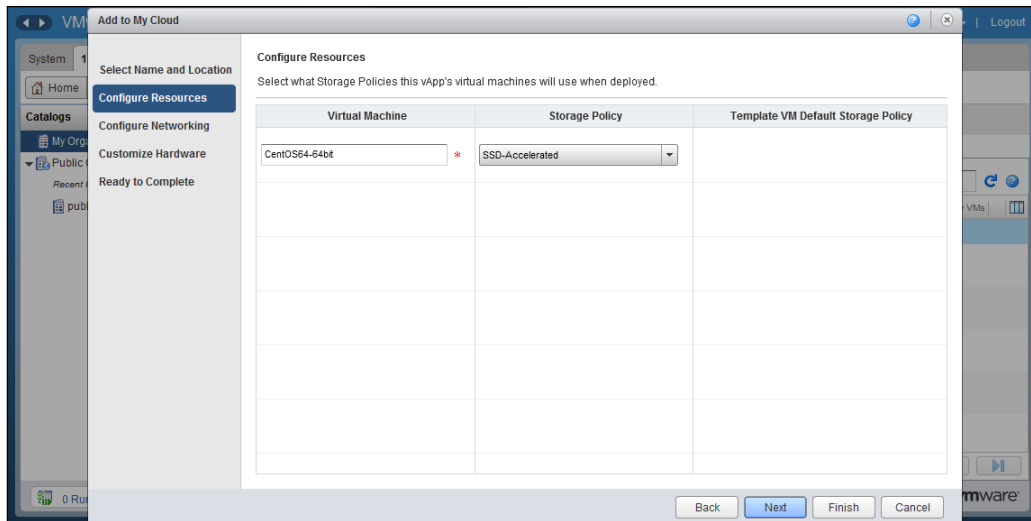
14. Right-click on the recently copied vApp template and click on **Add to My Cloud...**



15. In the **Select Name and Location** section, choose your desired name.
16. Choose the virtual datacenter where this vApp is going to be added and click on **Next**. Your screen will look similar to the following screenshot:

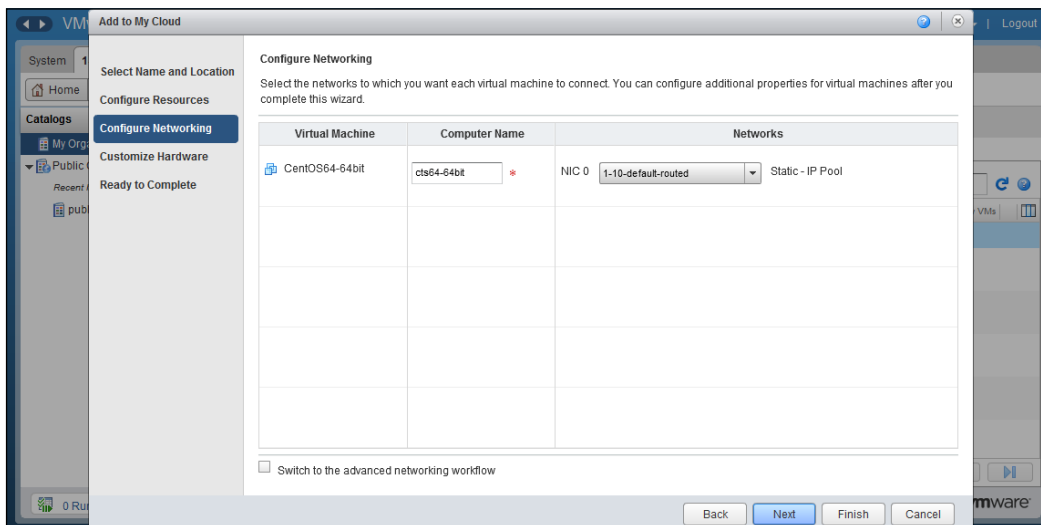


17. In the **Configure Resources** section, specify a virtual machine name and storage policy as shown in the following screenshot:



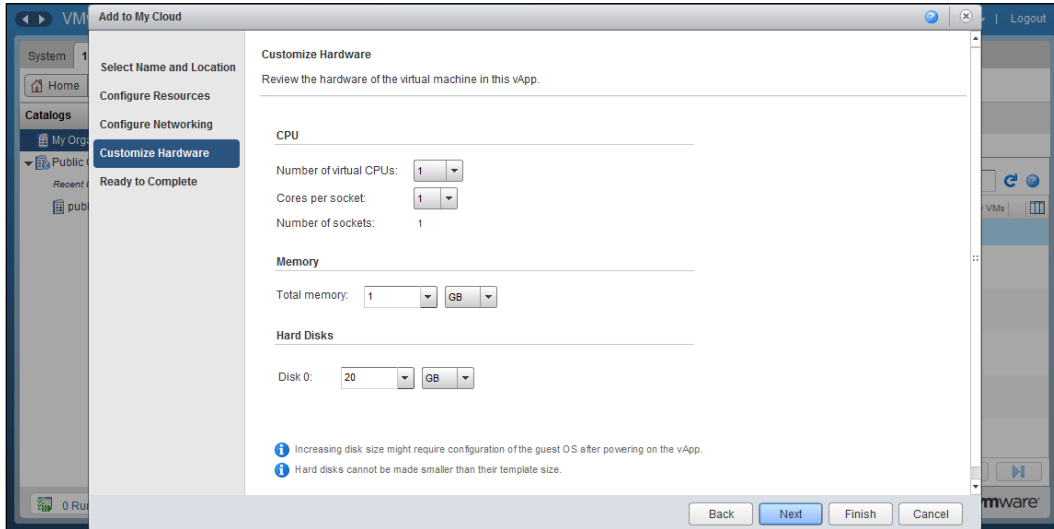
18. Click on **Next**.

19. In the **Configure Networking** section, specify a computer name, assign a vDC-routed organization network from the drop-down menu, and click on **Next**, as shown in the following screenshot:

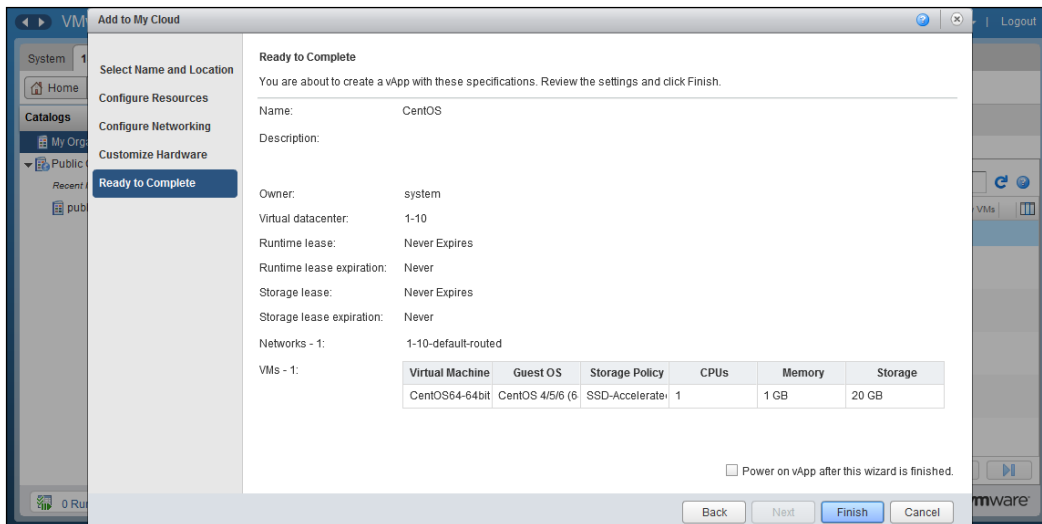


20. In the **Customize Hardware** section, you may wish to change the sizes of the CPU, memory, and hard disk.

21. Click on **Next** as shown in the following screenshot:



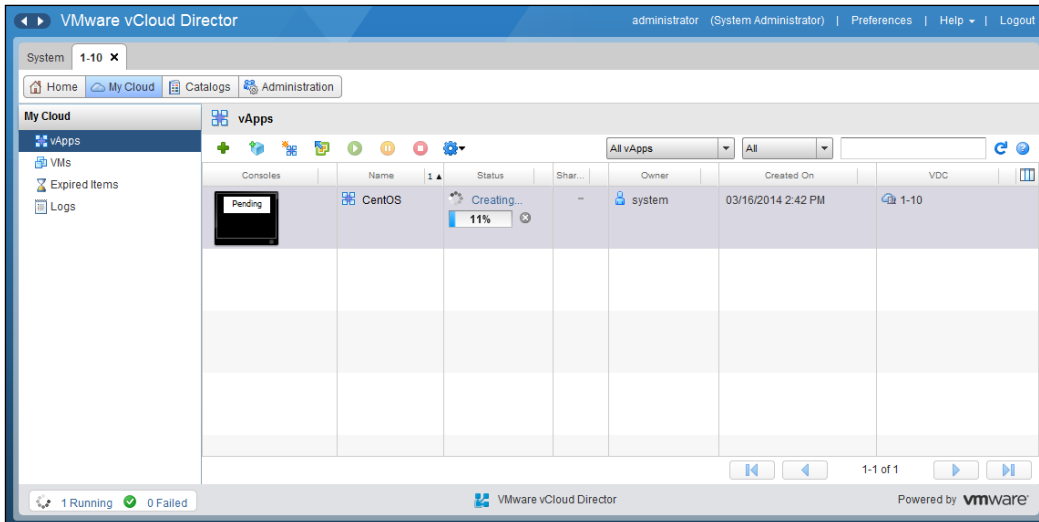
22. As shown in the following screenshot, review the information and click on **Finish**:



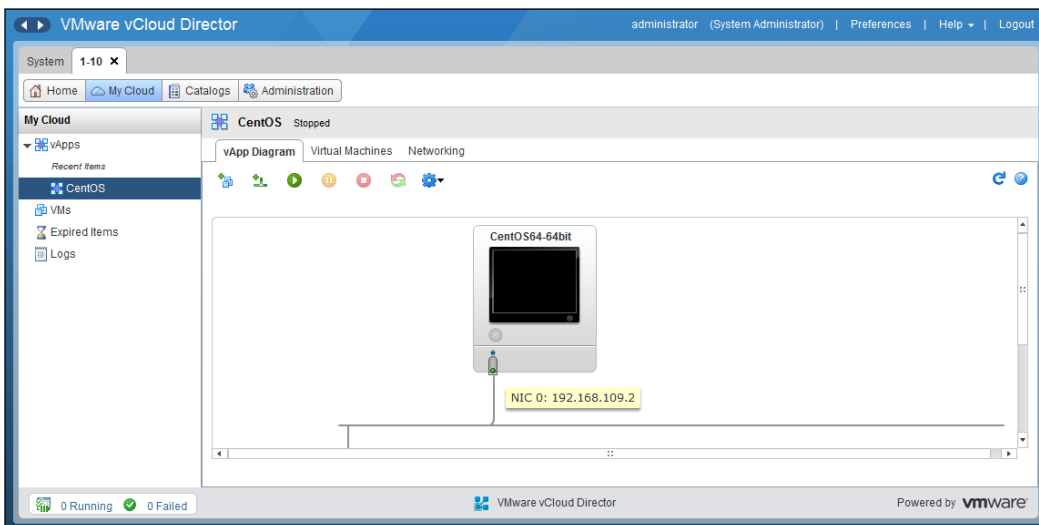
23. Click on the **My Cloud** tab.

24. In the left pane, click on **vApps**.

25. In the right pane, monitor the status. Wait until the status changes to **Stopped** before continuing, as shown in the following screenshot:



26. Right-click on this deployed vApp and click on **Open**.
27. Click on the **vApp Diagram** tab and scroll down so that all networks are visible, which you can see in the following screenshot:



Understanding catalogs

vCloud Director includes a content repository, which is a component in the vCloud Director storage. The content repository provides an abstraction to the underlying datastores and offers features to store, search, retrieve, and remove content.

