

Community Experience Distilled

VMware vCloud Director Essentials

Build VMware vCloud-based cloud datacenters from scratch





www.allitebooks.com

VMware vCloud Director Essentials

Build VMware vCloud-based cloud datacenters from scratch

Lipika Pal



BIRMINGHAM - MUMBAI

www.allitebooks.com

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

Copy Editors Alisha Aranha Mradula Hegde Gladson Monteiro

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 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

www.allitebooks.com

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.

www.allitebooks.com

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.

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.

www.allitebooks.com

www.allitebooks.com

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

Table of	Contents
----------	----------

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
Creating VI AN-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
Understanding SNAT rules in vCloud Director	115
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
[ii]	

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 screenshot 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.

Preface

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."



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.

Preface

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.

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
cell.log	This logfile is the console output from the vCloud Director cell
vcloud-container- debug.log	This logfile shows the debug-level log messages from the cell
vcloud-container-info. log	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

- [7] —

- 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
```

6. 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
```

- 7. Save the file.
- 8. 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.

9. 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:

```
Prot logger
logd;.rootlogger=ERROR, vcloud.system.debug, vcloud.system.info vcloud.system.syslog
logd;.appender.vcloud.system.syslog.appender
logd;.appender.vcloud.system.syslog.appender
logd;.appender.vcloud.system.syslog.topotstem.str.l.10
logd;.appender.vcloud.system.syslog.topotstem.syslogAppender
logd;.appender.vcloud.system.syslog.topot=conversionPattern=%d[SD8661] %=8.8p %=25.50t %=30.50c[1] %m %%%m
logd;.appender.vcloud.system.syslog.topot=conversionPattern=%d[SD8661] %=8.8p %=25.50t %=30.50c[1] %m %%%m
logd;.appender.vcloud.system.syslog.topot=conversionPattern=%d[SD8661] %=8.8p %=25.50t %=30.50c[1] %m %%%m
logd;.logger.com.vware.vcloud=DBBUG
logd;.logger.com.vware.stelled.wellent=DEBUG
logd;.logger.com.vware.stelled.wellent=DEBUG
logd;.logger.com.vware.stelled.wellent=DEBUG
logd;.logger.com.vware.stelled.wellent=DEBUG
logd;.logger.com.vware.stelled.setUent=DEBUG
logd;.logger.com.vware.stelled.setUent=DEBUG
logd;.logger.com.vware.stelled.setUent=DEBUG
logd;.logger.com.vware.stelled.setUent=DEBUG
logd;.logger.stelled.setUent_stelled.setUent=DEBUG
logd;.logger.stelled.setUent_org.apache.logd;.lonsleAppender
logd;.appender.stelled.setUentENESUG
# appender for all log requests with level >= DEBUG
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=DEBUG
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-debug.log
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-debug.log
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-debug.log
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-debug.log
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-debug.log
logd;.appender.vcloud.system.debug.FleeIogS/vcloud=Container-info.log
logd;.appender.vcloud.system.info.fleeIogS/vcloud=Container-info.log
logd;.appender.vcloud.system.info.fleeIogS/vcloud=Container-info.log
logd;.appender.vcloud.system.info.fleeStelle24488
logd;.appender.vcloud.system.info.fleeStelle24488
logd;.appender.vcloud.system.info.fleeStelle24488
logd;.appender.vcloud.system.info.logs/ucloud=Cont
```

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:

VMware vCloud Dir	ector	administrator (System Administrator) Preferences Help - Logout
System		
Home 😡 Manage & Monitor	🍇 Administration	
Administration	General	
- System Administrators & Roles	Ону зузют волиналатога сан ис	err ale debug information.
🏖 Users	Networking	
📇 Groups		
Roles	IP address release timeout	0 seconds *
A Found		The value must be a whole number between 0 and 2592000.
→ System Settings		Specifies how long to keep released IP addresses on hold before making them available for allocation
🧬 General		again. This is typically set to 2 hours to allow old entries to expire from client ARP tables. IP
i Email	Allow Overlandian Esternal b	
<i>∰</i> LDAP	Allow Overlapping External N	
Password Policy	based methods to isolate your exte	ama networks that run on the same network segment. You should only enable this setting if you are using non-vLAN- ernal networks.
PLicense 🔐	Default syslog server settings fo	or networks
ig Branding	Syslog server 1:	10.1.1.1
Public Addresses	Syclog conver 2:	10.1.1.2
Extensibility	Syslog server 2.	
Federation		The values must be valid in addresses.
		Apply Revert
🗿 0 Running 🔮 0 Failed		VMware vCloud Director Powered by VMWare

-[10]-

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 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:

View: Host & Clusters 🗘	You are logge Settings & Reports	d in as a Sy	stem Administrator	Logged in a	as:admin <u>Ch</u> a	ange Password	Logout	<u>Help</u>	<u>bout</u>
	Configuration	Update	s User	s Sys	tem Events	Audit Logs		Tasks	
Q	General Support Bac	kuns SSI	Certificate Networ	king					
🖃 🛃 Settings & Reports									
- VShield App	Connecting to a vCente	er server en	ables vShield Manag	er to display the	VMware Infras	structure inventor	1.		-
Data Security	HTTPS port (443) need	s to be ope	n for communication	between vShiel	d Manager, ESX	(and VC. For a fu	Il list of port	ts required	i,
Service Insertion	see section "Client and	User Acces	s" of Chapter "Prepa	ring for Installat	ion" in the "vSI	hield Installation a	and Upgrade	e Guide".	
- N Object Library	vCenter Server: 10	.144.36.10	1						
E 💋 Datacenters	Last successful in	ventony ung	late was on 5/10/13	11.50 AM (UTC	1				
PC1-DC	Last succession m	ventory upu	ace was on 5,15,15	11.55 AM (610,	/				
E III PCI-Resource-Cluster	DNE Comiona		Syslog Server Inf	ormation		8			Edit
	DNS Servers		Enosify the ID addr	occ or the name	of the system of				
	and other vSphere com	ponents.	You may optionally	specify the port	too.	server.			
	Primary Server:	10.144.36.	Syslog Server:	10.1.1.2					
	Secondary Server:	Not Config	Port:	514					
	Tertiary Server:	Not Config	, ore:	514					
	NTP Server								Edit
	Specify NTP server held	w For SSC				VSM s	erver and N	TP server	
	should be in sync. It is	recommen				10110		in server	
	NTD Commun. Nat. Co	- Count			OK	Cancel			
	NTP Server: Not Co	migurea							
									Edit
	Syslog Server								
	You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).								
	Syslog Server: Not Configured								
	4								Þ

- 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:

0 0	^		R <u>a</u>
-rw 1 vcloud vcloud	446 May 16 10:41	1 1368700861500.log	
-rw 1 vcloud vcloud	3492 May 16 11:09	9 1368702567205.log	
-rw 1 vcloud vcloud	446 May 16 11:12	2 1368702746051.log	
-rw 1 vcloud vcloud	446 May 16 11:18	8 1368703109193.log	
-rw 1 vcloud vcloud	446 May 16 11:24	4 1368703445150.log	
-rw 1 vcloud vcloud	446 May 16 11:30	0 1368703807273.log	
-rw 1 vcloud vcloud	446 May 16 11:36	6 1368704169410.log	
-rw 1 vcloud vcloud	446 May 16 11:42	2 1368704531559.log	
-rw 1 vcloud vcloud	446 May 16 11:48	8 1368704893679.log	
-rw 1 vcloud vcloud	446 May 16 11:54	4 1368705255818.log	
-rw 1 vcloud vcloud	446 May 16 12:00	0 1368705617951.log	
-rw 1 vcloud vcloud	2696 May 16 13:24	4 1368/098/6834. Log	
-rw 1 vcloud vcloud	3492 May 16 13:40	0 1368/11619539. log	
-rw 1 vcloud vcloud	3492 May 16 13:43	3 1368/11/98928. (og	
-rw 1 vcloud vcloud	446 May 16 13:46	6 1368/119993/6. log	
-rw 1 vctoud vctoud	5080 May 16 12:04	4 Certificates	
-rw-r 1 veloud veloud	2024 Mar 26 02:35	S cmt-logging.properties	
-rw-r 1 veloud veloud	20014 Mar 20 02:00	dota ovport sottings ini	
-rw-r 1 veloud veloud	570 Mar 20 02:34	data_export_settings.ini	
-rw-r 1 vcloud vcloud	46266 Mar 26 02:34	A data_export_settings.ini.save	
-rw-r 1 vcloud vcloud	46276 Aug 14 2012	data to export properties save	
-rw 1 vcloud vcloud	1441 May 16 12:04	alobal_properties	
-rw 1 vcloud vcloud	543 Mar 26 02:59	global.properties.romnew	
-rw 1 vcloud vcloud	1412 Jan 25 06:04	dobal.properties.romsave	
-rw-r 1 vcloud vcloud	73 Mar 26 02:34	4 installer.properties	
-rw-r 1 vcloud vcloud	0 Mar 26 02:56	6 java.util.logging.properties	
-rw-r 1 vcloud vcloud	0 Mar 26 02:56	6 krb5.keytab	
-rw-r 1 vcloud vcloud	3526 Mar 26 02:56	6 log4j.properties	
-rw-r 1 root root	3526 Feb 18 17:37	7 log4j.properties.default	
-rw-r 1 vcloud vcloud	3526 Aug 14 2012	2 log4j.properties.save	
-rw-r 1 vcloud vcloud	880 Mar 26 02:56	6 org.apache.aries.transaction.cfg	
-rw-r 1 vcloud vcloud	36 Mar 26 02:56	6 org.apache.karaf.features.cfg	
-rw-r 1 vcloud vcloud	1130 Mar 26 02:56	6 org.apache.karaf.log.cfg	
-rw-r 1 vcloud vcloud	1179 Mar 26 02:56	6 org.apache.karaf.management.cfg	
-rw-r 1 vcloud vcloud	1064 Mar 26 02:56	6 org.apache.karaf.shell.cfg	
drwx 3 vcloud vcloud	4096 May 16 13:24	4 org.eclipse.core.runtime	
drwx 3 vcloud vcloud	4096 Jan 25 06:06	6 org.eclipse.equinox.app	
drwx 4 vcloud vcloud	4096 May 16 13:48	B org.eclipse.osgi	
-rw-r 1 vcloud vcloud	3635 Mar 26 02:56	6 org.ops4j.pax.url.mvn.cfg	
-rw 1 vcloud vcloud	5088 May 16 12:04	4 proxycertificates	
-rw 1 vcloud vcloud	446 May 16 12:04	4 responses.propercies	
-rw 1 vcloud vcloud	445 Jan 31 02:01	responses.properties.save	
-rw-r 1 veloud veloud	220/ Mar 20 02:50	b system properties	
-rw-r 1 vcloud vcloud	166 Mar 26 02:30	d wod support config properties	
[root@voc1_etc]#	100 Har 20 02:34	+ vca_sapport_contractores	
Concerber crei# =			

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 = X5BpcRBwn7k1sRX7CHsug==
system.version = 2
audit.syslog.host =
audit.syslog.port = 514
[root@ etc]#
```

- [14] -

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 \$VCLOUD_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
```

```
-[15] —
```