Content is delivered to consumers in the form of catalogs. A catalog is a container for vApp templates and media files in an organization. In vCD 5.5, it's any file in the catalog. Catalogs can be shared, so the vApp templates in them are available to other users in the organization. Catalogs can also be published so that members of other organizations can have read access to the vApps, provided the organization is configured to allow publishing.

Catalogs are made available in four ways:

- **Private:** This is available to the owner or creator of the catalog only
- **Public:** This is available to other organizations in the cloud
- **Shared:** This is available to other specific users in your organization or available to other organizations in your cloud
- **Published:** This is available to subscribers in other vCloud Director clouds

The vCloud system administrator has to allow or disallow public sharing and publishing of organization catalogs. If this is shared, the organization catalogs can be shared as visible to other organizations. Catalogs can be made public to specific organizations or to all organizations. Catalogs can still be shared within an organization even if sharing with other organizations is not allowed. Sharing can be set or changed at any time.

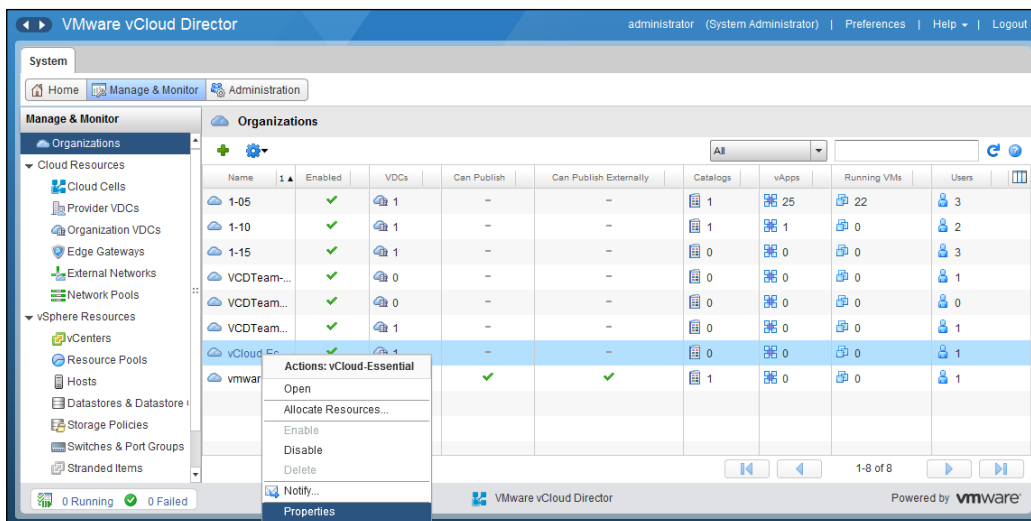
Publishing allows a catalog to be shared with organizations in other vCloud Director clouds. The system administrator also controls whether an organization can subscribe to catalogs that are externally published. Publishing can be set or changed at any time.

As a best practice, you should create an administration organization and share public catalogs that offer official build templates to the organization administrators of all organizations. As a consumer, other organization administrators should create a shared catalog for local templates and use the shared catalog provided by the administrative organization to create standard templates.

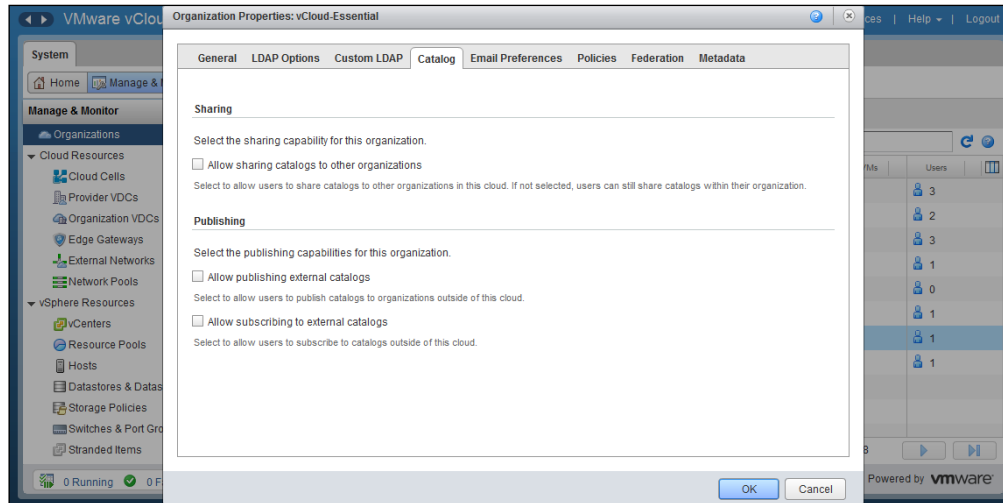
Creating and configuring a catalog

This section assumes that you already have an organization created and now want to change the options for catalog publishing:

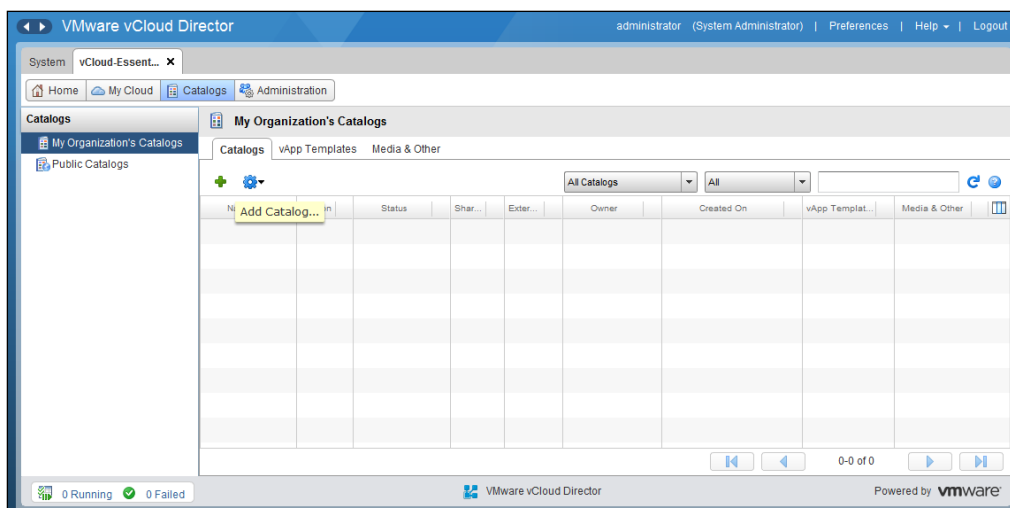
1. Start a browser. Type the URL of the vCD server in it. An example could be `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.
3. On the home screen, click on **Manage & Monitor** tab.
4. In the left pane, click on **Organizations**.
5. In the right pane, right-click on your desired organization and select **Properties**. This is shown in the following screenshot:



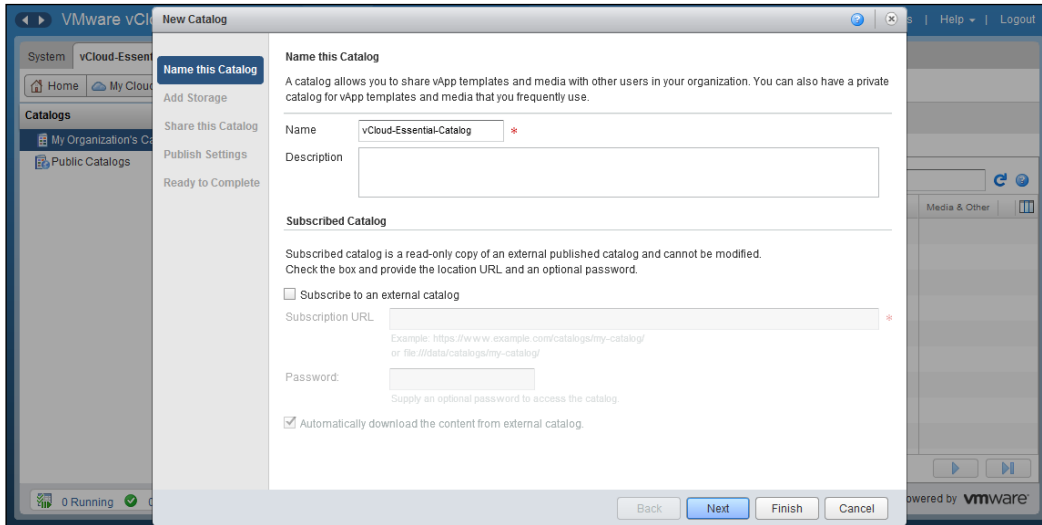
- Click on the **Catalog** tab, and you should see the **Sharing** and **Publishing** options as shown in the following screenshot:



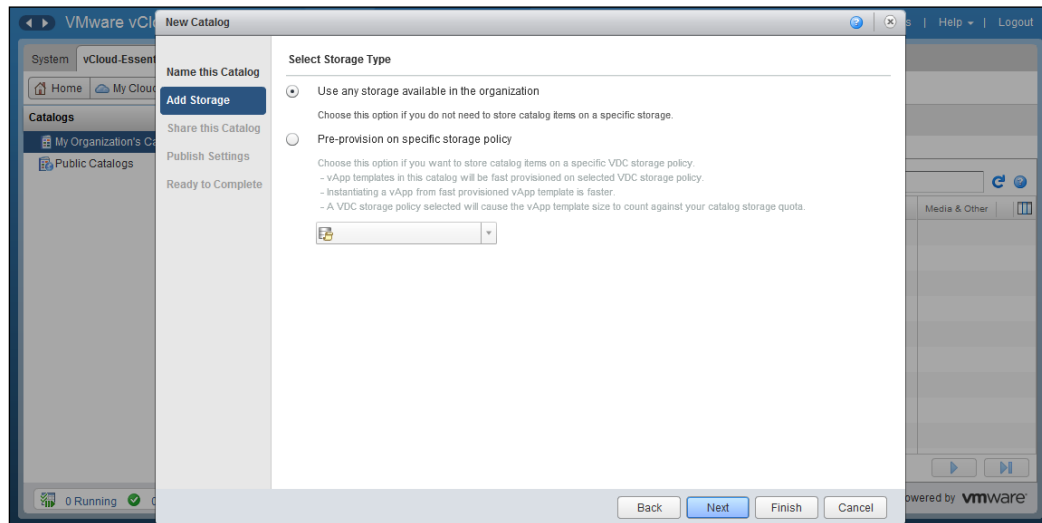
- Under **Sharing**, select **Allow sharing catalogs to other organizations**.
- Under **Publishing**, select **Allow publishing external catalogs** and **Allow subscribing to external catalogs** and click on **OK**.
- Right-click on the organization and click on **Open**.
- Click on the **Catalogs** tab.
- Click on the green **+** sign to add catalogs, as shown in the following screenshot:



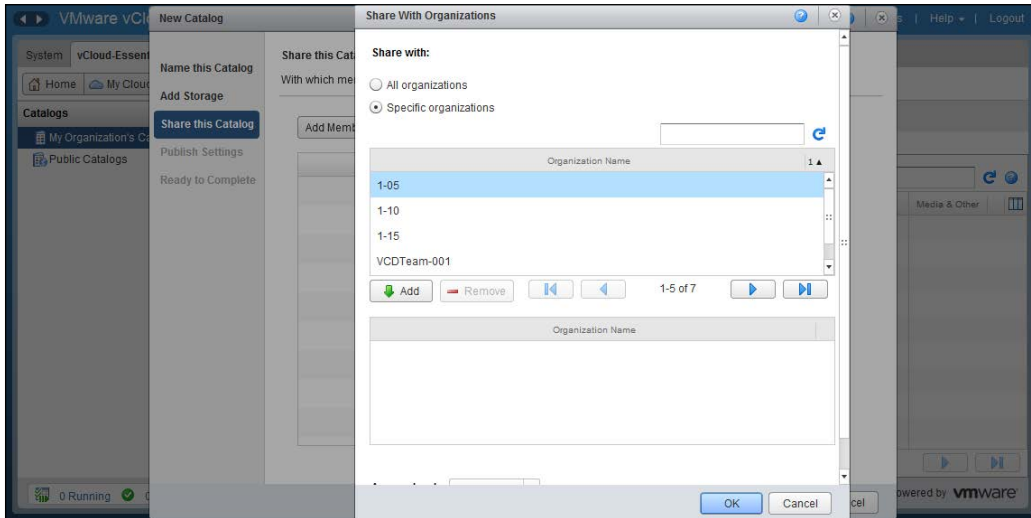
12. In the **Name this Catalog** tab, specify a catalog name in the **Name** textbox.
13. Under **Subscribed Catalog**, keep the option unselected. Click on **Next** as shown in the following screenshot:



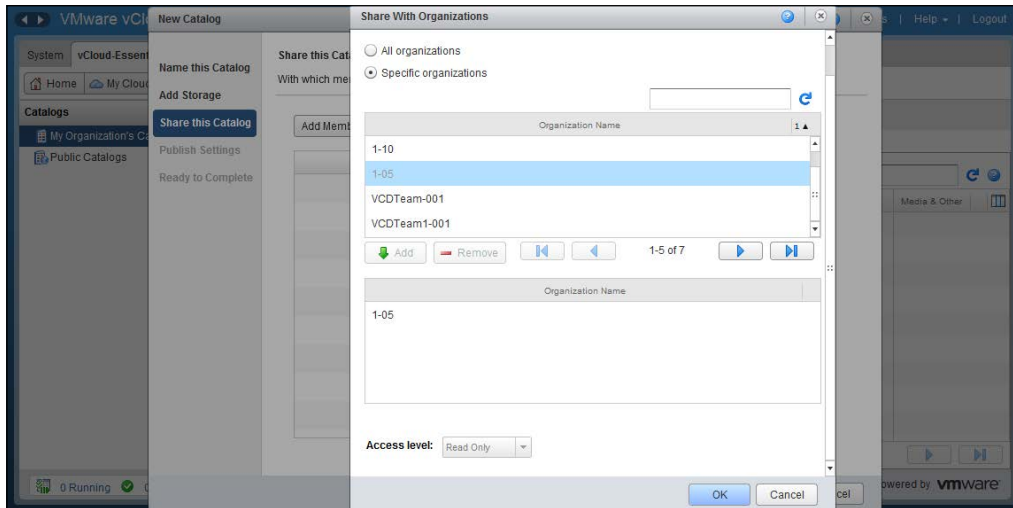
14. Under **Select Storage Type**, select **Use any storage available in the organization**.
15. Click on **Next** as shown in the following screenshot:



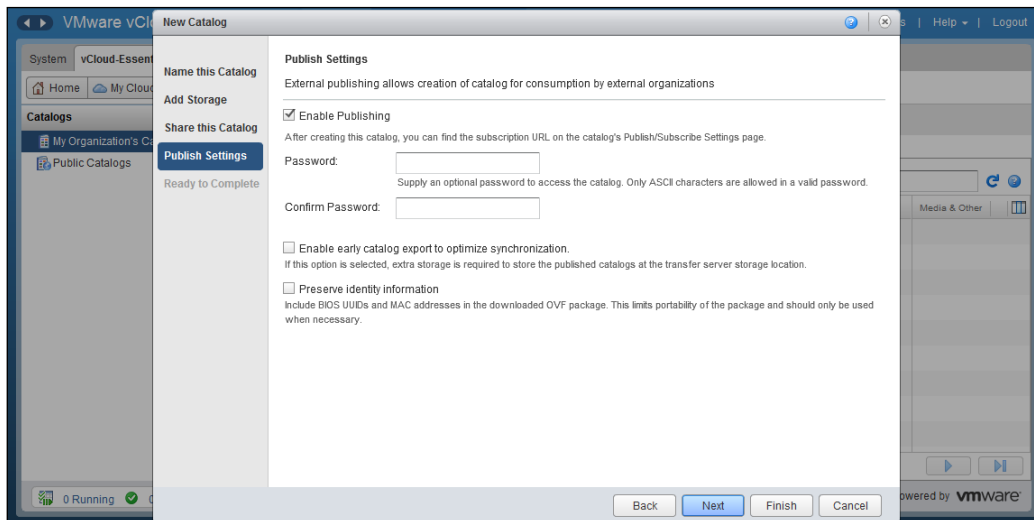
16. In the **Share this Catalog** section, you need to either add members you want to share or add an organization to share this catalog with. In this example, we will add an organization. Click on the **Add Organizations** button.
17. Select the **Specific organizations** radio button and select a specific organization from the list, as shown in the following screenshot:



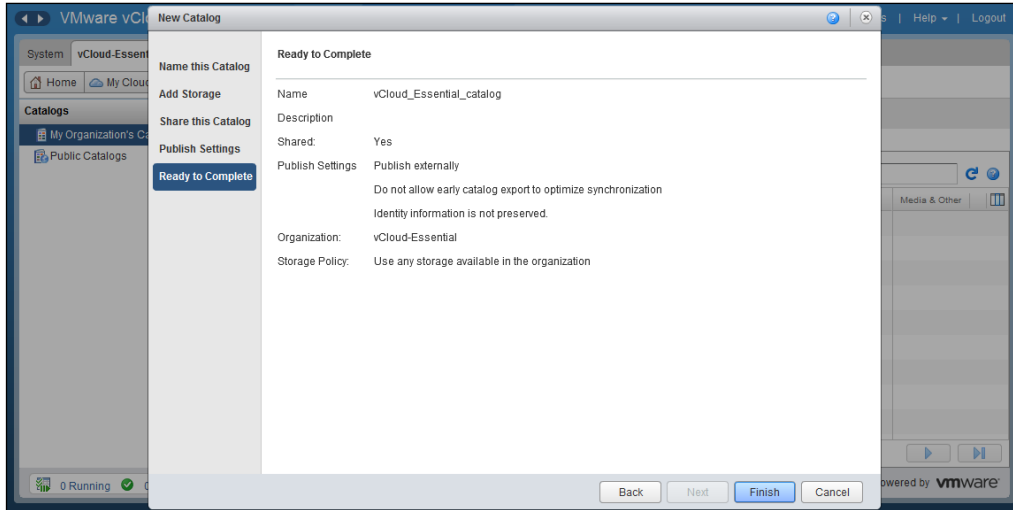
18. Click on **Add**.
19. Click on **OK**. This is shown in the following screenshot:




20. Under **Publish Settings**, select **Enable Publishing**.
21. Optionally, you can choose a password here.
22. Leave **Enable early catalog export to optimize synchronization** deselected; otherwise, it will start an OVA export and the OVA will sit in the transfer directory until its downloaded, which translates to a huge requirement of space.
23. Leave **Preserve identity information** deselected and click on **Next** as shown in the following screenshot:



24. Under **Ready to Complete**, review the information and click on **Finish**. This is shown in the following screenshot:



 When you use publishing, the OVA exports go via the transfer directory. Also, you need a lot more space in it.

Understanding vApp templates

vCloud Director offers several ways to populate catalogs with vApp templates and media. These options are available based on user roles and their associated rights. For example, only system administrators can import a virtual machine or media file from vSphere.

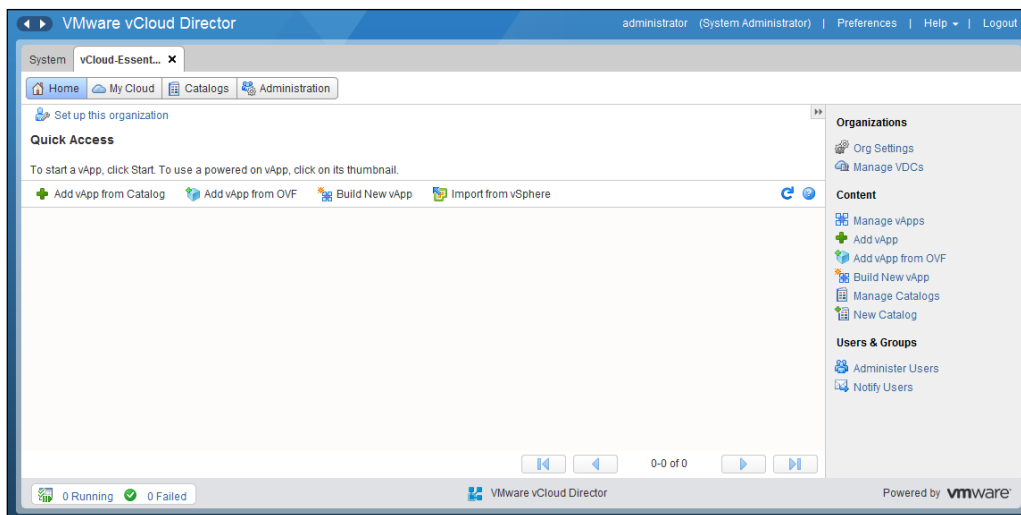
You can deploy an OVF template in vSphere and then import the resulting virtual machine as a vApp (in **My Cloud**) or vApp template in an organization catalog. The system administrator can import from vSphere; however, any organization administrator can export and import only OVF/OVA.

Not all vSphere OVF templates can be imported directly into vCloud Director. A user with sufficient privileges can upload an OVF template that is stored on their desktop computer to an organization catalog, or in vCD 5.5 to a vApp, or My Cloud as a vApp template.

Importing an OVF as a template

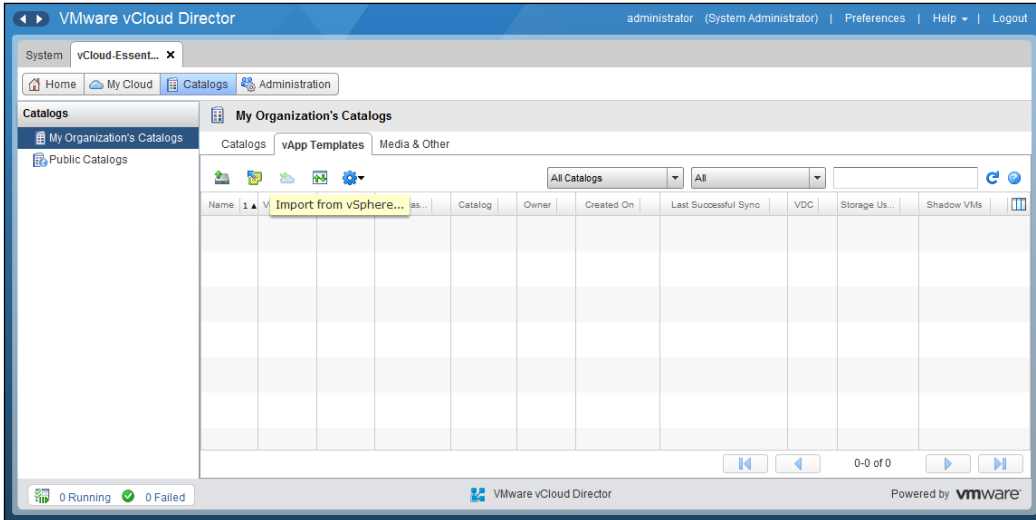
In this task, we will see how to import a vSphere virtual machine and also how to upload an OVF file and import it as template.