- 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
```

 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 .0.51 as the VMRC console proxy IP address. The second vCD cell uses 192.168.0.52 as the web portal IP and .0.53 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.

- [17] -

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

View: Host & Clusters		You are logo -DC	jed in as a S	ystem Admii	nistrator	Logge	ed in as:a	admin	Change P	assword	<u>Logout</u>	<u>Help Abou</u>	ut
					Endpo				d Net	work Vir	tualization		
Settings & Reports	Prepa	aration Net	work Scopes	Networks	Edges	661-8	8661-4	ld4d1	2f5593;	a)		Refres	sh
Cata Security		vsc cug	c gw (c)	507511	J/JZ 4	001 0		u iui	2100900	.,			
Data Security		Settings	Statistics	Configure	Firewall	DHCP	NAT	VPN	Load Balan	cer			
Service Insertion		Pools Vir	tual Servers										
		10013 11											
Datacenters													
Resource-Cluster	Lo	oad Balancer	Service Sta	tus: Disabled	d 🚺 Enat	ble							
	A loa	ad balancing	pool is a logi	cal set of de	vices, such	as web	servers,	that yo	u group toge	ether to r	eceive and p	rocess traffic.	•
	+	/ ×							Search				G
	1	Add					Serv	vice and	health che	ck			
		Name	1 🔺 Member:	Service	State	s	Port	Mon	itor F g Me	lancin thod	Interval (second s)	Timeout (seconds)	

11. Name this pool and click on Next. I have named it vCD-Web-80-443.

12. 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.
	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
URI	applicable for HTTP service load balancing.

- 13. Select the default Health Check settings and click on Next.
- 14. 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:

	You are logged in as a System Administra			rator Lo	tor Logged in as:admin <u>Cl</u>		e Password	Logout	Help About	
View: Host & Clusters 🗸 🖓	-DC								_	
	General	General App Fire		Endpoint Spool		oofGuard	ard Network Virtualization			
Q	Preparation Ne	twork Scones	Networks	daes					Refresh	
🖃 🔛 Settings & Reports										
- VShield App	🔷 vse-edg	🛊 vse-edge-gw (e75c73f1-9752-4661-8661-4d4d12f5593a)								
- 🛐 Data Security	Settings	Statistics	Configure F	irewall DH	CP NAT	VPN Load B	alancer			
- Cervice Insertion	Cottings	orariorica	configure 1	incition Dir		Codd L	alancer			
🛛 🚺 Object Library	Pools Virtual Servers									
🗄 📂 Datacenters										
	esource-Cluster									
🗄 🙀 Resource-Cluster										
Load Balancer Service Statur: Disabled										
	Let a land be a single set in a latitude set of during a such as such as such as the burners to show the star set of a such as the first set of the star set o									
	A load balancing pool is a logical set of devices, such as web servers, that you group together to receive and process traffic.									
	🕈 🥖 🗙 Search						arch			
				Service and health check						
					00111001	nee and near	Delessiel	Tobar of L		
	Name	1 Members	Service	Status	Port	Monitor F	Balancin	Interval (second	Timeout	
			0011100	Clatab	. one		Method	s)	(seconds)	
	VMRC-443	2	TCP		443	8080	ROUND_RC	5	15	
	vCD-Web-80-4	43 2	HTTP		80	80	ROUND RO	5	15	
		-	HTTPS		443	443	ROUND_RC	5	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.

Quiese 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
```

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.



If you change certificates of any product that is based on vCD (such as vCAC, Chargeback, and so on), you need to re-establish their connections in order to accept the new SSL certificates.