1. Open a browser. Type the URL of the vCD server into it. An example would be `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.
3. On the home screen, click on the **Manage & Monitor** tab.
4. In the left pane, click on **Organizations**.
5. In the right pane, right-click on your desired organization and click on **Open**. This is shown in the following screenshot:

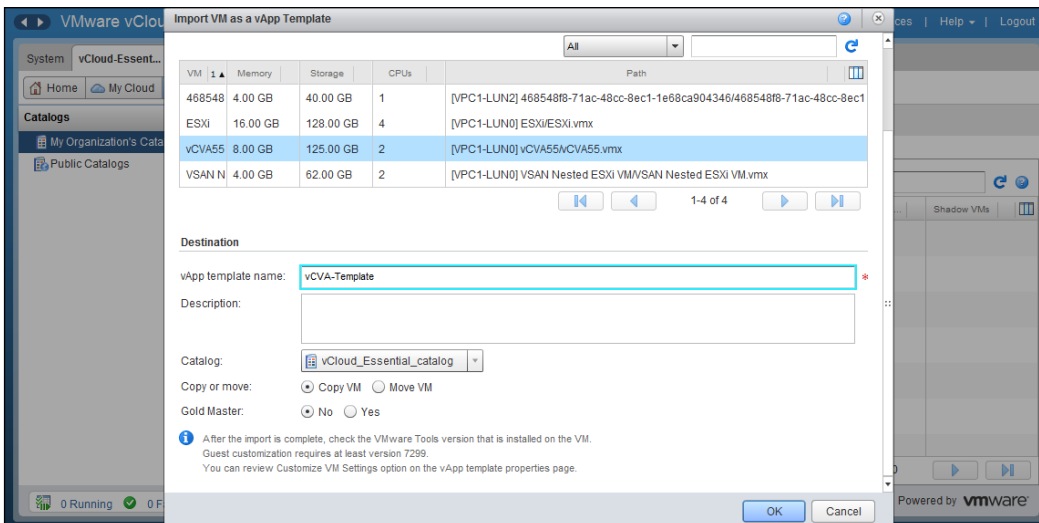


6. On the organization home page, click on the **Catalogs** tab.
7. In the right pane, click on the **vApp Templates** tab

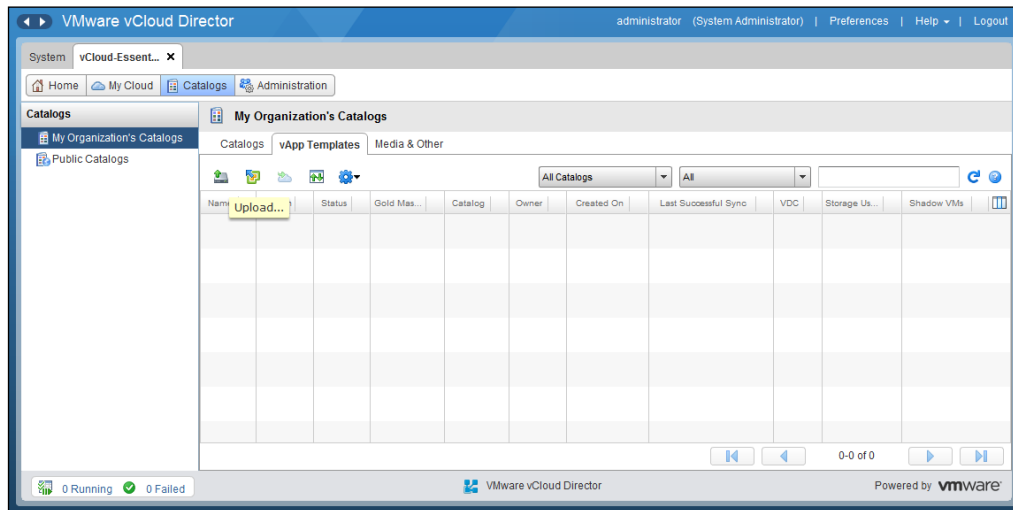
- Click on the **Import from vSphere** icon, as shown in the following screenshot:



- In the **Import VM as a vApp Template** wizard, choose the vCenter it is backing, select the particular VM, specify a vApp template name, specify description, keep the specified catalog, select **Copy** from **Copy or move**, and assign **Gold Master** as **No**.
- Click on **OK** as is shown in the following screenshot:



11. Monitor the status. Wait until the status changes to **Ready** before continuing.
12. For uploading an OVF file as a vApp template, click on the **vApp Templates** tab in the right pane and click on the **Upload** icon. This is shown in the following screenshot:



13. In the **Upload OVF package as a vApp Template** panel, click on **Browse**.
14. In the **Open file** window, select your OVF and click on **Open**.
15. In the **Name** textbox, specify a name.
16. In the **Description** textbox, specify a description.
17. From the **Catalog** drop-down menu, select the catalog where you want to upload this OVF to.
18. Click on **Upload**.
19. Monitor the running status of the upload using the **Transfer Progress** window. If the **Transfer Progress** window has not opened, click on the **Gear** icon and select **View uploads and downloads**.
20. When the transfer is complete, close the **Transfer Progress** window by clicking on **Close**.

Summary

In this chapter, we covered some aspects in implementing vCloud Director. We discussed how to create and deploy a vApp and how to create and share catalogs. Also, we went through how to create vApp templates using various options.

In the next chapter, we will see how to create and replace SSL certificates for vCloud Director. We will also go through the procedures of configuring and managing vCD access control.

6

Managing Security

VMware vCloud Director secures client server communication using SSL. If you wish to secure the connection of vCloud Director, then you need to create two certificates for each vCloud Director cell in the group. Then, you need to import those certificates into the host KeyStores before you can install and configure a vCloud Director server group.

So, in a nutshell, each vCloud Director cell in a cluster requires two SSL certificates, one for each of its IP addresses (web portal and console proxy).

All the directories in the pathname of the SSL certificates must be readable by the user: `vc1oud.vc1oud`. This user is created by the vCloud Director installer.

This chapter will cover the following topics:

- Creating and processing certificate requests
- Configuring and managing vCloud Director access control

Creating and processing certificate requests

If your vCloud Director environment does not require high-class security and trust concerns are minimal, then self-signed SSL certificates are your best bet. If you require high-class security, then a certified authority certificate needs to be used.

Each vCloud Director cell requires two SSL certificates. This is because they have two IP addresses for connectivity. These certificates will be stored in a Java KeyStore file. You can either use a certificate that is signed by a trusted certification authority or a self-signed one. However, third-party-trusted signed certificates provide the highest level of trust, as a 2048-bit key length provides a high level of security; however, they also cost a lot of money or require an internal CA.

Creating a self-signed certificate

Before you generate self-signed SSL certificates, you need to make sure all of the following prerequisites are met:

- Ensure that the vCloud Director cell has Java 6 Runtime Environment installed prior to creating the certificates. JRE 6 enables the `keytool` command to create the certificate.
- List the IP address, which is set in the vCD cell. You can use the `ifconfig` command to get the IP address's configuration.

Let's look at how to create a self-signed SSL certificate:

1. Log in to the vCloud Director cell using SSH. You should use root credentials.
2. Change the directory to `/opt/vmware/vcloud-director/jre/bin/` using the following command:

```
# cd /opt/vmware/vcloud-director/jre/bin/
```
3. To create an untrusting self-signed certificate for the HTTP service, run the following command, which will create an untrusting certificate in a KeyStore file named `certificates.ks`:

```
# keytool -keystore certificates.ks -storetype JCEKS -storepass  
passwd -genkey -keyalg RSA -alias http
```

4. Answer the `keytool` questions. When the `keytool` asks for your first and last names, type the fully qualified domain name associated with the IP address you want to use for the HTTP service, for example, `testcloud.vcloud.xyz.com`.

For the remaining questions, provide answers that are appropriate to your organization and location.

5. Create a certificate-signing request for the HTTP service. The following command creates a certificate-signing request in the `http.csr` file:

```
# keytool -keystore certificates.ks -storetype JCEKS -storepass  
passwd -certreq -alias http -file http.csr
```
6. Create an untrusting certificate for the console proxy service. The following command adds an untrusting certificate to the KeyStore file created in step 3:

```
# keytool -keystore certificates.ks -storetype JCEKS -storepass  
passwd -genkey -keyalg RSA -alias consoleproxy
```

- To verify whether the certificates are imported, list the contents of the KeyStore file. You can see two certificates are being listed: `http` and `consoleproxy`. To do this, run the following command:

```
# keytool -storetype JCEKS -storepass vmware -keystore /tmp/
certificates.ks -list
```

The results will look like the following.



```
[root@cis-se-lab-vpc1-vcd bin]# ./keytool -storetype JCEKS -storepass vmware -keystore /tmp/certificates.ks -list
Keystore type: JCEKS
Keystore provider: SunJCE
Your keystore contains 2 entries
consoleproxy, Sep 16, 2013, PrivateKeyEntry,
Certificate fingerprint (MD5): 26:58:7A:98:80:81:22:58:28:27:8B:40:8A:07:29:76
http, Sep 16, 2013, PrivateKeyEntry,
Certificate fingerprint (MD5): 91:35:D7:2B:D0:0F:0A:63:AF:6B:54:54:72:4D:F0:0F
[root@cis-se-lab-vpc1-vcd bin]#
```

- You can append a `-v` parameter to the end of the `keytool -list` command to see more verbose information about the certificates. The verbose output provides additional information such as the expiry or validity date of the certificate.

By default, self-signed certificates are valid for 90 days. To increase the duration, add the switch `-validity <number_of_days>` while creating your certificate.

If you are using self-signed SSL certificates, you can either change the certificate at any time or upgrade them to signed SSL certificates to have a high level of trust. However, when vCD is attached to any third-party tool with the old certificates, you need to reconnect it to get the new certificate in effect.

In this section, we learned how to create and process self-signed certificates. In the next section, we will discuss how to replace the certificates.

Replacing certificates in vCloud Director

The vCloud Director configuration script (`/opt/vmware/vcloud-director/bin/configure`) allows you to replace or upgrade the SSL certificates in a vCloud Director cell. Where vCloud Director is already configured, the script validates the database connection details and prompts for SSL certificate information. However, it skips all the other configuration steps so that the existing configuration is not modified.

Before you replace the existing certificates or upgrade them to externally signed certificates, you need to perform the following few things as prerequisites:

- Stop the vCloud Director service on each of those servers, the certificates of which you want to replace. This was discussed in *Chapter 1, Configuring and Maintaining vCloud Director*.
- Obtain the location and password of the KeyStore file that includes the SSL certificates for this server. This has been discussed in the preceding section.
- Obtain the password for each SSL certificate.

Let's look at how to replace a default SSL certificate:

1. Log in to the vCloud Director machine cell using SSH. You should use root credentials.
2. Change the directory to `/opt/vmware/vcloud-director/bin` using the following command:

```
# cd /opt/vmware/vcloud-director/bin
```
3. Shut down the vCloud Director service on the server by running the following command:

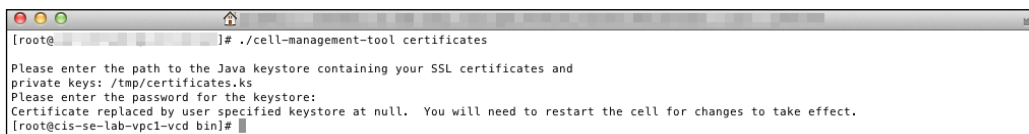
```
# ./cell-management-tool -u username -p password cell -s
```

More on the vCD cell maintenance tasks was discussed in *Chapter 1, Configuring and Maintaining vCloud Director*.
4. Run the configuration script on the server as follows:

```
# /opt/vmware/vcloud-director/bin/configure
```
5. Specify the full path to the Java KeyStore file that holds the new certificates.
6. Enter the KeyStore and certificate passwords.
The configuration script replaces the certificates and restarts the vCloud Director service on the server.
7. You can also use a cell management tool to replace an SSL certificate. To do this, run this command:

```
# ./cell-management-tool certificates
```

The output will look like the following.



```
[root@cis-se-lab-vpcli-vcd bin]# ./cell-management-tool certificates
Please enter the path to the Java keystore containing your SSL certificates and
private keys: /tmp/certificates.ks
Please enter the password for the keystore:
Certificate replaced by user specified keystore at null. You will need to restart the cell for changes to take effect.
[root@cis-se-lab-vpcli-vcd bin]#
```

In this section, we discussed how to replace certificates in vCloud Director. In the next section, we will discuss how to configure and manage vCloud Director access control.

Configuring and managing vCloud Director access control

Lightweight Directory Access Protocol (LDAP) is an application protocol that helps users in accessing and maintaining the directory information with the help of an IP network.

To provide centralized authentication for a vCloud organization, use an LDAP service to provide a directory of users and groups to import into an organization. While individual users can be created for each organization inside vCloud Director, which can be tedious. LDAP provides an integrated directory of users for an organization. The only caveat is that LDAP options can only be set by a system administrator and cannot be modified by an organization administrator.

LDAP can provide you with multiple methods of authentication, but this totally depends on the type of LDAP server you are connected to. You can have different LDAPs for different organizations. A system administrator should import the users and groups into the organization, and they should assign them with roles before they can be used.

A system administrator needs to import users. vCloud Director does not automatically import all the users and groups from the LDAP source. The authentication credentials of the imported users will be validated by the LDAP source through vCloud Director. Only the users imported to a vCloud Organization will be authenticated.

vCloud Director does not support hierarchical domains, and it does not have access to the LDAP directly. So, vCloud Director cannot change or edit any user details in the LDAP other than importing them into vCloud, and this is why you can also use SSO with it.

LDAP systems can provide a great deal of user details: name, e-mail, address, and so on. vCloud Director synchronizes this information for the imported users. The period of synchronization must be configured by either the system administrator or the organization administrator.

Though you can use LDAP at both the system and organization level, VMware recommends that you create at least one system user to mitigate the risk of having the LDAP system offline and not being able to authenticate and manage the system.

There are two ways to configure LDAP authentication: Simple and Kerberos. A simple authentication sends a user's **distinguished name (DN)** and a password to the LDAP server. The LDAP server will then allow you to execute searches on the information in the LDAP directory.

Kerberos is a ticket-based system for authentication between the client and server. With Kerberos, both the client and server need to prove their identity to each other. Kerberos uses symmetric key cryptography and can also leverage public key cryptography.

Configuring organization access

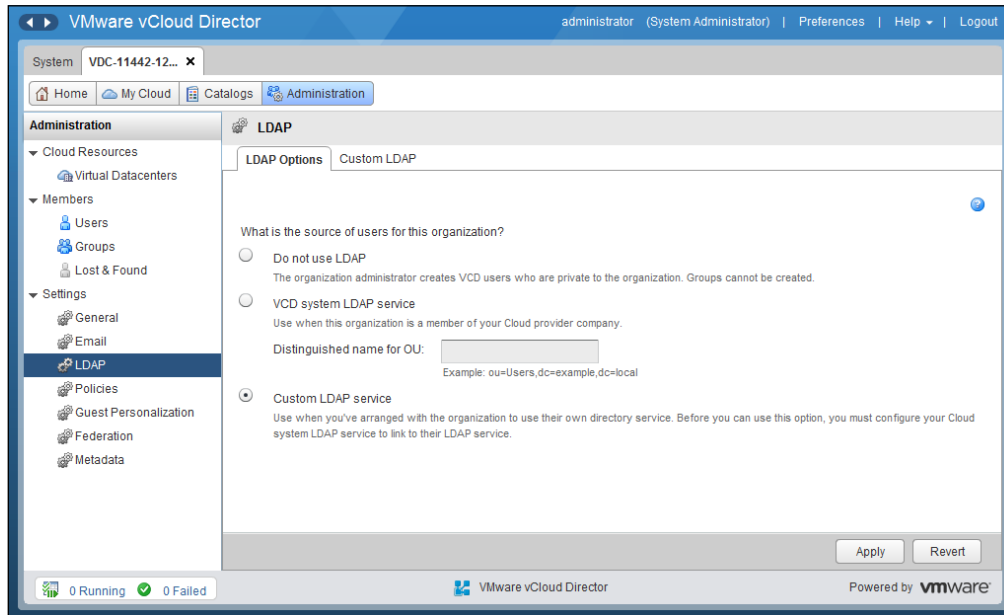
vCloud Director presents three options to configure LDAP on an organization. They are as follows:

- **Do not use LDAP:** This does not connect to any LDAP. All of the users in this organization are internally defined in the vCloud Director system.
- **Use the vCloud Director System LDAP service:** The organization leverages the LDAP service that has been configured at the system level. In order to leverage the system-defined LDAP, all organization users must be defined in the same **organization unit (OU)** in the LDAP database.
- **Use a custom LDAP server:** A custom LDAP server allows an organization to use its own LDAP service.

Perform through the following steps to configure LDAP in vCloud Director:

1. Open a browser. Go to the URL of the vCD server, for example, `https://serverFQDNyourvcdFQDN/cloud`.
2. Log in as the administrator.
3. Click on the **System** tab.
4. Click on the **Manage & Monitor** tab.
5. Click on **Organizations**.
6. Right-click on an organization.
7. Click on **Open**.
8. Click on the **Administration** tab.
9. Click on **LDAP** in the left panel.

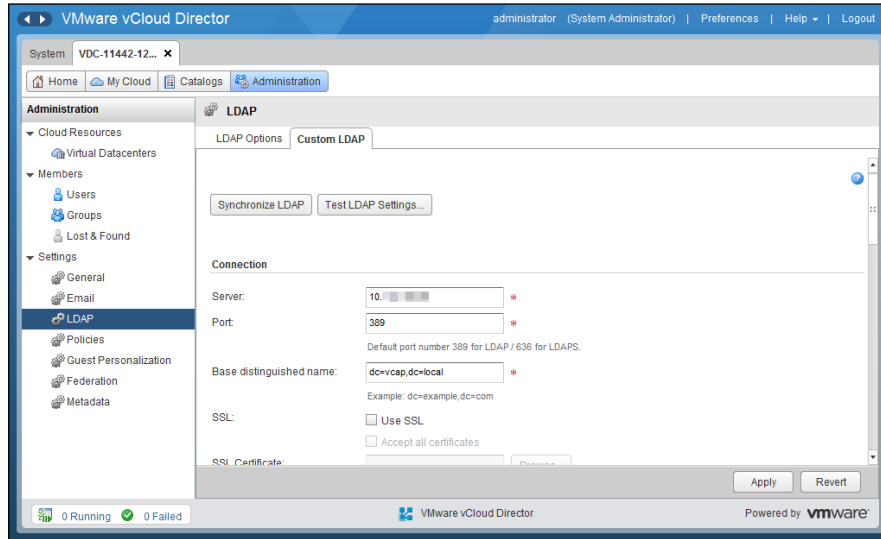
10. Select **Custom LDAP service** as shown in the following screenshot:



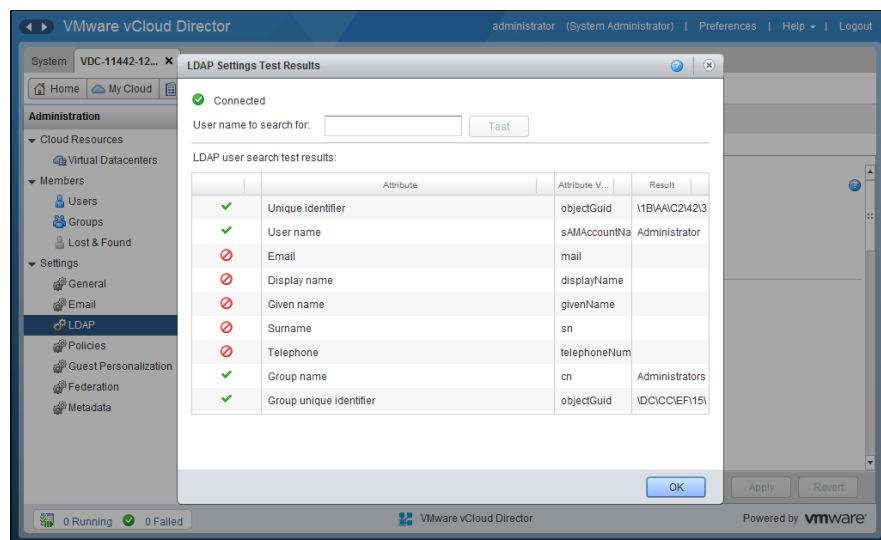
11. Specify the following settings based on your environment:

- AD server address (**Server**)
- Server Port (**Port**)
- **Base distinguished name**
- **Use SSL**
- **Authentication method**
- **User name**
- **Password**

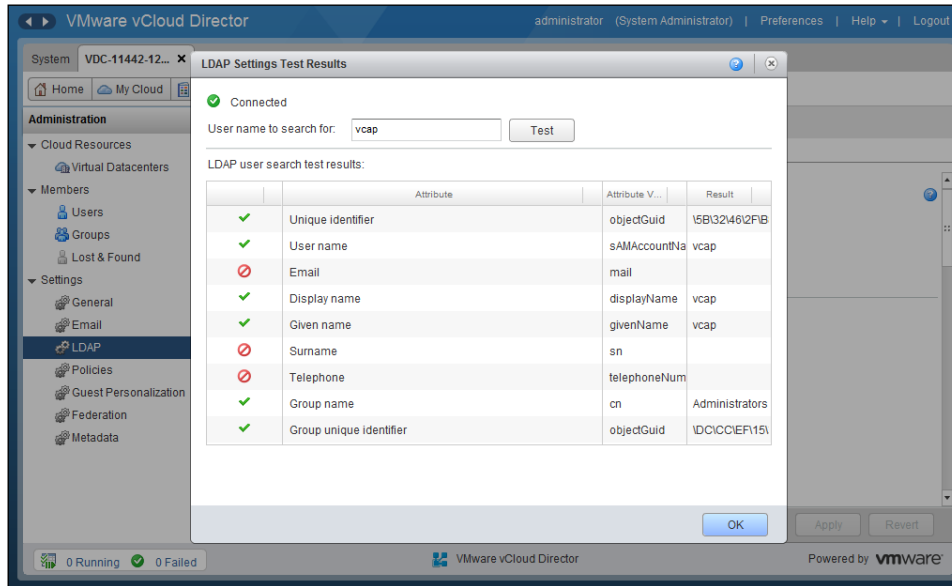
This is shown in the following screenshot:



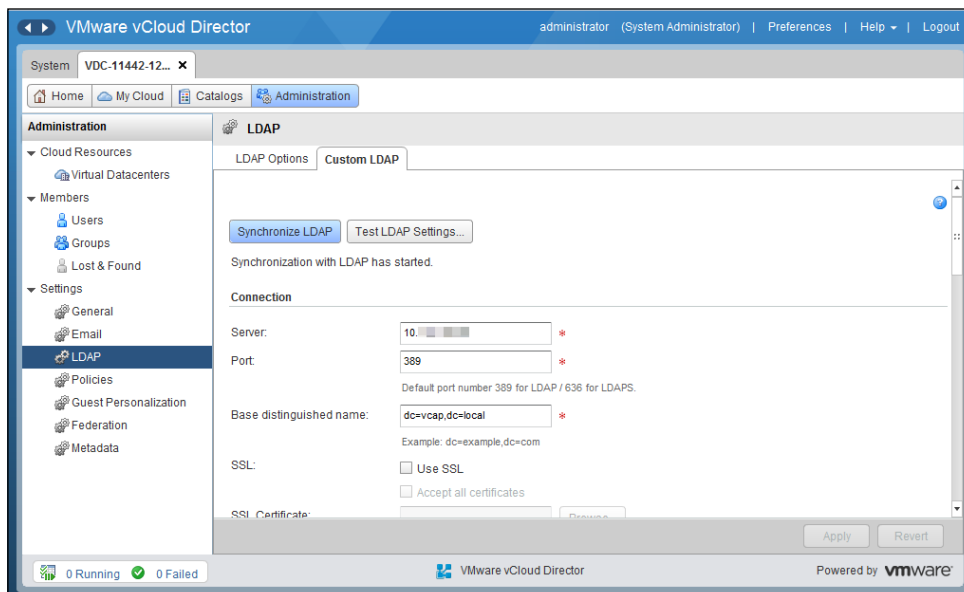
12. Choose the default **User Attributes** settings.
13. Choose the default **Group Attributes** settings.
14. Click on **Apply**.
15. To test the connection, scroll to the top of the page and click on **Test LDAP Settings...** If it is successful, you will see the following screenshot. There may be a couple of red marks as those fields are empty in the AD.