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 ]
```
5. 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:

[roote ~]# 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 25026 1 0 15:21 ? 00:00:00 /bin/bash /opt/vmware/vcloud-director/bin/vmware-vcd-watchdog
vcloud 25065 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-dir
ector/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
CLUUD_HUME=/opt/vmware/vcloud-director -Djava.lo.tmpdir=/opt/vmware/vcloud-director/tmp -Djava.library.path=/opt/vmware/vcloud-director -Djava.n
et.preteripv4stack=true -boracle.jdbc.detaultMchar=true -bile.encoding=uir-8 -blog4].contiguration=file:/opt/wWware/vcloud-director/etc/log4j.p
roperties - jar /opt/vmware/vcloud-director/system/org.ecijpse.osgl-3.6.0.2010051/.jar - configuration /opt/vmware/vcloud-director/stetor
100 2300 1 0 13:21 1 0 00:00:00 /00/100 0/00/00 0/00 0/00
duu / op//wwware/vcloud-director/lags_Dkaraf bara/lowd-director_Dkaraf bara/lowd-director/lags_Dkaraf bara/lowd-director/lags_Dkaraf bara/lowd-director_Dkaraf bara/lowd-direc
erve (udu-director/etg) - balan.nome/opt/vmware/vclode-director-opt/vmware/vclode-director/etg) - balan.nome/opt/vmware/vclode-director/etg/intervel/vclode-director/etg/interve
verse versus and encourse of the second s
-Dorg.ops4i.pax.logging.DefaultService.og.level=ERBOR -Dkaraf.name=root -Diava.awt.headless=true -DVCLOUD HOME=/opt/vmware/vcloud-director -Diav
a.io.tmpdir=/opt/vmware/vcloud-director/tmp -Diava.librarv.path=/opt/vmware/vcloud-director -Diava.net.preferIPv4Stack=true -Doracle.idbc.defaul
tNChar=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
[root@ ~]#

6. 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 \$VCLOUD_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 \$VCLOUD_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:

VMware vCloud Dir	ector			administrator	(System Administrator)	Preferences	Help 🖌	Logout
System								
🚹 Home 😡 Manage & Monitor	🍇 Administration							
Administration	Email							
✓ System Administrators & Roles	SMTP Settings SMTP server name: SMTP server port User name: Password: Sender's email address:	25		Requires au	thentication			A
 LDAP Password Policy License Panding Public Addresses Extensibility Federation 	Email subject prefix: Test destination: System Notification Setting Send system notification to	Email address JS O All	s of the test email rec	Test SMTP set ipient.	tings.			
🗿 0 Running 🕥 0 Failed			ese email address ter comma-separated	es email addresses. Id Director		Apply	Reviewed by VMIV	•rt vare

- [26]-

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:



- [27] -

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

Managing vSphere 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:

VMware vCloud Director			administrator (Sy	ystem Administrator)	Preferences Help - Logout							
System												
🚹 Home 😡 Manage & Monitor 🖓 Administration												
Some basic Cloud entities appear to be r After you provision Cloud resources from	nissing. The Quick Start s your vCenter, you can se	section can guide et up your first or	you through the preparatory steps. ganization.		Support							
Quick Start					Getting Started Help							
First, provision your Cloud resource	·S	Then allocate	e resources to an organization		VMware Support							
1 Attach a vCenter		S Crea	ate a new organization		About							
2 Create a Provider VDC		S 6 Alloc	cate resources to an organization									
3 Create an external network		7 Add	a catalog to an organization									
4 Create a network pool												
Tasks												
System												
Anage Provider VDCs	lanage organiz	ations	🛔 Manage your system adminis	strators								
	Anage organiz	ation VDCs	+ Add a new system administra	ator								
Manage network pools	Manage Edge G	ateways	Notify users									
🖓 0 Running 🔮 0 Failed		K	VMware vCloud Director		Powered by VMWare							

- 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**.

	Attach New vCenter			
System	Name this vCenter	Name this vCenter Enter the connection information, name, and description for the new vCenter as you want it to	appear in VCD.	
Some After Quici Fin C C C Task:	Ready to Complete	Host name or IP address: * Port Number 443 * User name: * Password: * VCenter name: * Description: * vSphere Web Client URL: Use vSphere Services to provide this URL Use the following URL:		
		Back	Finish Cancel	ware [.]

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.

Attach New vCenter	0	8	
Attach New vCenter System Name this vCenter Connect to vShield Manager Ready to Complete Attach New vCenter Connect to vShield Manager Coulck Firs C C C C C C C C	Connect to vShield Manager vShield Manager is required for network services in VCD. Enter the connection information for the vShield Manager that is associated with this vCenter. Make sure that vShield Manager is already registered with the vCenter. Host name or IP address: Vser name: Password: *	8	Logout
	Back Next Finish Cancel		ware ⁻

— [34] —

- 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:

VMware vCloud D	ire	ctor				admin	istrator (Syste	em Administrator)	Preferences	s Help - Logout	
System											
🚮 Home 😡 Manage & Monitor 🍇 Administration											
Manage & Monitor		Hosts									
Crganizations	•	⊗ -					All	-		C 3	
Cloud Resources		Name	1 🔺	Status	En	Ready	Available	VCD Network Isolatic	Total	vCenter	
Provider VDCs		10.		0	0	0	~	-	🗗 O	VCAP-CIA-vCenter	
Organization VDCs	E	10.		0	~	~	×	×	🗗 0	VCAP-CIA-vCenter	
Edge Gateways		10.		0	~	~	×	×	🗗 O	VCAP-CIA-vCenter	
External Networks	E										
Network Pools											
✓ vSphere Resources	Ľ										
Centers 🖓	h										
Resource Pools	E										
	h										
Storage Profiles	E										
Switches & Port Groups											
Stranded Items											
Logs	•								1-3 of 3		
0 Running 🔮 0 Failed				K VN	lware vCl	oud Director			Pov	wered by VMWAre	

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

VMware vCloud D	Dire	ctor				admini	strator (Syste	em Administrator)	Preferences	Help - Logout
System										
Home Manage & Monito	or	Administration								
Manage & Monitor		Hosts								
Organizations	•						All	-		୯ ଜ
- Cloud Resources					-					
Cloud Cells		Name	1 🔺	Status	En	Ready	Available	VCD Network Isolatio	Total	vCenter
Provider VDCs		10.	Act	ions: 10		0	×	-	₫ 0	VCAP-CIA-vCenter
Organization VDCs		10.	Enable	Host		×	×	×	🗗 0	CAP-CIA-vCenter
Edge Gateways		10.	Disable	Host		×	×	×	🗗 0	VCAP-CIA-vCenter
External Networks	11		Redep	lov All VMs						
Network Pools			Prepar	e Host						
			Unprep	are Host						
vCenters			Upgrad	le Host Agent	_					
Resource Pools			Repair	Host						
Hosts			Open i	n vSphere Web Clier	nt					
Datastores & Datastore C			Proper	ties						
Storage Profiles										
Switches & Port Groups										
Stranded Items										
E Logs	Ŧ								1-3 of 3	
🖓 0 Running 🔮 0 Failed)			K VM	ware vCl	oud Director			Pov	vered by VMWare

— [37] —

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

VMware vCl	Prepare Hosts				3	es Help - Logout
System	To use the selected hosts ir administrative privileges on	Cloud, the sy each host.	stem needs to install the Cloud agent	on each host. This installation requ	res	
Manage & Monitor	A single credential for all Administrator user name:	hosts: root				
Cloud Resources	Password:	1				C 3
Cloud Cells	A credential for each hose	st:				vCenter
Provider VDCs	Host		Administrator User Name	Password		CAP-CIA-vCenter
Constant Con	10.					VCAP-CIA-vCenter
Edge Gateways	0					VCAP-CIA-vCenter
Network Pools						
P vCenters						
Resource Pools						
Hosts						
Datastores & Data						
Storage Profiles						
Switches & Port C						
E Stranded Items						
E Logs						
👔 0 Running 🛇 0				ОК	Cancel	owered by VMVAre

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:

VMware vCloud Dir	rec	tor				admini	istrator (Syste	m Administrator) Pr	eferences	Help - Logout
System										
Home 😡 Manage & Monitor	8	Administration								
Manage & Monitor		Hosts								
Organizations	1	0} -					All	•		C' 🥹
Cloud Resources		Name	1 🔺	Status	En	Ready	Available	VCD Network Isolatio	Tota	vCenter
Provider VDCs		10.		0	× .	× .	×	×	🗗 0	VCAP-CIA-vCenter
Crganization VDCs		10.		ctions: 10	-	×	×	~	ි මේ	VCAP-CIA-vCenter
🦁 Edge Gateways			Enabl	a Host	-					
			Disab	le Host						
Network Pools ::			Rede	plov All VMs						
✓ vSphere Resources			Prepa	re Host						
Centers VCenters			Unpre	epare Host						
C Resource Pools			Upgra	de Host Agent						
Hosts			Repai	ir Host						
Datastores & Datastore C			Open	in vSphere Web Clie	ent					
Storage Profiles			Prope	erties						
Switches & Port Groups										
Stranded Items										
📰 Logs 👻									-2 of 2	
🗿 0 Running 🔮 0 Failed				🛃 VM	ware vClo	oud Director			Pow	rered by VMWare

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

VMware vCloud Dir	re	ctor				admin	istrator (Syste	em Administrator) Pr	eferences	Help - Logout
System										
Home Manage & Monitor	ł	administration								
Manage & Monitor		Hosts								
Organizations Cloud Resources	•	⊕ •					All	•		C 0
Cloud Cells		Name	1 🔺	Status	En	Ready	Available	VCD Network Isolatio	Tota	vCenter
Provider VDCs		10.		0	× .	×	×	×	di 0	VCAP-CIA-vCenter
Organization VDCs		10.		0	0	×	~	×	🗗 0	VCAP-CIA-vCenter
Edge Gateways			Action	ns: 10.						
	E		Enable Ho	ost						
Network Pools ::			Disable H	ost						
	E	_	Redeploy	All VMs	_					
P vCenters	L		Prepare H	lost						
Resource Pools			Unprepare	e Host						
Hosts			Upgrade I	Host Agent						
Datastores & Datastore C		-	Repair Ho	SI	_					
Storage Profiles	Ľ		Open in V	opriere web cilent						
Switches & Port Groups			ropenies	,						
Stranded Items										
🔲 Logs 🗸 🗸								۱	-2 of 2	
0 Running 🔮 0 Failed					ware vClo	oud Director			Pow	ered by VMWare

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 thinks 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:

VMware vCloud E	Din	ector		administrator	(System Administrator)	Preferences	Help 🚽	Logout
System								
Home 😡 Manage & Monit	or	Number 2017 Administration						
Manage & Monitor		Resource Pools						
Organizations	1	<u>ه</u> -			All 👻			c 🕤
 Cloud Resources 		Name	1.		vCenter			
Cloud Cells					Voontoi			
Provider VDCs		Resource-Cluster1		CAP-CIA-VCenter				
Organization VDCs								
Edge Gateways								_
External Networks								_
Network Pools	::							
 vSphere Resources 								
2 vCenters								_
hesource Pools								
Hosts								
Datastores & Datastore C								
Storage Profiles								
Switches & Port Groups								
Stranded Items						11011		N. 1
E Logs	٣					1-1 0/1		PI
🗿 0 Running 🔮 0 Failed		1		ware vCloud Director		Powere	ed by VMIV	vare [.]

6. 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:

VMware vCloud Dir	rector			administrator (System	n Administrator)	Preferences	Help - Logout
System							
Home Manage & Monitor	Section Administration						
Manage & Monitor	Resource Pool Prop	erties: Resource-Clu	ıster1		3 8		
 Organizations Cloud Resources Cloud Cells 	Name: Memory reservation: CPU reservations (u	Reso s (used/total): 0.00 sed/total): 0 MH	ource-Cluster1 MB / 22,410.00 MB łz / 58647 MHz				C 3
Organization VDCs Getage Category	Datastores available	to this resource:					
Edge Gateways	Datastore	Туре	Connected	Capacity (Used/Total)	% Used		
Network Pools	datastore1	VMFS5	~	972.80 MB / 35.00 GB	2.71%		
	NFS	NFS	×	7.04 GB / 1,007.93 GB	0.70%		
P vCenters	datastore1 (2)	VMFS5	~	972.80 MB / 35.00 GB	2.71%		
Secource Pools	datastore1 (1)	VMFS5	¥	972.80 MB / 35.00 GB	2.71%		
Hosts							_
Storage Profiles					ОК		
Switches & Port Groups							
Logs -						1-1 of 1	
0 Running 🔮 0 Failed			VMware vCloud [Director		Powere	d by vm ware [.]

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-yourvcloud-from-1-5-to-5-1-watch-out-for-the-anystorage-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:

vmware [®] vSphere Web Cli	ent 🕇 🖉 - 한 root@localos - Help -	Q Search
Home - I	INFS Actions -	=- I
	Getting Started Summary Monitor Manage Related Objects	🔹 🔄 Recent Tasks 🗖
VPC4-DC	Settings Alarm Definitions Tags Permissions Files Profiles Scheduled Tasks	All Running Failed
datastore1 (1)	Manage Storage Capabilities	V Resource-Cluster1
datastore1 (2)	System Storage Capability	
	NFS: Assign User-Defined Storage Capability (?)	
	Capability Name: None 🔹	My Tasks • More Task
	Description: Creates a ne	ew User-Defined Storage Capability
		Work In Progress NFS: Assi
		T the Alarms
	OK Cancel	All Ne Ac

- 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:

Chapter 2

Rules and Profiles 🔹	I Grund VM Storage Profiles		
VM Storage Profiles	0 😚 l 🕼 🦃	Q Filter	🔹 👻 Recent Tasks
	Versul Center Create a new VM Storage Profile This list is empty.	Associated VMs	All Running Faile
			My Tasks More Ta My Tasks More Ta My Tasks More Ta My Tasks More Ta
			- 10 Alarms

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:

m ware [®] vSpher	Create New VM Storage I	Profile			?	earch
					ŀ	
Rules and Profiles	vCenter:	VPC4-VCSA -				
The Storage Profiles	Name:	NFS-Storage				cent Tasks
	Description:				i I	Running
	Storage Capabilities:	Clear All Select All		Q Filter	'	
		Name	Туре	(4		
		✓ NFS	User-Defined			
						rk in Progre
						ew VM Stora
						• rms
	•				Þ	New (0)
				OK Cance	əl	

6. Click on OK.

7. 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:

Rules and Profiles	I G VM Storage Profiles			
Transformation of the second s		Q Filter	-	🔻 🗊 Recent Task
r NFS-Storage	Resource	Associated VMs 0	Assoc 0	All Running
				My Tasks 👻
				👻 📝 Work in Pro
				- 🖸 Alarms
				All (0) New (

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

vm	Enable VM Storage Profiles				
	vCenter Server: VCSA 🗸]			
3	Enable or disable VM Storage Profile the cluster must have a license that i	es for a host or a cluster. To enable the ncludes VM Storage Profiles.	feature for a host, its license must in	clude VM Storage Profiles. To enable t	the feature for a cluster, all the
5	Hosts and Clusters:				
	Disable Enable C	•			Q Filter
	Name Enables VM C	torage Profiles on the colocted	Licensing Status	VM Storage Profile Status	Notes
	Resource-Clust entity	torage promes on the selected	All hosts Licensed	Disabled	
	Resource-Cluster2	DC	No hosts	Unknown	
	Hosts in selected cluster:				

- 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.

VMware vCloud Di	rector			administrator	(System Adm	inistrator) Pre	eferences Help -	Logout
System								
Home Manage & Monitor	Administration]						
Manage & Monitor	🙋 vCenters							
Organizations	😨 🌼 -				All	-		୯ 🌚
Cloud Cells	Name	1 A Status	vCenter Server	Port Number	Version	vShield Mana	vCenter Proxy	
Provider VDCs	VCAP-CIA-vC	Actions: VCAP-	10 CIA-vCenter	443	5.1.0	10.	🛃 localhost.localdoma	in
Crganization VDCs	-	Reconnect	Reconnect					
Edge Gateways		Refresh						
		Refresh Storage	Profiles					
Network Pools ::		Enable						
 vSphere Resources 		Disable						_
G vCenters		Detach						_
Resource Pools		Open in vSphere	Web Client					
Hosts		Properties						
Datastores & Datastore C								
E Storage Profiles								_
Switches & Port Groups								
Stranded Items						4 4		NR)
📰 Logs 🔻	r					-		14
0 Running 🥝 0 Failed			VMware v	Cloud Director			Powered by VIIIV	vare [.]

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.

-[47]-

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:

VMware vCloud E	Dir	ector				administrat	or (System Administrato	r) Preferences	Help - Logout
System									
Home 😡 Manage & Monit	or	🍓 Administration							
Manage & Monitor		F Storage Pro	file	5					
Organizations	1	∞ -					All	•	C 0
 Cloud Resources 		News	1.	Devident	Our starting M	Deed	Devisioned	Description	Detertory L 1000
Cloud Cells		Name	1.	Provider v	Organization V	Used	Provisioned	Requested	Datastores
Provider VDCs		F NFS-Storage		1	G @	0.70%	0.70%	0.00%	⊟ 1
Organization VDCs									
Edge Gateways									
🚣 External Networks									
Network Pools	::								
2 vCenters									
Resource Pools									
Hosts									
Datastores & Datastore C									
📑 Storage Profiles									
Switches & Port Groups									
Stranded Items									
Elogs	Ŧ							1-1 of 1	
🗿 0 Running 🔮 0 Failed					VMware vCl	oud Director		Powered	by vm ware

- 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:

System	Storage Profile Prop	erties:	NFS-Storage			3 ×		
🚮 Home 🕠 Manage & Mo								
lanage & Monitor	Name: NFS-Stor	age						
Crganizations	Datastores & Datas	store Cl	usters					
Cloud Resources								Ge
Cloud Cells				All	•	G	ted	Datastores [
Provider VDCs	Name	1 🔺	Storage Used	Requested Storage	vCenter		%	81
Organization VDCs	NFS		0.70%	0.00 Bytes	VCAP-CIA-vCenter			
Edge Gateways								
Letternal Networks								
Network Pools								
vSphere Resources								
Centers VCenters							_	
Resource Pools								
Hosts								
Datastores & Datastor								
Storage Profiles					1-1 of 1			
Switches & Port Group								
Stranded Items					OK	Cancel	pf 1 (D DI

- [48] -

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**:

vm	2	New Distributed Port Group			(?) ₩	Н
	~	1 Select name and location	Configure settings Set general properties of the r	rew port group.		
•		3 Ready to complete	Port binding:	Static binding +		5
E			Port allocation:	Elastic Elastic Elastic Elastic Elastic port groups automatically increase or decrease the number of ports as needed.		
			Number of ports: Network resource pool:	8 ×		
			VLAN			
			VLAN type: VLAN ID:	VLAN • 100 •		
			Advanced			Ire
			Customize default policie	is configuration		Pc
				Back Next Finish C	Cancel	

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.

3. 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:



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

vn	dvSwitch - Edit Settings		(2
	General Advanced	MTU (Bytes): Default max. number of ports per host:	1600 • 512 •	35
		Discovery protocol Type: Operation:	Cisco Discovery Protocol	Por
		Administrator contact Name: Other details:		gre Set
			OK Cancel)

- [52]-

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

Managing vSphere Resources

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:



Managing vSphere Resources

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.

- [57]-

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:

View: Host & Clusters 🗘 🦓	You are logged in	as a System Administrator	Logged in as:admin	Change Password	Logout	<u>Help About</u>
	General A;	pp Firewall Endpoint	SpoofGuard	Network Virtu	alization	
Q	Preparation Network Scop	pes Networks Edges				Refresh
E Settings & Reports						
Data Security	Connectivity Segment					
Service Insertion	Segment IDs & Multic	Edit Settings		×		Edit
Object Library	The pool of segment ID us	Describe a second tip and an		- to this . Chiefd		
Datacenters	Segment ID pool:	manager.	i multicast range uniqu	e to this vShield		
10.	Multicast address range	Segment ID pool: * 50	00-5200			
 □ 10. □ System vDC (69426cdf-fae5-4b □ ○ vcc-org1-vdc (a937126e-7e39-4 		Multicast addresses: * 22	5.1.1.0-225.1.1.255			
🗄 📾 vCloud Connector Node				Ok Cancel	J	

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:

	You	are logged in as a System Ac	Iministrator	- Logg	ed in as:admi	n <u>Change</u>	Password	Logout	Help	About
View: Host & Clusters +	-00							linghing	4	
Q	General	App Firewall	Endp	oint	SpoofGua	rd NG	twork virtu	alization		
Settings & Reports	Preparation	Network Scopes Networks	Edges							Refresh
Straings a hepoto	Connectivity	/ Segment ID								
Data Security										
Service Insertion	Network Co	propertivity for VXI AN Tr	affic					Reso	lve	Edit
Object Library	All hosts in	Prepare Infrastructure For	VXLAN N	etworking					×	
E V Datacenters										
DC	Hosts & Clu	Select participating	Selec	t partici	pating cl	usters			T	J
- I 10		clusters	Select o each clu	ne or more ster, design	clusters to pa ate a distribu	rticipate in V ted switch to	XLAN netwo transport V	rking. For KLAN traffi	с.	
10.		Specify transport							-	
- System vDC (69426cdf-fae5-4b		attributes	Use	Cluster	▲ D	istributed Switch	à	VLAN		
🕀 😓 vcc-org1-vdc (a937126e-7e39-4				nih R	esource d	vSwitch				
will vCloud Connector Node										
						Drové	iour New	t Cana		
						Prev	Nex Nex	Cano		

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

View: Host & Clusters 🗧 🖓	Yo -DC	u are logged in as a Syst	tem Administrator	Logged in as:admin	Change Password	Logout	<u>Help About</u>
Q	Gener	al App Firewa	ll Endpoint	SpoofGuard	Network Virtu	alization	Defrech
Settings & Reports Settings & Reports Service Insertion Datacenters Dotecenters Dotecenters Dotecenters Dotecenters System vDC (69426cdf-fae5-4b B vccorg1-vc	Preparation Connectivit Network C All hosts in Hosts & Cl	Network Scopes Net V Segment ID Prepare Infrastructu Select participatii clusters Specify transport attributes	AN Traffic re For VXLAN Netwo Distributed Sw Can dvSwitcd	rking ransport attrib switches were design v LAN preferred MT tch Teaming P h LACP - Fail Ove Static E LACP - LACP -	utes ated for transporting V U setting for each swit vertige of the set of the set of the set of the set of th	(XLAN traffic tch. MTU (bytes) 1600	Edit
				Previ	ous Next Finis	h Cance	

- 14. Click on the **Finish** button.
- 15. 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**.
- 16. Expand the cluster and do the following:
 - ° Make sure that the status of each ESXi host is **Ready**.
 - ^o 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:

	Add Provider VDC	2 8	Logout
System	Name this Provider VDC Select Resource Pool	Name this Provider VDC A Provider VDC is a group of compute, memory, and storage resources from one vCenter. You can allocate portions of a Provider VDC to your organizations using vCloud Director.	
Some b After yo Quick S First, O O O O Tasks Syste	Add Storage Ready to Complete	Name: Gold-pVDC Description: Image:	
		Back Finish Cancel	nware [.]

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

	Add Provider VDC							3	×	
System Home Some ba After you	Name this Provider VDC Select Resource Pool Add Storage	Select Resource Pool Resource pool supplies the Pro availability (HA) and fault tolerar resources available to its Pay-A Select a vCenter Server and a	ovider VDC Ince (FT). 1 As-You-Go resource p	with compute and memory You can add more than one and Allocation Pool VDCs. ool:	y resources an a resource pool	d vCenter s to a provic	ervices, such as high ler VDC to increase ti	ne	_	
Quick S	Prepare riosts	vCenter	1 🔺	Resource Pool	1 🔺		vCenter Path			
First,	Ready to Complete	bir-1st-1-dhcp439		CIS-Hybrid-Cluster		CIS-Hybr	id-Cluster			
00000		The following external networks	s are availa	VCAP-Cluster	pu selected:	VCAP-CI	uster			
Tasks Syste		Network Selected resource pool: CIS-H	ybrid-Cluste	Gateway	Subnet		DNS			
		Selected resource pool: CIS-H	yonu-ciusu	C 1					•	nware [.]
					Back	Next	Finish	Cancel	J	

— [66] —

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

	Add Provider VDC			3 8	Logout
System	Name this Provider VDC	Add Storage Select storage profiles this provider VDC will offer.		<u>^</u>	
Some bi	Add Storage		All	G	
After you	Prenare Hosts	Storage Profile	Datastores		
Quick S	Ready to Complete	* (Any)	datastore1 (2), NFS-Local (1)		
First,	Ready to complete	Gold	datastore1 (2), NFS-Local (1)		
0					
0					
0				1000	
0		Add Remove			
Tasks					
Syste		Storage Protile	datastore1 (2) NESJ ocal (1)		
В		0014			
4					
I OR			Back Next Finish	Cancel	nware [.]

- 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:

	Add Provider VDC								3 8	Logout
System	Name this Provider VDC Select Resource Pool	Prepare Hosts To use the selected host. This installation	resource po on requires ro	ol's hosts in vClou ot privileges for ea	d Director, ti ich host.	ne system needs to insta	ll the v(Cloud Director agent on	each	
Some ba	Add Storage	There are 1 host(s)	that need to	be prepared.						
Quick S	Prepare Hosts Ready to Complete	One credential for root User Name: Password: A different crede	or all hosts: root	host:						
0		Host	initial for each	Status		root User Name		Password		
Tasks		10		٥		root				
Syste										
						Back	Next	Finish Ca	ncel	n ware [.]

- [67] -



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:

Chapter 3

VMware vCloud D	ire	ector					admi	nistrator	(System	Administrator) Preferences	Help 👻	Logout