16. To search for a user, type the username in **User name to search for**.
17. Click on **Test**. You will see the result as shown in the following screenshot:



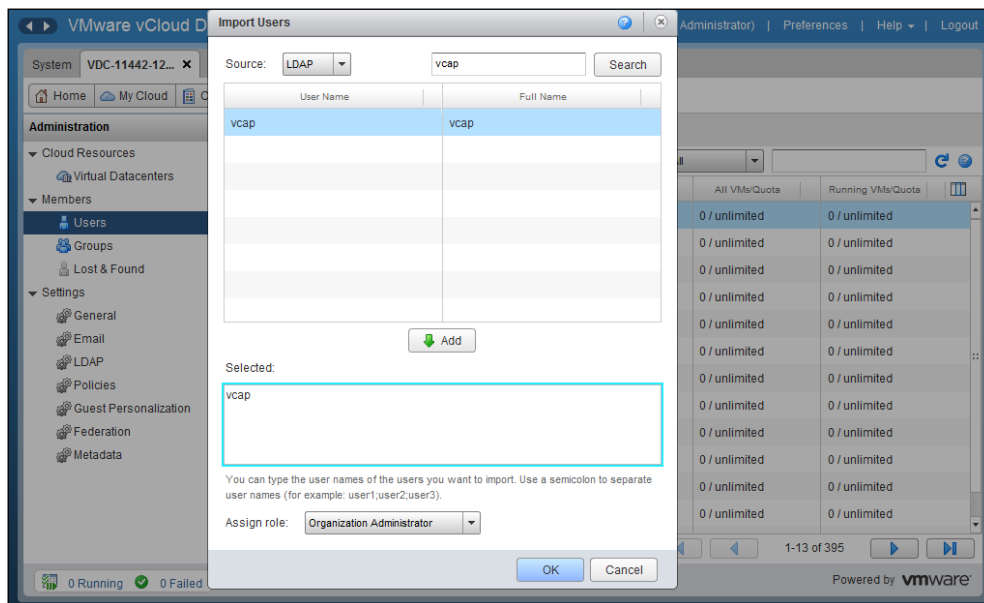
18. Click on **OK**.
19. Click on **Synchronize LDAP**. This is shown in the following screenshot:



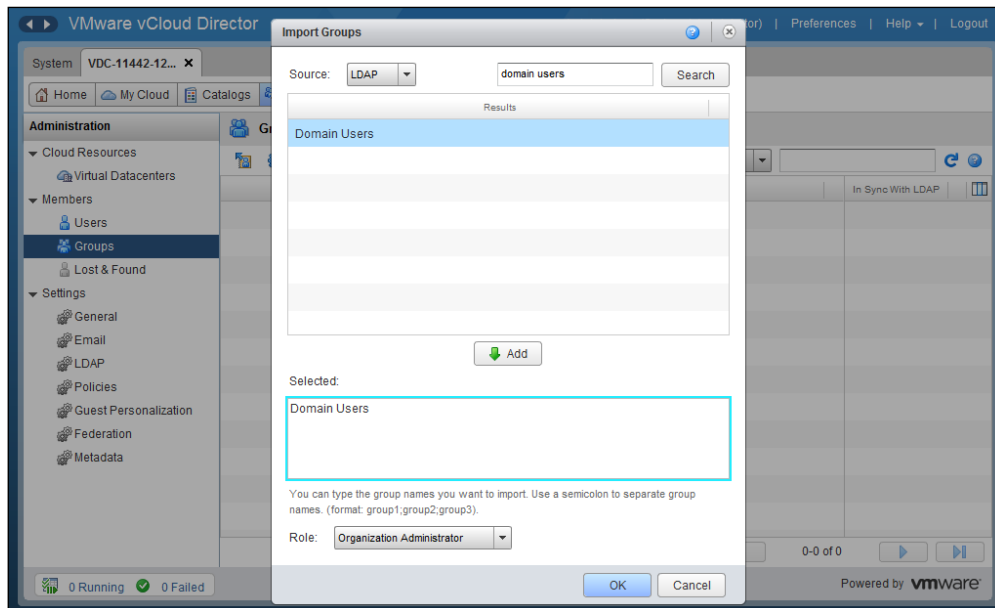
Configuring different types of access controls in vCD requires importing users/groups into the organization. In the following section, we will see how to do that.

Let's import users from the active directory:

1. Open a web browser. Go to the URL of the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD as an administrator.
3. Click on the **System** tab.
4. Click on the **Manage & Monitor** tab.
5. Click on **Organizations**.
6. Right-click on an organization.
7. Click on **Open**.
8. Click on the **Administration** tab.
9. On the left panel, click on **Users**.
10. Click on the **Import** icon.
11. Type a username and click on **Search**.
12. Select the username and click on **Add**. This is shown in the following screenshot:



13. Click on **OK**.
14. In the left panel, click on **Groups**.
15. Click on the **Import** icon.
16. Specify the group name there and click on **Search**.
17. Select the group there and click on **Add**.
18. Click on **OK**. This is shown in the following screenshot:



19. Click on **Logout**.

Creating roles to improve organization security

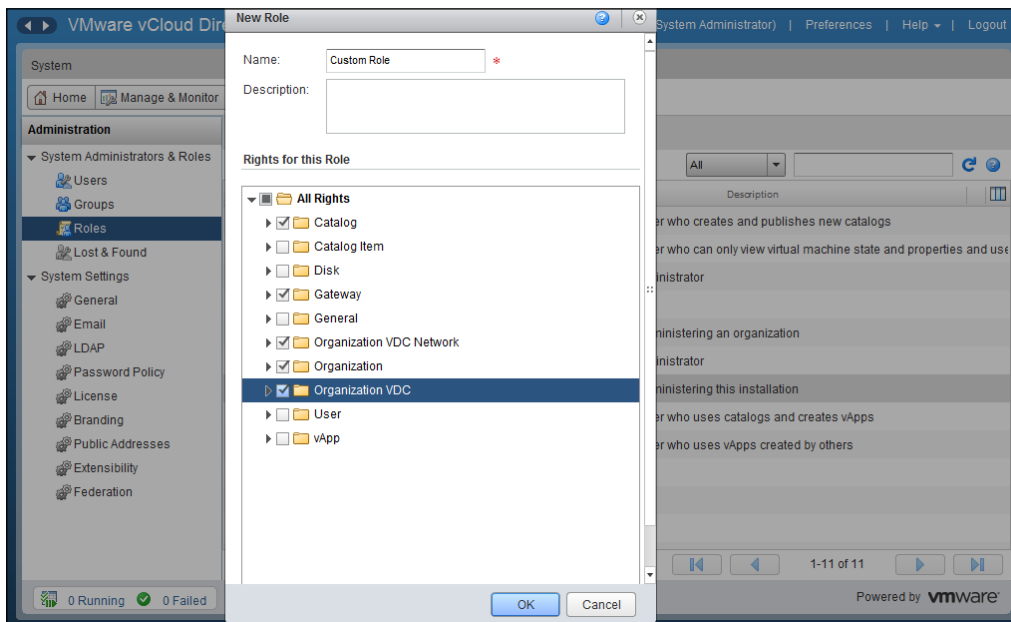
Importing users/groups in the vCloud Director organization is not the end of the task to grant access control. Sometimes your organization may need to create a custom role and assign permissions to the user.

Let's create a custom role and add a user:

1. Open a web browser. Go to the URL of the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.

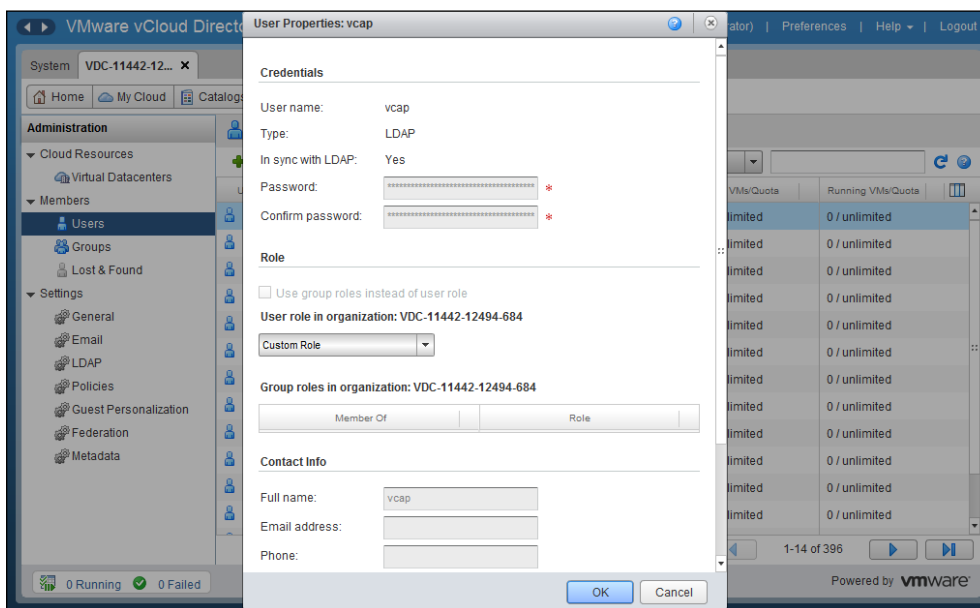
3. Click on the **System** tab.
4. Click on the **Administration** tab.
5. In the left panel, click on **Roles**.
6. Click on the green color + sign to create a role.
7. In the **New Role** wizard, specify and select the following options:
 - **Name**
 - **Description**
 - **Catalog**
 - **General**
 - **Organization**
 - **Organization VDC Network**
 - **User**
 - **vApp**

The **New Role** wizard is shown in the following screenshot:



8. Click on **OK**.
9. Click on the **Manage & Monitor** tab.
10. Click on **Organizations**.

11. Right-click on an organization.
12. Click on **Open**.
13. Click on the **Administration** tab.
14. On the left panel, click on **Users**.
15. Select an already imported user.
16. Right-click on the user and select **Properties**.
17. Select the recently created custom role from the **User role in organization** dropdown. This is shown in the following screenshot:



18. Click on **OK**.

Configuring vCenter SSO as access management for vCloud Director

Since vCloud Director 5.1, VMware gives you an option to import users from VMware vCenter Single Sign-On. You have already seen how to import users from LDAP. These users are similar to users imported from LDAP sources. Users can be imported from any system configured in vCenter Single Sign-On as an identity provider.

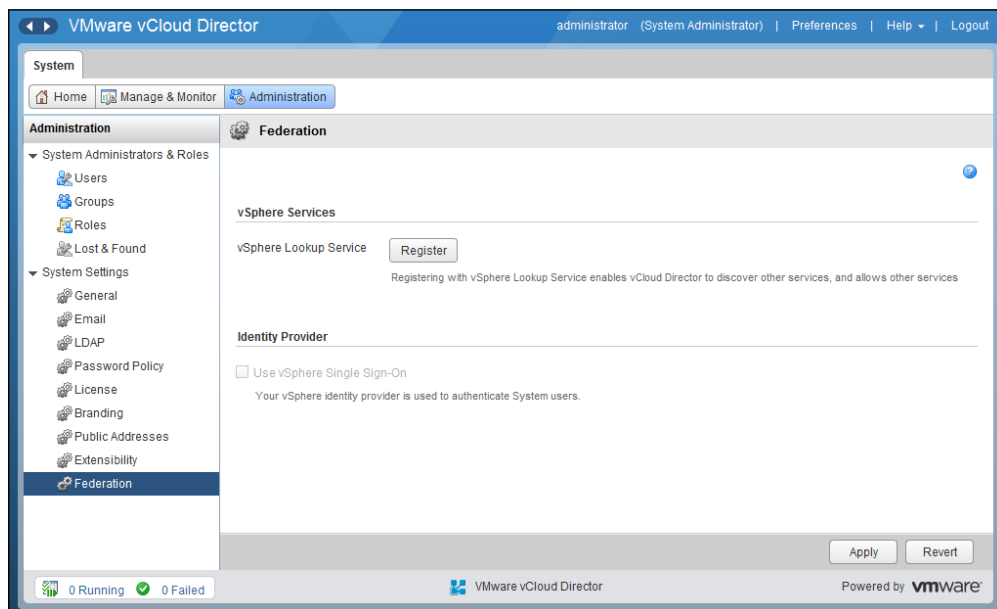
When you enable vCenter SSO in vCloud Director, users will be authenticated by the vSphere identity provider.

You need to register vSphere Lookup Service in the vCloud Director **Administration** tab under **Federation**. Once you configure **Federation**, you can import the users or groups from the vSphere identity provider. Note that only vCloud Director system administrator users can be authenticated through vCenter Single Sign-On.

Let's look at how to configure and maintain VMware Single Sign-On for vCloud Director.

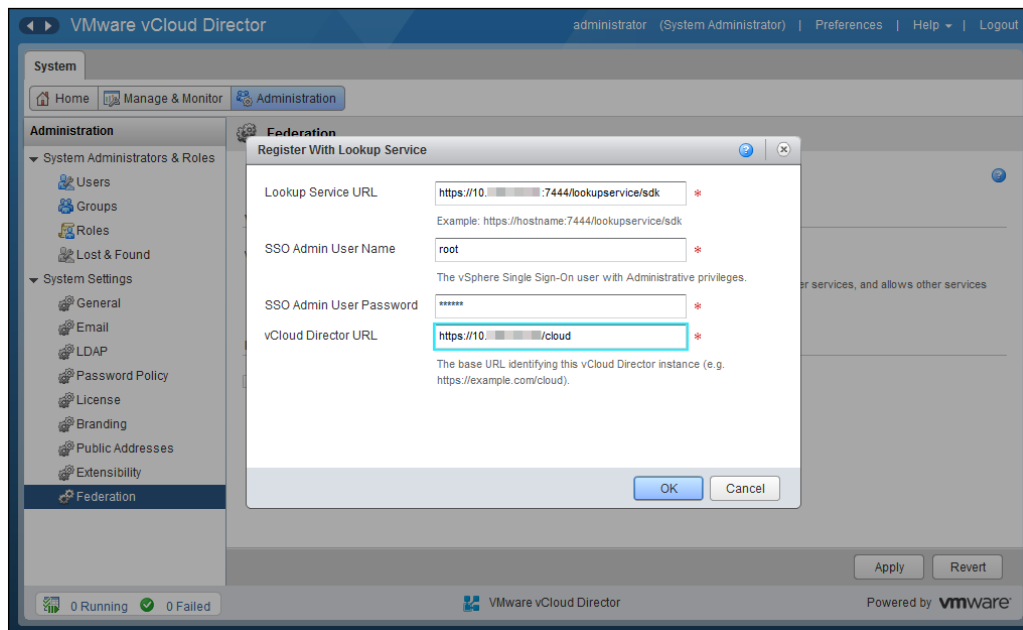
To configure the vCenter SSO in vCloud Director, follow these steps:

1. Start a web browser. Go to the URL of the vCD server, for example, `https://serverFQDN/cloud`.
2. Log in to vCD by typing an administrator user ID and password.
3. Click on the **Administration** tab.
4. Click on **Federation** in the left panel. This is shown in the following screenshot:



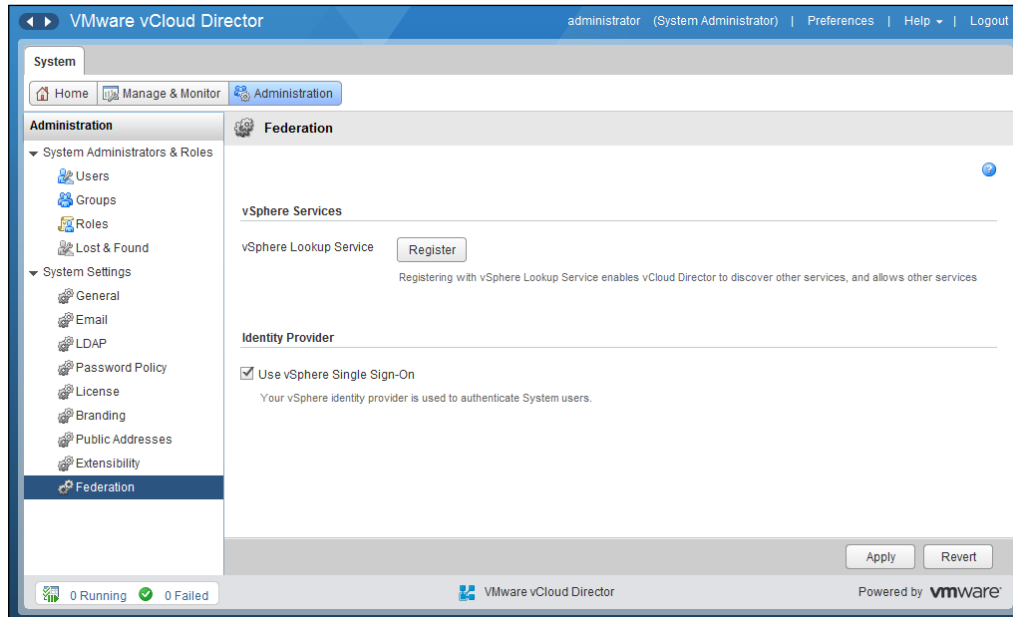
5. From the **vSphere Services** section, click on **Register for vSphere Lookup Service**. Specify the following options there:
 - **Lookup Service URL**
 - **SSO Admin User Name**
 - **SSO Admin User Password**
 - **vCloud Director URL**

This is shown in the following screenshot:

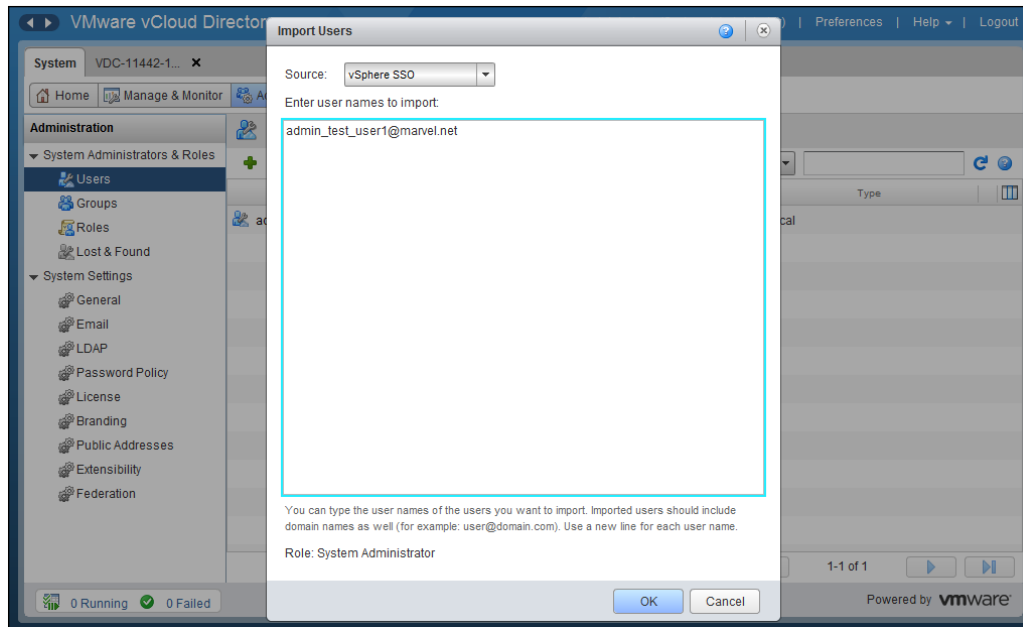


6. Click on **OK**.

7. Once it is registered, select the checkbox **Use vSphere Single Sign-On** from the **Identity Provider** section. This is shown in the following screenshot:



8. Click on **Apply**.
9. Once the vSphere SSO is fully configured, click on **Users** from the **Administration** tab.
10. Click on the **Import Users** icon.
11. Select **vSphere SSO** as a source.
12. In the **Enter user names to import** textbox, specify the usernames you want to import. You can type the usernames of the users you want to import. Imported users should include domain names as well (for example, `user@domain.com`). Use a new line for each username. This is shown in the following screenshot:



13. Click on **OK**.

Summary

In this chapter, we discussed certificate management in vCloud Director. We discussed how to create and process self-signed certificates request and how to replace certificates. We also discussed user access control using LDAP, custom roles, as well as vCenter SSO.

Index

A

- access control, vCloud Director**
 - configuring 163
 - managing 163
- allocation model, organization vDC**
 - allocation pool model 88
 - pay-as-you-go model 88
 - reservation pool model 89
- allocation pool model 88**
- archived basic reports**
 - managing 28, 29

C

- catalog**
 - about 148
 - configuring 149-154
 - creating 149-154
 - private 148
 - public 148
 - published 148
 - shared 148
- cell 5**
- cell.log, audit logs 6**
- cell management tool**
 - about 20
 - using 21
- centralized logging, in vCloud Director**
 - about 6
 - configuring 6
 - configuring, for vShield Manager 11
 - configuring, reasons 7
 - default Log4j configuration, modifying 7
 - enabling 8, 9

- certificate requests**
 - certificates, replacing in vCloud Director 161
 - creating 159
 - processing 159
 - self-signed certificate, creating 160, 161
- certificates**
 - replacing, in vCloud Director 161-163
- certificates command 22**
- Classless Inter-Domain Routing (CIDR) 77**
- Client1 VM 96**
- custom guest vApp**
 - deploying, steps 131
- custom role**
 - creating 169-171
- custom vApp properties 131**

D

- DEBUG level 8**
- denial-of-service (DoS) attacks 82**
- Destination network address translation.**
 - See* DNAT
- DHCP Service, vCloud Director**
 - about 100-102
 - DHCP pool, configuring 102-104
 - Edge DHCP, setting up 102
- diagnostics.log, audit logs 7**
- Direct Connect organization network, vCloud Org networks**
 - about 122
 - configuring 123, 124
- distinguished name (DN) 164**
- DNAT**
 - about 114
 - configuring 115, 116

DNAT rules, vCloud Director 114, 115

DNS relay
configuring 97-100

E

ERROR level 7

ESXi host
adding, to provider vDCs 36-38
disabling 38-40
unpreparing 38-40

external network, vCloud Director 49, 101

External-Public 50

F

FATAL level 7

firewall service, vCloud Director
about 111
vShield Edge device firewall,
configuring 111-114

G

generate-certs command 22

I

INFO level 8

IP addressing, types
DHCP addressing 139
manual IP addresses 140
static addresses 140

IP_Hash, load balancing method 18

**isolated organization vDC network,
vCloud Org networks**
about 122
configuring 125, 126

L

LDAP

about 81, 163
configuring, in vCloud Director 164-168
configuring, on organization 164

lease setting, vCloud Director organization
runtime lease setting 82
storage lease setting 82

LEAST_CONN, load balancing method 18

Lightweight Directory Access Protocol.