System													
付 Home 😡 Manage & Monito	r	🍓 Administratior	ı										
Manage & Monitor		Provider \	/DCs	5									
Organizations	1	+ 🔅-			Manage	Monitor)		All	-			C 😮
Cloud Resources Cloud Cells		Name	1 🔺	Status		Enabl	Org VD	Datastor	Reso	ource Po	vCenter		
R Provider VDCs		Gold-pVDC		0		× .	۵ 🗠	2	\bigcirc	1	🕝 bir-1st-1-dhcp439	9	
Organization VDCs		la Silver		0		×	۵ 🗠	I 1	\bigcirc	1	🕝 bir-1st-1-dhcp439	9	
🦁 Edge Gateways													
Letternal Networks	Ľ												
Network Pools	:												
	Ľ												
2 vCenters	I.												
Resource Pools													
Hosts													
Datastores & Datastore C													
🔁 Storage Profiles	I.												
Switches & Port Groups	t.												
Stranded Items											1.2 of 2		
🔟 Logs	Ŧ										1-2 01 2		
0 Running 😣 2 Failed					4	VMware v0	Cloud Directo	r			Powere	ed by VM	ware [.]

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

VMware vCloud Di	ire	ctor					admir	istrator	(Sys	tem Administrato	or)	Preferences	Help 👻	Logout
System														
Home 😡 Manage & Monitor	r &	🗞 Administratio	n											
Manage & Monitor		Provider \	VDCs											
Organizations	•	+ 🔅-		Manage	Monitor)			All		•			C 3
Cloud Resources		Name	1 🔺	Status	Enabl	Org V	D	Datastor		Resource Po		vCenter		
Provider VDCs	I	Gold-pVDC		Actions: Gol	d-pVDC	2)	2		<i> </i> 1	đ	bir-1st-1-dhcp43	9	
Organization VDCs		Silver		Open)	1		<i>i</i> 1	đ	bir-1st-1-dhcp43	9	
Edge Gateways				New Organizati	on VDC									
🚣 External Networks	E			Enable		1								_
Network Pools ;				Disable										
				Delete										
2 vCenters				Enable VXLAN										
C Resource Pools				Notify										
Hosts				Merge with										
Datastores & Datastore C				Properties										
E Storage Profiles	E													_
Switches & Port Groups														
Stranded Items	H													
🔟 Logs	•											1-2 of 2		
0 Running 🔕 2 Failed				1	/Mware v0	loud	Director					Powere	ed by ທ	nware [.]

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

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

VMware vClou	Merge Provider vDC: 0	sold-pVDC			O	× nces Help + Logout
System	Select the Provider V	DCs to merge with t	his one:	Ali	C	
Home Manage & N	Name	1 A Datastor	Org VD	vCenter		
Manage & Monitor	Silver	I 1	۵٥	🕝 bir-1st-1-dhcp439		
Organizations Cloud Resources Cloud Colls						vCenter
Provider VDGs						dhcp439
Organization VDCs Edge Gateways	📮 Add 📄 💻 Rei	nove				dhcp439
External Networks	Name	Datastor	Org VD	vCenter		
Network Pools	D Silver	1	△ 0	📴 bir-1st-1-dhcp439		
VCenters						
Hosts						
Datastores & Datast	Name and Description	n				
Storage Profiles	Name:	Gol	d-pVDC			_
Stranded Items	Description:					2
📲 0 Running 🔕 2 Fa	MAILEIDE			ОК	Cancel	Powered by VMWare

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:



Managing vCloud Director Resources

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.

Managing vCloud Director Resources

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:

Chapter 3



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

Create Network Pool Wizard		3	()
Network Pool Type Configure VLAN-backed Pool Name this Network Pool Ready to Complete	Network Pool Type A network pool is a collection of virtual machine networks that are available to be consumed by VDCs to create vApp networks and by organizations to create organization VDC networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks. A VXLAN network pool is automatically created when the containing Provider VDC is created.		
	 Select a network pool type from the list below: VLAN-backed Create a network pool backed by a range of VLAN IDs. The VLAN's must be pre-provisioned. Network isolation-backed Create a network pool backed by Cloud isolated networks. A Cloud isolated network spans hosts and provides traffic isolation from other hosts. The system provisions Cloud isolated networks automatically. VSphere port group-backed Create a network pool backed by a vSphere port group. The port group must be pre-provisioned. 		
	Back Next Finish	Cancel	

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.

Create Network Pool Wizard							3 8
	VLAN ID Range						
Network Pool Type	Enter a VLAN ID range (format: 1-1000) and clic	sk Add.				
Configure VLAN-backed Pool	101-105	Add) *				
Name this Network Pool	101 - 105	Modify					
Ready to Complete		Remove					
	Select vNetwork Dist	ributed Switch					
			G		All	1	e
		vCenter	1 🔺 🛄	vDS	1.	vCenter	
	vc0			vpc1-dvs	v	rc0	
		1-1 of 1				1-1 of 1	
	These provider VDCs	will connect to networ	ks allocated from this	new network poo	d:		
			Pro	vider VDC			
	VPC1-pvDC						-
					Back	Next Finish	Cancel

- 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**.

Managing vCloud Director Resources

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:

Chapter 3

New External Network							0
Select vSphere Network Configure External Network Name this External Network	Select vSphere Network An external network uses a network in vSpher an external IPSec-VPN network that connects If you don't see the vCenter you need: attach Select vCenter and vSphere Network	re to connect to a net s to a given organizati n a different vCenter.	work outside of your cloud.	The netwo	rk can be a pu	blic network such as the Internet, c	or even
leady to Complete		G					C
	vCenter	1 🛦 🛄	vSphere Network	1 🔺	VLAN	Datacenter	1 10
	vc0		Mgmt		14	dc	
			NFS		5	dc	
			vMotion		6	dc	
	These provider VDCs will connect to this new VPC1-pvDC	external network:				1-3 of 3	M
					Back	Next Finish (Cancel

- 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:

New External Network		Add Subnet			 Image: Second sec		0	8
Select vSphere Network Configure External Network	Configure External Network Specify the network settings for address ranges or IP address	Gateway address: Network mask: Brimary DNS:	10.10.10.253 255.255.255.0	s	8	supply IP addresses to VM	s in organizations by adding IP	
Name this External Network Ready to Complete	Gateway address	Secondary DNS: DNS suffix: Static IP pool:				Secondary DNS	Static IP Pools	
		Enter an IP range (fo address and click Add 10.10.10.101-10.10. 10.10.10.101 - 10.	rmat: 192.168.1.2 - 19 J. 10.200 10.10.200	2.168.1.100) or Add Modify Remov				
	Add Modify	Total: 100		ок	ancel	Back	iext Finish Cance	91

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

New External Network	New External Network 🥥 😣								
Select vSphere Network Configure External Network	Configure External Net Specify the network setti address ranges or IP ad	twork ings for this new externa dresses using the Static	I network. You can have th IP Pool control.	is network automatically	supply IP addresses to	o VMs in organizations by adding IP			
Name this External Network	Gateway address	Subnet Mask	IP Pool (Used/Total)	Primary DNS	Secondary DNS	Static IP Pools			
Ready to Complete	10.10.10.253	255.255.0	0.00%			10.10.10.10.10.10.200			
					Back	Next Finish Cancel			

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

New External Network						3					
Select vSphere Network Configure External Network Name this External Network Ready to Complete	Ready to Complete You are about to create an external network. Review these settings and click Finish to create it. Network name: External-ProviderNW Description: vSphere network: VSphere network: Mgmt IP subnets: IP										
	Gateway address	Subnet Mask	Primary DNS	Secondary DNS	Static IP Pools						
	10.10.10.253	255 255 255 0			10,10,10,101-10,10,10,200						
				Back	Next Finish	Cancel					

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:
 - ^o 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.
 - ^o The storage lease setting: The 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	 (a) (b) (c) (c)
New Organization Name this Organization LDAP Options Add Local Users Catalog Email Preferences Policies	Rame 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: Vicloud-Essential 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://dit.org/organization.voc/anst.prov.div.organization/vc/anst.prov.div.organization URL:
Ready to Complete	Inttps://d1bsuuti-vcd-vip.vcdsiabs.vmware.com/44.s/cloud/org/vCloud-Essential/ Organization full name: vCloud Director Essentiats Appears in the Cloud application header when users log in. An organization administrator can change this full name. Description:
	Back Next Finish Cancel

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

New Organization	 8
Name this Organization	LDAP Options An organization can use an LDAP service as the directory of users and groups that can be added to the organization.
LDAP Options	What is the source of users for this organization?
Add Local Users Catalog	Do not use LDAP The organization administrator creates VCD users who are private to the organization. Groups cannot be created.
Email Preferences	VCD system LDAP service Use when this organization is a member of your Cloud provider company.
Policies Ready to Complete	Distinguished name for OU: Example: ou=Users,dc=example,dc=local
	Custom LDAP service Use when you've arranged with the organization to use their own directory service. Before you can use this option, you must configure your Cloud system LDAP service to link to their LDAP service.
	Back Next Finish Cancel

- 7. Under the Add Local Users tab, click on Next.
- 8. Under the Sharing tab, select Allow sharing catalogs to other organizations.
- 9. 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:

New Organization			×
Name this Organization LDAP Options Add Local Users Catalog Email Preferences Policies Ready to Complete	Catalog Configure share and publish settings for this organization. Sharing Select the sharing capability for this organization. ✓ Allow sharing catalogs to other organizations Select to allow users to share catalogs to other organizations in this cloud. If not selected, users can still share catalogs within their organization. Publishing Select the publishing capabilities for this organization. ✓ Allow publishing external catalogs Select to allow users to publish catalogs to organizations outside of this cloud. ✓ Allow subscribing to external catalogs Select to allow users to subscribe to catalogs outside of this cloud.		-
	Back Next Finish	Cancel	

- [84] -

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

New Organization		×
	Leases	1
Name this Organization	Specify the maximum time that vApps and vApp templates can run and be stored in this organization's VDC(s).	
LDAP Options	vApp leases:	
Add Local Users	Maximum runtime lease: 7 V Days V	
Catalog	How long vApps can run before they are automatically stopped.	
Email Preferences	Maximum storage lease: 30 V Days V	
Policies	How long stopped vApps are available before being automatically cleaned up.	
	Storage cleanup: Move to Expired Items	
Ready to Complete	vApp template lease:	
	Maximum storage lease: 90 V Days V	L
	How long vApp templates are available before being automatically cleaned up.	
	Storage cleanup: Move to Expired Items	
	Default Quotas	
	These values suggest the default quotas for how many VMs a User can store and power on in this organization. They can be changed by an organization administrator.	
	All VMs quota:	
	Running VMs quota: O 1 🔅 O Unlimited	Ŧ
	Back Next Finish 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:

New Organization			2	×
	Description:			*
Name this Organization	LDAP option:	Do not use LDAP		
LDAP Options	Local users:	0		
Add Local Users	Catalog sharing:	Cannot share catalogs.		
Catalog	Policies:	vApp leases:		
Email Dreferences		Maximum runtime lease:	7 Days	
Email Preferences		Maximum storage lease:	30 Days	
Policies		Storage cleanup:	Flag for deletion	
Ready to Complete		vApp template lease:		
		Maximum storage lease:	90 Days	
		Storage cleanup:	Flag for deletion	::
		Stored VM quota:	Unlimited	
		Running VM quota:	Unlimited	
		Password lockout enabled:	false	
		Invalid logins before lockout:	5	
		Account lockout interval (minutes):	10	
			Allocate resources to this organization after the wizard is finishe	d. 🔻
			Back Next Finish Cancel	

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:

VMware vCloud Dir	rector				administrato	or (System Administrato	r) Prefere	nces Help - Logout
System								
Home 😡 Manage & Monitor	🍓 Administration							
Manage & Monitor	Organization VDC	s						
Organizations	+ 🔅-		Ma	anage Monitor		All	•	C' 🥹
Cloud Cells	New VDC 1	Status	En	Allocation Model	Organization	Provider VDC	Resource	vCenter
Provider VDCs	4 05	0	1	Allocation Pool	05	VPC1-pvDC	<i>i</i> 1	CO vc0
Organization VDCs	4 VCD	0	× .	Allocation Pool	🛆 VCD	VPC1-pvDC	<i>i</i> 1	vc0
Edge Gateways	vmware	۲	× .	Pay-As-You-Go	a vmware	VPC1-pvDC	🥝 1	CO vc0
External Networks ::								
Network Pools								
▼ vSphere Resources								
Page VCenters								
Resource Foois								
Datastores & Datastore C								
Storage Policies								
Switches & Port Groups							1-3 of 3	3
👬 0 Running 🔮 0 Failed				VMware vCloud Dir	ector			Powered by VMWare

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

New Organization VDC							9 8
Select Organization Select Provider VDC	Select Organization An organization VDC provides an organization For which organization is this Organization V	on with the DC being	resources it needs. created?				
Select Allocation Model				All	•		G
Configure Allocation Model	Organization	1 🔺	Full Name	E.		Description	
Allocate Storage	O5						
Select Network Pool & Services	🛆 VCD						
Configure Edge Gateway	CDT						
Name this Organization VDC	🛆 VC						
Ready to Complete	Cov vCloud-Essential	vC	Cloud Director Essentials				
	C vmware						
					•	1-6 of 6	
					ack N	ext F	inish Cancel

7. 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:

New Organization VDC								3
Select Organization	Select Provider VDC You can allocate resou	irces to an org	anization by cre	ating an Organization VE	DC that is partitioned from a Pro	vider VDC		
Select Provider VDC	Select the Provider VD	IC.						
Select Allocation Model					All	•		G
Configure Allocation Pool Model	Provider VDC 1	Status	Enabled	Processor (Used/Total)	Memory (Used/Total)		Storage (Used/Total)	
Allocate Storage	D VPC1-pvDC	0	~	25.51%	27.64%		0.56%	J
Select Network Pool & Services								
Configure Edge Gateway						1.	1 of 1	M
Name this Organization VDC	The following networks	are available	to the Provider	VDC you selected:				
Ready to Complete	Network			Gateway	Subnet		DNS	
	- VPC1-ExtNW		10.		255.255.248.0	10	. , 10	
	Selected Provider VD0	C VPC1-nvD0	which has 1 re	esource pool(s)				
			, 111011100 110	5500100 (500(5)				
					Back	Ne	d Finish	Cancel

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



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							3	
	CPU allocation:	18.71	GHz	2				
Select Organization	The maximum amount of CPL	available to the virtual mach	ines ru	nning within this organization	VDO	C (taken from the supporting provi	der VDC, VPC1-pvDC).	
Select Provider VDC	CPU resources guaranteed	50 🔺 % (9.36GI	Hz, 10% of available Provid	der \	/DC capacity of 93.54GHz)		
Select Allocation Model	The percentage of the resource	es guaranteed to be availabl	e to virt	ual machines running within i	it.			
Configure Allocation Pool Model	vCPU speed:	1 GHz						
Allocate Storage	This value defines what a virtu would consume a maximum o	al machine with one vCPU w f twice this value.	vill cons	ume at maximum when runni	ing w	vithin this organization VDC. A virt	ual machine with two vCPU:	S
Select Network Pool & Services	Memory allocation:	70.26	GB					
Configure Edge Gateway	The maximum amount of men	nory available to the virtual m	achines	running within this organizat	tion \	/DC (taken from the supporting p	rovider VDC, VPC1-pvDC).	
Name this Organization VDC	Memory resources guarant	eed: 50 🔷 % (35.130	6B, 10% of available Provid	der \	/DC capacity of 351.29GB)		
Ready to Complete	The percentage of the resource	es guaranteed to be availabl	e to virt	ual machines running within i	it.			
	Maximum number of VMs:	• 100 🗼	🔵 Un	limited				
	A safeguard that allows you to	control the maximum number	er of virl	ual machines in this organiza	ation	VDC.		
	The committed resources	from Provider VDC, 'VP	C1-pvD	C' using these allocation	1 set	ttings:		
	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%)	
	1.4		đ			Back Next	Finish Can	cel

- 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:

New Organization VDC					(2)
Select Organization Select Provider VDC	Allocate Storage You can control the storage alloca	tion to the organization by settir	ng a limit, enabling thin	provisioning of storage and fast provisioning	g of virtual machines.
Select Allocation Model	Cleane	- Define	1.	Auszlahle Chromen	C m
Configure Allocation Pool Model	storag	e Policy	12 113 12 / 42	Available Storage	
Allocate Storage	199D		42,110,12142		
Select Network Pool & Services					
Configure Edge Gateway					
Name this Organization VDC					
Ready to Complete	🐺 Ada 🛛 📟 Remove				
	Storage Policy	Available Storage		Storage Limit	
	SSD	42,113.12 / 42,351.75 GB	8470.35	GB (requires 20% of 42,113.12 GB	available storage)
	Defending for a firm				
	Detault instantiation policy: SS	D	•		
				Back Next Fin	ish Cancel

- 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:

New Organization VDC					3	8
Select Organization Select Provider VDC Select Allocation Model Configure Allocation Pool Model Allocate Storage Select Network Pool & Services Configure Edge Gateway Name this Organization VDC Ready to Complete	Select Network Pool & Services Select the network pool that provides vApp networks to this organization VDC and specify the vApp network quota from this pool. Network pool: VPC1-pvDC-VXLAN-NP • • A VXLAN network pool is automatically created when the containing Provider VDC is created. Network Quota Total available networks: 100000 Quota for this organization: 1000 • • • 3rd Party Services Network level services available with the selected network pool:					- :
	Enable	Service		Template		
				Back Next Finish	Cancel)

- [92] -

- 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:

New Organization VDC				3 🛛
New Organization VDC Select Organization Select Provider VDC Select Allocation Model Configure Allocation Pool Model Allocate Storage Select Network Pool & Services Configure Edge Gateway Name this Organization VDC Ready to Complete	Name this Organization VDC Enter the name and description for this new Organization VDC. Name: vCloudEssential-OrgvDC * Description: Image: Image: Image: Enabled			
			Back Next Finish C	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.

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

VMware vCloud Dir	rector administrator (System Administrator) Preferences Help + Logout
System Elastic ×	
😭 Home 🛆 My Cloud 目 Cat	talogs K Administration
Administration	1 Elastic
	vApps vApp Templates Media Storage Profiles Edge Gateways Org VDC Networks Resource Pools
✓ ← Virtual Datacenters Recent Items	+ ŵ•
🝙 Elastic	Add Gateway 1 Status Mul5-Interface Mode # Used NICs # External Networks # Organization VDC Networks
✓ Members	
Users	
Lost & Found	
▼ Settings	
General	
Email	
2 LDAP	
Policies	
Guest Personalization	
@ rederation	
metauald	
	0-0 of 0
	4 B
0 Running 🔮 0 Failed	VMware vCloud Director Powered by VMWare'

- 8. On the **Configure Edge Gateway** screen, click on the **Configure IP Settings** section. Use the other default settings and click on **Next**.
- 9. On the **Configure External Networks** screen, select the external network and click on **Add**.
- 10. 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:

	New Edge Gateway					😮 🙁 Logout
		Configure External Netwo	rks			^
Syster	Configure Edge Gateway	Select the external networks	s to which the new edge gatev	vay can connect.		
Hd Hd	External Networks	If the external network is no	t listed, you have to create a	a new external network		
Admin	Configure IP Settings			All	•	C
- Clou	Name and Description	Name 1	IP Pool (Used/Total)		vSphere Network	
	Summary	🧏 vpc2-extnl-nw	<mark>3</mark> 5.00%	TenantVM-N	letwork	
						letworks
🗕 Mem						
à						
- Setti		📮 Add 🛛 💻 Remove			1-1 of 1	
d		Magaa	IR Real (Lead Total)	Pahara Naturali	Default Calauras	
6		- vnc2-extnl-nw	35 00%	Tenant/M-Network	Denault Gateway	
6		-22 1002 00001111	0.0075	Tendire in rection	•	
i i i i i i i i i i i i i i i i i i i						
á						
á		Lies default geteureu fer l	DNS Balay			
		Use the above selected defaul	ווש העפומא. It gateway for DNS relay. Togethi	er these parameters will be use	d for the gateways' default routing a	nd DNS
		forwarding.			· · ·	v
				Back	Next Finish	Cancel (are

- 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:

Edg	ge Gateway Pro	operties: ne	w-edge							3	(*)	Logou
	General	onfigure Ext	ernal Networks	Configure IP Setting	gs Sub-Allocat	e IP Pools Co	nfigure Rate Lim	its Syslog S	erver Settings			
						All	•			G	•	
	Name	1 🔺		IP Pool (Used/Total)			vSphere Ne	twork				
	🚽 vpc2-extnl	l-nw		35.00%		TenantVM-Net	work					letwork
	Add Na	- Remove) IP P	ool (Used/Total)	vSphere N	etwork		1-1 of 1 Default Gateway				
	🚽 vpc2-extnl	I-nw		35.00%	TenantVM-Netw	vork		۲				
	Use default Use the above s	gateway for selected defau	DNS Relay. It gateway for DNS	relay. Together these pa	rameters will be use	ed for the gateway	s' default routing and	d DNS forwardin	g.		Ŧ	
									ок	ancel		vare

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:



-[102]-

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

Co	onfigure Services: new-edge				0	
5) G	DHCP NAT Firewall Static Rou Dynamic Host Configuration Protocol (Dh manage IP address ranges and lease pa	ting VPN Load Balancer ICP) automates IP address assignment rameters for each of the organization vD	to virtual machines conne	ected to organization vDC networks. Yo this edge gateway.	You can configure and	
	Enable DHCP	IP Ranne	Default Lease	May Lease	Fnabled	
	r approve err	in tearinge	Densen Escape	HAR COURT		
				Add	dit Delete	
					OK Cancel	

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

Con	nfigure Services: new-edge						0	(8) 0
S)	DHCP NAT Firewall Static Dynamic Host Configuration Protocc manage IP address ranges and leas	Routing VPN Load Balancer (DHCP) automates IP address as e parameters for each of the organi	ignment to virtual machines co zation vDC networks connecte	onnected to org d to this edge g	anization vDC networ ateway.	ks. You can config	gure and	
-	Applied On	IP Range Add DHCP Pool	Default Lease	(*)	Max Lease	Enable	d	
•		DHCP automatically provides I ✓ Enable pool Applied on: routed-or IP range: 192.166. Default lease time: 3600 Max lease time: 7200	2 addresses to VMs. <u>a</u> -mw ▼ 1.100-192.168.1.200 ★ Seconds ★ Seconds OK Cance	•	Add			
						ОК	Cance	

-[103]-

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:

Chapter 4



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



-[105]-

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:

	Configure Services: new-edge				0	X	put
Sy	DHCP NAT Firewall St	atic Routing VPN Load E	alancer				
Ma	IPSec VPN service helps you o	Configure Public IPs		0	ways in this organization, across		
	Enable VPN	Specify the public IPs for ea	ch of the external ne	tworks.			Ξ.
	Configure Public IPs	External Network	IP Address	Public IP			ks.
	Public IPs can be configured for	vpc2-extnl-nw	10.	10.			
	Name Local				eer Network Peer Organization		
-							
							ш.
							ш.
							.
							.
				OK Cancel	L. Delete Peer settings.		
						_	
					OK	el	

- 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:

	Configure Services: new-edge	Add a Site-to-Site VPN configuration	u 😣 😒
S	DHCP NAT Firewall Static Ro	Name: Site-To-Site *	
Ma	IPSec VPN service helps you create se		ways in this organization, across
		Enable this VPN configuration Establish VPN to: a network in this organization	
	Public IPs can be configured for each o	Local & Peer Network in this organization a network in another organization a network in another organization	ks
F	Name Local End Point	Peer Edge Gateway:	er Network Peer Organization
		Local Networks: Peer Networks: routed-org-nw (192.168.100.0/24	
•			
		VPN connection settings	
		Local Endpoint: vpc2-extnl-nw v Use Public IP	
		Peer Endpoint:	
1		Shared Key:	····
		ОК	Cancel OK Cancel