See LDAP

**limit setting, vCloud Director
organization** 82

load balancing method
IP_Hash 18
LEAST_CONN 18
ROUND_ROBIN 18
URI 18

Log4j configuration

modifying 7-9

logging levels, vCloud director

DEBUG 8
ERROR 7
FATAL 7
INFO 8
OFF 8
TRACE 8
WARN 8

M

managed by property 32

maximum transmission unit (MTU) 73

N

network address translation (NAT) 139

network pools 71, 72

network pools, types

port groups 73
vCDNI 73
VLAN 72
VXLAN 74

network resources, vCloud Director

managing 70, 71
network pools 71
provider external networks 76, 77

NFS Transfer Server Storage 15

O

OFF level 8

organization access

configuring 164-169

organization access configuration

users, importing from active
directory 168, 169

- vCenter SSO, configuring 171-175
- organization network services**
 - configuring 95, 96
 - uses 97
- organization network services configuration**
 - DHCP Service, vCloud Director 100
 - DNAT rules, vCloud Director 114
 - DNS relay, configuring 97
 - firewall service, vCloud Director 111
 - SNAT rules, vCloud Director 117
 - static routes, configuring in Org Gateway 110
 - static routes, vCloud Director 108
 - VPN tunnels, vCloud Director 104
- organization-to-organization VPN tunnel**
 - configuring 106-108
- organization unit (OU) 164**
- organization, vCloud Director**
 - creating 83-85
 - managing 81, 82
- organization vDCs (Org vDC)**
 - about 63, 71
 - allocation model 88
 - comparing, with provider vDCs 88
 - creating 89-93
 - managing 86, 87
- Org Gateway**
 - static routes, configuring 110
- OVF file**
 - importing, as vApp templates 155-157

P

- pay-as-you-go model 88**
- port groups, network pools 73**
- private catalog 148**
- provider external network**
 - about 76-78
 - creating 78-80
 - diagrammatic representation 77
 - distributed switches 78
 - standard switch 78
- provider vDCs**
 - about 63
 - creating 65-68
 - ESXi hosts, adding to 36-38

- managing 64-70
- merging 68-70
- public catalog 148**
- published catalog 148**

Q

- Quiese 20**
- quota setting, vCloud Director organization 82**

R

- recover-password command 23**
- reservation pool model 89**
- role**
 - custom role, creating 169
- ROUND_ROBIN, load balancing method 18**
- routed organization network, vCloud Org networks**
 - about 122
 - configuring 124, 125
- runtime lease setting, vCloud Director organization 82**

S

- security association identifier (SAID) 73**
- self-signed certificate**
 - creating 160, 161
- self-signed SSL certificates**
 - retrieving 22
- shared catalog 148**
- shell commands, vCD**
 - using 21-24
- SMTP alert settings, in vCloud Director**
 - configuring 26
- SNAT**
 - about 117
 - configuring 118
- SNAT rules, vCloud Director**
 - about 117
 - logical diagram 117
 - SNAT packet flow 117
- Source network address translation.**
 - See SNAT

SSL certificate
replacing 162, 163

static routes, Org Gateway
configuring 110, 111

static routes, vCloud Director
about 108
diagrammatic representation 109
types 108

storage lease setting, vCloud Director organization 82

storage profiles
about 42
configuring 43-47
monitoring, in vCloud Director 47, 48

syslog server
configuring, in vCloud Director 10, 11

system event
fields 11

T

TRACE level 8

transfer storage space
setting up 15

types, IP addressing
DHCP addressing 139
manual IP addresses 140
static addresses 140

U

URI, load balancing method 18

V

vApps
about 129
copying, between catalogs 138
creating 130, 131
deploying 130, 131
vCloud Director vApp, creating 132-147

vApp templates
about 154
OVF file, importing as 155-157

vCD cell
managing 20

vCD GUI
syslog, configuring 10

vCDNI, network pools 73

vCD server
URL 169

vCenter Chargeback reports
managing 28, 29

vCenter Server
registering, with vShield Manager 32-35

vCenter SSO
configuring, in vCloud Director 171-175

vCloud cell deployment logs
capturing, steps 25

vCloud cell load balancing
vCNS, using for 16-20

vcloud-container-debug.log, audit logs 6

vcloud-container-info.log, audit logs 6

vCloud Director (vCD)
about 5, 31
access control, configuring 163
access control, managing 163
certificates, replacing 161-163
configuring, for scalability 13-15
DHCP Service 100
DNAT rules 114
ESXi host resource, managing 36
firewall service 111
network resources, managing 70, 71
organization, managing 81
shell commands, using 21-24
SNAT rules 117
vApps 130
vCenter SSO, configuring in 172-174
VPN tunnels 104
vSphere resources, monitoring in 40-42
VXLAN, preparing for 57-60
warning alerts, configuring 27

vCloud Director organization
creating 83-86
lease setting 82
limit setting 82
managing 81, 82
quota setting 82

vCloud Director vApp
creating 132-147
deploying 138

vCloud Org networks
Direct Connect organization network,
configuring 123, 124

- isolated organization network,
 - configuring 125, 126
- isolated organization network, types 122
- routed organization network,
 - configuring 124, 125
- types 122
- vCloud process**
 - starting 23
 - stopping 23
- vCloud support bundle**
 - using 24
- vCloud System Administrator**
 - tasks 6
- vCloud vApp**
 - about 130
 - custom guest vApp 131
- vCNS**
 - used, for vCloud cell load balancing 16-20
- vDCs**
 - organization vDCs 63
 - provider vDCs 63
- vDS-External distributed switch 77**
- vDS-Prod 50**
- virtual appliances.** *See* **vApps**
- virtual datacenters.** *See* **vDCs**
- Virtual eXtensible Local Area Network.**
 - See* **VXLAN**
- virtual machine network interface**
 - card (vmmnic) 60
- VLAN, network pools**
 - about 72
 - creating 74-76
- vmware-vcd-watchdog.log, audit logs 7**
- VPN tunnels, vCloud Director**
 - about 104-106
 - diagrammatic representations 104, 105
 - organization-to-organization VPN tunnel,
 - configuring 106-108
 - types 104
- vShield Edge**
 - configuring, for compact configuration 121
 - configuring, for full configuration 121
 - configuring, steps 120
 - Direct Connect organization vDC
 - network 122
 - failure, events 119
 - managing 119
 - routed organization vDC network 122
 - vCloud Org networks 122
- vShield Edge device firewall**
 - configuring 111-113
- vShield Manager**
 - centralized logging, configuring for 11, 12
- vSphere compute resources**
 - about 32
 - ESXi host, disabling 38-40
 - ESXi host resource, managing 36
 - ESXi hosts, adding to provider virtual
 - datacenter 36-38
 - vCenter Server, registering 32-35
- vSphere network resources**
 - port group, managing 50-52
 - VXLANs 53-56
- vSphere port groups**
 - creating 50, 51
- vSphere storage profiles.** *See* **storage profiles**
- vSphere storage resources**
 - about 42
 - storage profiles, configuring 43
 - storage profiles, monitoring in vCloud
 - Director 47
- VXLAN**
 - about 53-56
 - features 53
 - mandatory components 53
 - preparing, for vCloud Director 57-60
- VXLAN, network pools 74**
- VXLAN Tunnel End Point (VTEP) 74**

W

- warning alert**
 - configuring 27
- WARN level 8**

Y

- YYYY_MM_DD.request.log, audit logs 7**



Thank you for buying VMware vCloud Director Essentials

About Packt Publishing

Packt, pronounced 'packed', published its first book "*Mastering phpMyAdmin for Effective MySQL Management*" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: www.packtpub.com.

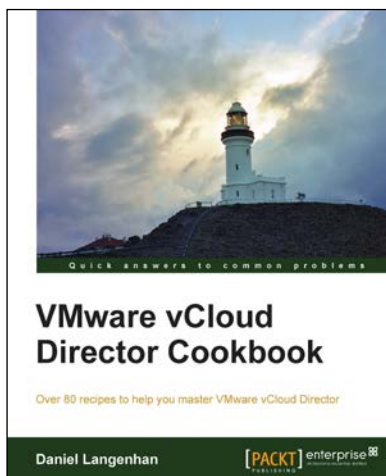
About Packt Open Source

In 2010, Packt launched two new brands, Packt Open Source and Packt Enterprise, in order to continue its focus on specialization. This book is part of the Packt Open Source brand, home to books published on software built around Open Source licenses, and offering information to anybody from advanced developers to budding web designers. The Open Source brand also runs Packt's Open Source Royalty Scheme, by which Packt gives a royalty to each Open Source project about whose software a book is sold.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.



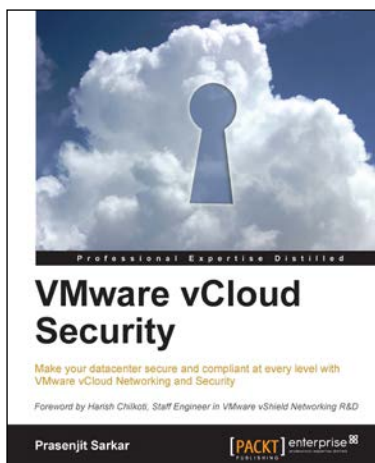
VMware vCloud Director Cookbook

ISBN: 978-1-78217-766-1

Paperback: 364 pages

Over 80 recipes to help you master VMware vCloud Director

1. Learn how to work with the vCloud API.
2. Covers the recently launched VMware vCloud Suite 5.5.
3. Step-by-step instructions to simplify infrastructure provisioning.



VMware vCloud Security

ISBN: 978-1-78217-096-9

Paperback: 106 pages

Make your datacenter secure and compliant at every level with VMware vCloud Networking and Security

1. Take away an in-depth knowledge of how to secure a private cloud running on vCloud Director.
2. Enable the reader with the knowledge, skills, and abilities to achieve competence at building and running a secured private cloud.
3. Focuses on giving you broader view of the security and compliance while still being manageable and flexible to scale.

Please check www.PacktPub.com for information on our titles

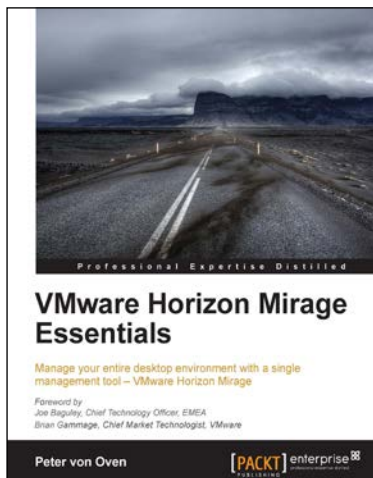


Instant VMware vCloud Starter

ISBN: 978-1-84968-996-0 Paperback: 76 pages

A practical, hands-on guide to get started with VMware vCloud

1. Learn something new in an Instant! A short, fast, focused guide delivering immediate results.
2. Deploy and operate a VMware vCloud in your own demo kit.
3. Understand the basics about the cloud in general and why there is such a hype.



VMware Horizon Mirage Essentials

ISBN: 978-1-78217-235-2 Paperback: 166 pages

Manage your entire desktop environment with a single management tool - VMware Horizon Mirage

1. Deliver a centralized Windows image management solution for physical, virtual, and BYOD.
2. Migrate seamlessly to new versions of operating systems with minimal user downtime.
3. Easy-to-follow, step-by-step guide on how to deploy and work with the technology.