-[107]-

- 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:

DHCP NAT Firewall St	atic Routing VPN Load Balancer	
Static routes allow traffic betwee	n networks. Ensure that the firewall rules are configured appropriately.	
Enable static routing		
Name	Add Static Route	
	Applied any and with my	
	Name: voc2-extri-nw	
	Notwork:	
	Fiter network address in CIDR format For example: 192 168 2 0/24	
	Next Hop IP: 192.168.1.1 *	
	Enter next hop router IP address. For example: 192.168.0.100.	
	OK Cancel	
	Add Edit	

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 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 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:

	Edit Firewall Rule		3 8				
Rules can be added dropping them at the Carl Enable firewall Default action Applicable to traffic tha	Enabled Name: Source:	Firewall_10.10.10.10 _Any Any Valid values can be IP address, CIDR, IP range, "any", "internal"	*	les can be chang r dropping them	ed by selecting a into a different lo	one or more cation withir	rules, dragging and n the list.
Rule Id	Source port:	and "external".		Protocol	Action	Log	Enabled
1	Destination:	10.10.10.20	*	TCP	Allow	(#)	4
	Destination port: Protocol: Action: I Log network tra	Valid values can be IP address, CIDR, IP range, "any", "internal" and "external". 443 TCP Allow Deny dflc for firewall rule	Cancel				Edit Dalate
		ОК	Cancel		Ac	l	Edit Delete

- 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.

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

VMware vCloud Dir	ector				adminis	trator (System A	Administrator)	Pref		Help 🗸 Logout
System vcc-vdc1 ×										
付 Home la My Cloud 🗎 Cat	alogs 🖓 Administra	ation								
Administration	强 vcc-vdc1									
	vApps vApp Te	emplates Media	Storage Profile	es Edg	e Gatewa	ys Org VDC N	etworks Re	source P	ools	
✓ → Virtual Datacenters Recent Items	+ 🔅-					All	•			C 3
rcc-vdc1	Name	1 A Status	Gateway Ad	dress	Туре	Connected To	IP Pool (Used	Total)	Shared	Owner 🛄
- Members	d routed-org-nw	Actional rout	400.400.4/	p.1/24	Routed	🥥 new-edge	2.44%	-	-	vcc-vdc1
Groups	👄 vcc-vdc1-defau	Configure Service	ea-org-nw	1/24	Isolated		0.00%		-	vcc-vdc1
Lost & Found		IP Allocations								
✓ Settings		Connected vApp	8							
i General		Reset Network		-						
iger Email		Open in vSphere	Web Client							
<i>∰</i> LDAP		Properties								
Policies				-						
Guest Personalization										
# Metadata										
-								1-2	of 2	
🗿 0 Running 🔮 0 Failed			VMware	vCloud	Director				Powere	d by vm ware [.]

- 7. Go to the **Firewall** tab and click on **Add**. Here, specify a name for the firewall rule.
- 8. Specify the source IP address and the source port.
- 9. 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.
- 10. Specify the destination IP address and the destination port.
- 11. 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.
- 12. Specify the protocol and its action.
- 13. A firewall rule can allow or deny traffic that matches the rule. Choose the type of acceptance here.
- 14. Select the **Enabled** checkbox.
- 15. 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.
- 16. 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.

Chapter 4



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:

	Config	gure Services: new-edge		3 🛛	out
S		Edit Destination NAT Rule			
Ad	N S ad	A destination NAT rule changes inbound packets. Use the Applie rule. Use the Original (External) addresses from that network to IP/range control to specify a ran	the destination IP address and, optionally, port of d on control to specify a network on which to apply the IP/range control to specify a range of destination IP which the rule applies. Use the Translated (Internal) e of IP addresses to which destination addresses on	IP	
		inbound packets will be translate specific port or ICMP packet typ	d. You can optionally constrain matching packets to a P Translated Port Protocol Er	habled	
	1	Applied on:	vpc2-extnl-nw v	~	
-		Original (External) IP/range:	10.0.101 *		cs
		Protocol:	TCP 👻		
			Original port: 443		
-			ICMP type: ANY		
		Translated (Internal) IP/range:	172.16.0.101 *		
		Translated port:	443 💌		
		Enabled			
			OK Cancel		
		<u> </u>	Add SNAT Add DNAT Edit	Delete	
			ок	Cancel	e.

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:



-[117]-

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:

DHCP NAT	Firewall Static Routing VPN Load Balancer
Network Address Source NAT (SN	Translation /NATL modifies the source/destination IP addresses of parkets arriving to and leaving from this Edge Gateway. Add Source NAT Rule
Applied On	A source NAT rule changes the source IP address of outbound packets. Use the Apolled on control to specify a network on which to apoly the Protocol Enabled
vpc2-extnl-nw	nule. Use the Original (Internal) source IP/range control to specify a range of source IP addresses from that network to which the rule applies. Use the Translated (External) source IP/range control to specify a range of IP addresses to which source addresses on outbound packets will be translated. For more information, see the Help.
	Applied on: routed-org-nw
	Translated (External) source IP/range: 10.0.0.101 *
	OK Cancel
	Add SNAT Add DNAT Edit Delete

-[118]-

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:

	New Organization VDC N	letwork					3	- Logout
System v	Select Network Type Name and Description Ready to Complete	Select Network Type Create a network for use by vApps in this virtual datacenter. You can create a routed network that provides controlled access to machines and networks outside of the VDC via an edge gateway, or an isolated network that only machines in this VDC can connect to. You can also create a network that connects directly to an external network. O Create an isolated network within this virtual datacenter.						
- Members			work by connecting to	All			G	er
		Name 1	# External Networ	# Organization VD	Available	e Networks		¹¹ :1
A Gro		new-edge	- <u>la</u> 1	9_1	8			51
& Los								
di Ger								
a© Em;								
<i>i</i> <i>i</i> → LD/					1-1	l of 1		
a Poli		0.0						
a Gue		 Connect directly to 	an external network:					
a Fed				All	•		C 📀	
@ Met		Name 1 🔺	IP Pool (Used/Total)) v	Sphere Network	VCenter		
600			<mark>3</mark> 5.00%	🚨 Tenai	ntVM-Network	🛃 VPC2-VCSA		
27 op.								
20 Ru					Back	t Finish	Cancel	invare

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

- 9. Specify a name for the external organization network and description (This is optional.).
- 10. 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.
- 11. Review the information and click on **Finish**.

Configuring a routed organization network

Execute the following steps to configure a routed organization network:

- 1. Start a browser. Go to the URL of the vCD server, 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.
- 6. Click on the green-colored + sign. You will see a screen similar to the what's shown in the following screenshot:

	New Organization VDC N	letwork				3 🛛	- Logout
System v	Select Network Type	Select Network Ty Create a network fo	pe r use by vApps in this vi	rtual datacenter.			
Administrat	Configure Network Name and Description Ready to Complete	Network You can create a routed network that provides controlled access to machines and networks outside of the VDC via an edge gateway, or an isolated network that only machines in this VDC can connect to. You can also create a network that connects directly to an external network. Omplete O create an isolated network within this virtual datacenter. Image: Create a routed network by connecting to an existing edge gateway:					
Rec							
♥ Members Use Gro		Name	1 🔺 # External Networ	# Organization VD	Available Networks		51 51
≗ Los							
ې Em LDA کې Poli		Connect directly	to an external network:		1-1 of 1		
in Gute and A		Namo 1 🛦	IP Pool (Used/Total)	All vi	Sphere Network VCe	C @	
ugr		- vpc2-extn	<mark>3</mark> 5.00%	🗳 Tenal	ntVM-Network	/CSA	
🗿 0 Ru					Back Next Fini	sh Cancel	m ware [.]

- 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**:

	New Organization VDC Network				
		Configure Network		^	
System	Select Network Type	Enter the network settings of the new organization VDC network for this virtual datacenter.			
付 Home	Configure Network	Gateway address: 192 168 100 1	*		
Administrat	Name and Description	Network mark:			
- Cloud Res	Name and Description	14etwork midsk. 255.255.255.0	*		
🔫 🕋 Virt	Ready to Complete	Use gateway DNS			
Rec		Select this option to use DNS relay of the gate	away. DNS relay must be pre-configured on the gateway.	C 🕲	
		Primary DNS: 192.168.100.1		er 🛛 🛄	
- Members		Secondary DNS:		p1	
📇 Use		DNS suffix:		:: :1	
📇 Gro					
👗 Los		Static IP pool:			
✓ Settings		Enter an IP range (format: 192.168.1.2 - 192.1	168.1.100) or IP address and click Add.		
eer وي الم		192.168.100.100 - 192.168.100.200	Add		
@" EIII -@ L D.4		192,168,100,100 - 192,168,100,200	Modify		
Poli			Demons		
a Gue			Remove		
i Fed					
a Met					
💭 0 Ru				mware ⁻	
			Back Next Finish	Cancel	

- 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:

	New Organization VDC N	etwork				3	- Logout	
System v	Select Network Type	Select Network Type Create a network for u	se by vApps in this vi	irtual datacenter.				
Administrat Cloud Res Virt	Name and Description Ready to Complete	You can create a routed network that provides controlled access to machines and networks outside of the VDC via an edge gateway, or an isolated network that only machines in this VDC can connect to. You can also create a network that connects directly to an external network.						
Rec ■ • • • • • • • • • • • • •		Create a routed net	work by connecting to	All		G		
🖁 Use 🍰 Gro 🔒 Los		© new-edge	#External Networ	9 Organization VD	Available Networks		51	
✓ Settings Ø Ger Ø Em								
Poli		Connect directly to an external network:						
i Gue i Fed i Met		Name 1 🛦	IP Pool (Used/Total	All ()	Sphere Network	VCenter		
🗿 0 Ru		- 🛃 vpc2-extn	35.00%	🔬 Tenar	Next	C2-VCSA	m ware	

- 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

Managing Catalogs and vApps

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:



[130]-

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 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.
Managing Catalogs and vApps

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:

VMware vCloud Di	irector						administrator (System.	Administrato	or) Prefe		ip 🕶 Logout
System											
😭 Home 😡 Manage & Monito	🛗 Home 😡 Manage & Monitor 🖓 Administration										
Manage & Monitor	🛆 Org	anizations									
📥 Organizations	+ 🔅	•					All		•		C 😮
Cloud Resources		Name	1 🔺	Enabl	VDCs	Can Publi	Can Publish Externa	Catalo	vApps	Running V	Users 🛛
Provider VDCs	۵ 1-05	Actions: 1-05		× .	④ 1	×	-	1	器 23	di 22	🔓 3
Crganization VDCs	l-10	Open		× .	@ 1	-	-	0 🔝	28 o	🗗 0	🔓 2
🥺 Edge Gateways	l 1-15	Allocate Resources		×	@ 1	-	-	0 🔝	26 0	🗗 0	🔓 2
-ze External Networks		Enable		× .	@ 0	-	-	0	28 o	🗗 0	🖁 1
Network Pools		Disable		× .	@ 0	-	-	0	3E 0	di 0	å o
		Delete		× .	@ 1	-	-	🗐 0	26 0	🗗 0	å 1
Resource Pools	vCloud	Properties		× .	@ 1	×	×	0	38 0	d 0	å 1
Hosts	🛆 vmwar	e_service		× .	@ 1	~	×	1	38 o	🗗 0	å 1
Datastores & Datastore (
📑 Storage Policies											
Switches & Port Groups	_										
Stranded Items	•								1-4	3 of 8	
🗿 0 Running 🔮 0 Failed]			¥	VMware vCI	oud Director				Powered by	vm ware [.]

- 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:

VMware vCloud Di	rector administrator (System Administrator) Preferences Help +	Logout
System 1-05 ×		
付 Home 🛆 My Cloud 🗎 Ca	atalogs 🚳 Administration	
My Cloud	🖁 vApps	
vApps	🔶 🎲 🧏 🔽 🔕 🥥 🔕 🔯 🗸 🗛 🖓 🖓	C 😮
Expired Items	Consoles Build New vApp 1 A Status Shar O Created On VDC	
Logs	38 esxi-Tenant1 Running - 🔮 dr. 03/14/2014 10:40 AM 🚳 1-05	^
	BE esxi-Tenant1 Running -	
	86 esxi-Tenant1 Running - 🖁 dr. 03/14/2014 12:35 PM 🚳 1-05	
	8 esxi-Tenant1 Running - 🖁 dr. 03/14/2014 12:37 PM 🚳 1-05	
	🔀 esxi-Tenant1 Running – 🔓 dr. 03/14/2014 12:37 PM 🚳 1-05	7
	I 1-6 of 23	
🗿 0 Running 🔮 0 Failed	Vilware vCloud Director Powered by VII	ware [.]

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:

♦ VM	New vApp		۲	
VM System 1	New vApp Select Name and Location Add Virtual Machines Configure Resources Configure Virtual Machines Configure Virtual Machines Ready to Complete	Select Name and Location A vApp is a cloud computer system that contains one or more virtual machines. Describe this vApp and configure its Virtual Datacenter and lease settings. Name: VCD-Essecntial-vApp * Description: Virtual Datacenter Virtual Datacenter (VDC) in which this vApp is stored and runs when it is started. Virtual Datacenter (VDC) in which this vApp is stored and runs when it is started. Leases Runtime lease: NeverExpires V Hears V How long this vApp can run before it is automatically stopped. Storage lease: NeverExpires V Hears V	× *	Logout
🖏 0 Ru		When this vApp is stopped, how long it is available before being automatically cleaned up. Back Next Finish Cancel		mware

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:

VM	New vApp								 (*) 	Logout
System 1	Select Name and Location Add Virtual Machines	Add Virtual Machines You can search the cata new VM and install an o	ilog for virtual perating syste	machines to add em.	to this vApp or ac	dd a	new, blank VM. Once the vApp is	created, you can powe	r on the	
My Cloud	Configure Resources	Look in: 🚯 Public Ca	talogs	-			All 🔻		G	-
🗗 VMs	Configure Virtual Machines	Name 1 🛦	os	Gold Master	vApp		Created On	Disk Info		G
Z Expired	Configure Networking	w2008r2-stnd	Microsoft W	-	w2008r2-stnd	рι	02/13/2014 3:45 PM	40.00 GB	-	
📰 Logs	Ready to Complete	W2K12-STD-64BIT-SC	Microsoft W	-	W2K12-STD-6	рι	02/14/2014 11:01 AM	40.00 GB	::	
		W2K12-STD-64BIT-SC	Microsoft W	-	W2K12-STD-6	рι	02/13/2014 11:13 PM	40.00 GB		
		W2K12-STD-64BITv2	Microsoft W	-	W2K12-STD-6	рι	02/13/2014 4:12 PM	40.00 GB	-	
		📮 Add 🛛 🗕 Rem	ove				6-10	of 13		
		Name	os	Gold Master	vApp		Created On	Disk Info		
		VCVA	SUSE Linux	-	vCVA	dr	03/11/2014 1:08 PM	125.00 GB		
		w2008r2-stnd	Microsoft Wi	-	w2008r2-stnd	рι	02/13/2014 3:45 PM	40.00 GB		
										-
		💠 New Virtual Machin	e							
0 Ru							Back Next	Finish	Cancel	m ware [.]

- 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:

Chapter 5

► VM	New vApp			3	Logout
System 1	Select Name and Location Add Virtual Machines	Configure Resources Select what Storage Policies this vApp's virt	ual machines will use when deployed.		
My Cloud	Configure Resources	Virtual Machine	Storage Policy	Template VM Default Storage Policy	
VApps	Configure Virtual Machines	vCVA *	SSD-Accelerated v		C 0
Logs	Configure Networking	w2008r2-stnd *	SSD-Accelerated 💌		^
	Ready to Complete				
					•
0 Ru				Back Next Finish Cancel	m ware [.]

- 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:

♦ VM	New vApp						3	۲	Logout
System 1 My Cloud VApps B VMs	Select Name and Location Add Virtual Machines Configure Resources Configure Virtual Machines	Configure Virtual Name each virtua machines after yo Show network Adapter choice choosing among	Machines I machine and sele u complete this wiz adapter type can affect both network adapter	orking performan support for vari	to which you want it to connect the and migration compatibility. Co	ct. You can configure	additional properties for virtual		C 3
Expired	Custom Properties	Virtual Machine	Computer Name	Primary NIC	Network Adapter Type	Network	IP Assignment		
E Logs	Configure Networking Ready to Complete	 [™] vCVA [™] [™] w200 [™] 	vCVA-001-0	NIC 0 NIC 0	VMXNET 3 *	None None 1-05-default-iso Add Network	iated •		-
🖓 0 Ru						Back	Next Finish Cancel		m ware [.]

- 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:

Chapter 5

♦ VM	New vApp				9	Logout
System 1 Home My Cloud VApps Ws	Select Name and Location Add Virtual Machines Configure Resources Configure Virtual Machines	Ready to Complete You are about to create a vA Name: Description:	pp with these specifications. Review th vCD-Essecritial-vApp	e settings and click Finish.		 C @
Logs	Custom Properties Configure Networking Ready to Complete	Owner; Virtual datacenter: Runtime lease: Runtime lease expiration: Storage lease; Storage lease expiration: Networks - 1:	system 1-05 Never Expires Never Never Expires Never 1-05-default-routed			
		VMs - 2:	Virtual Machine vCVA w2008r2-stnd	Guest OS SUSE Linux Enterprise 11 (64-bit) Microsoft Windows Server 2008 R2	Storage Policy SSD-Accelerated SSD-Accelerated	-
🗿 0 Ru				Back	Next Finish Cancel	m ware [.]

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:

VMware vCloud Dir	ector administrator (System Administrator) Prefe	erences Help - Logout
System 1-05 ×		
🕼 Home 🛆 My Cloud 🗐 Ca	talogs 🛛 🍇 Administration	
My Cloud	CD-Essecntial-vApp Stopped	
▼ ₩ vApps	vApp Diagram Virtual Machines Networking	
Recent Items	°a 1 O O S \$a	C' 🥹
≩ Expired Items ☐ Logs	VCVA W2008r2-stnd	
		¥
0 Running 🔮 0 Failed	VMware vCloud Director	Powered by VMWare

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.

Managing Catalogs and vApps

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.

 Edge Gateway

 Organization VDC Network (10.10.10.0/24)

 vApp
 vApp

 vApp
 vApp

 192.168.100.2
 192.168.100.204 (Manual)
 192.168.100.103 (DHCP)
 Direct-Connect vApp

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.

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

VMware vCloud Dir	ector				4	administrator (System Admini	istrator) Preferer	nces Help -	Logout				
System 1-10 ×													
🚹 Home 🛆 My Cloud 🗐 Ca	talogs d	🍓 Administ	ration										
Catalogs	🚯 Р	ublic Cata	logs										
My Organization's Catalogs	Cata	Catalogs vApp Templates Media & Other											
Public Catalogs	0 -	All Catalogs V All V											
	Na 1 🔺	Version	Status	External	Organization	Created On	vApp Templates	Media & Other					
	🚯 d	18	Ready	-	1-05	02/11/2014 11:32 PM	2 4	🔥 1					
	🔀 р	80	Ready	-	vmware_service	02/13/2014 3:17 PM	🕮 14	6 🗟					
		Oper	n n n n n n n n n n n n n n n n n n n	y									
		Publ	ish/Subscribe Setting	s									
		Shar	e										
		Sync	nge Owner						_				
		Dele	te										
		Prop	erties						_				
	_												
							1-2 of	2					
🐐 0 Running 🔮 0 Failed					VMware vCloud Director			Powered by VII	ware [.]				

10. 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:

VMware vCloud Dir	ector								s Help -	
System 1-10 ×										
🕼 Home 🛆 My Cloud 🗐 Ca	talogs 🍇 Administration									
Catalogs	🔢 public catalog									
My Organization's Catalogs	vApp Templates Me	edia & Other								
Recent Items	🖄 💀 🌼-			All	Catalogs	▼ AI	•			C 😮
i public catalog	Name 1 🛦 Ve	ersion Status	Gold Mas	Owner	Created On	Last Successful Sync	VDC	Storage Us	Shadow VMs	
	E CentOS63-32bit 3	Ready	-	🖁 system	02/13/2014 3:4		🚇 vmw	20.00 GB	0 🛃	*
	E CentOS63-64bit 3	Ready	-	👗 system	02/13/2014 3:2		🚇 vmw	20.00 GB	0 🖾	
	CentOS64-32bit 3	Ready	-	💧 system	02/13/2014 3:2		🚇 vmw	20.00 GB	0 🖾	
	CentOS64-6 AC	tions: CentOS64-64	bit -	🔒 system	02/13/2014 3:2		🚇 vmw	20.00 GB	0 🖾	
	🖹 centosminir Oper	n		🖁 system	02/24/2014 10:		🚇 vmw	2.00 GB	0 🛃	
	😻 w2008r2-sti	to My Cloud mload	-	🔒 system	02/13/2014 3:4		🚇 vmw	40.00 GB	0 🖾	
	W2K12-STE Uplo	ad new version	-	🔒 system	02/14/2014 11:		🚇 vmw	40.00 GB	🛃 0	
	🖹 W2K12-STE Sync	-	-	🖁 system	02/13/2014 11:		🚇 vmw	40.00 GB	🛃 0	
	W2K12-STC Copy	y to Catalog		🔒 system	02/13/2014 4:1:		🚇 vmw	40.00 GB	0 🖾	
	Move to Catalog Delete			-				1-10 of 14		
🖓 0 Running 🔮 0 Failed	Delete Delete Open in vSphere Web Client Properties				d Director			Po	owered by VIII	iware [.]

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

Chapter 5

System 1-10 ×												
🕼 Home 🖾 My Cloud 📋 Ca	italogs 😽 Administrat	ion										
Catalogs	public catalog	l.										
My Organization's Catalogs	vApp Templates	Media & Oth	ier									
Public Catalogs Recent Items	🔊 🚮 Сору Са	talog Item						0	× .			CO
🗐 public catalog	Name Select	destination (catalog:							Storage Us	Shadow VMs	
	CentOS Destin	CentOS Destination catalog:										-
	CentOS		This ca	talog is loca	I to your organ	ization.			D vmw	20.00 GB	@ 0	
	CentOS									20.00 GB	0	
	CentOS								de vmw	20.00 GB	0	
	🗶 centosn								D vmw	2.00 GB	0	
	🐮 w2008r:						ок	Cancel	🗈 vmw	40.00 GB	0	
	3 W2K12-STD-64	5	Ready	-	👗 system	02/14/2014 11			Cat vmw	40.00 GB	0	
	💹 W2K12-STD-64	5	Ready	-	👗 system	02/13/2014 11			C vmw	40.00 GB	@ 0	
	1 W2K12-STD-64	4	Ready	-	👗 systen	02/13/2014 4:1			Cat vmw	40.00 GB	0	
	_							14		1-10 of 14		
0 Running O Failed				14	/Mware vClou	d Director				,	Powered by VII	ware

- 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:

VMware vCloud Dir	rector					administrator	(System Administrato	r) F	references	Help 👻	Logout
System 1-10 ×											
🚮 Home 🛆 My Cloud 🗐 Ca	talogs 🖏 Administration										
Catalogs	My Organization's Cat	alogs									
My Organization's Catalogs	Catalogs vApp Templates	Media & Other									
Recent Items	🛓 📴 🖄 💀 🔅	-		All Cat	alogs	-	u .	•			? 🕜
🔢 public catalog	Name 1 🛦 Versi	Status	Gold M	Catal	Ow	Created	Lest Successful Sy	V	Storage	Shadow VMs	
	E CentOS64-64 1	Copying	-	VCD-E	🔓 syste	03/16/2014 2	!	@ 1 -1	20.00 GB	0	
		13/1									
											_
											_
											-
									1-1 of 1		
🚯 1 Running 🔮 0 Failed			🛃 VMwa	re vCloud D	irector				Power	red by VIIIV	are

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

VMware vCloud Dir	ector							administrator		ator) F			
System 1-10 ×													
🛗 Home 🛆 My Cloud 📃 Cat	talogs 🍇 Adr	ministra	tion										
Catalogs	🚺 My Org	janizat	ion's Cat	alogs									
My Organization's Catalogs	Catalogs	vApp 1	emplates	Media & C	Other								
✓ Public Catalogs Recent Items	2 😨	2	💀 🌼			All Catalog	s	▼ A	I	•		G	3
🗊 public catalog	Name	1 🔺 \	/ersi	Status	Gold M	Catal Ow		Created	Last Successful Sy	V	Storage	Shadow VMs	
	E CentOS64	4-64	1	Ready	-	🗊 vCD-E 🖁	syste	03/16/2014 2		@ 1-1	11 20.00 GB	🕑 0	
					Actions: Cen	tOS64-64bit							
					Open								- 1
					🆄 Add to My Clou	d							
					Download								- 1
					Upload new ve	Upload new version							_
					Sync								- 1
					Copy to Catalo	g							- 1
					Move to Catalo	g							- 1
					Delete		-						-
					Open in vSphe	re Web Client	-						- 1
					Properties		-						_
							-				1-1 of 1		
0 Running 🔮 0 Failed					🛃 VMw	rare vCloud Direc	tor				Power	red by VMVa	are [.]

- 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:

System 1 Select Name and Location Configure Resources Configure Networking Customize Hardware Ready to Complete	🥥 🛛 🛞 👘 Logout
Leases This vApp will remain powered on indefinitely. It will not be deleted after power-off or suspend. You can edit these leases at any time by going to the vApps properties.	Cribe this vApp and select its Virtual Datacenter. Started. spend. You can edit these leases at any time by going to the

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

Chapter 5

	Add to My Cloud			2 8	- Logout
System 1	Select Name and Location Configure Resources Configure Networking	Configure Resources Select what Storage Policies this vApp's virt Virtual Machine	ual machines will use when deployed. Storage Policy	Template VM Default Storage Policy	
✓ Public (Recent I ■ public)	Customize Hardware Ready to Complete	CentOS64-64bit *	SSD-Accelerated v		C 3
🗿 0 Ru				Back Next Finish Cancel	mware [.]

- 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:

	Add to My Cloud				3 8	- Logout
System 1	Select Name and Location Configure Resources	Configure Networking Select the networks to which complete this wizard.	you want each virtual machin	e to connect. You can configure additional properties for virtual machi	nes after you	
🖪 My Orga	Configure Networking	Virtual Machine	Computer Name	Networks		
🛨 🔂 Public (Customize Hardware	🚰 CentOS64-64bit	cts64-64bit *	NIC 0 1-10-default-routed - Static - IP Pool		
Recent /	Ready to Complete					C ()
E pub						VMs III
		Switch to the advanced n	etworking workflow			
🗿 0 Ru				Back Next Finish	Cancel	m ware [.]

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

Managing Catalogs and vApps

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

	Add to My Cloud		3	۲	r Logout
VVM System 1 Home Catalogs My Orga Public (Recent public)	Add to My Cloud Select Name and Location Configure Resources Configure Networking Customize Hardware Ready to Complete	Customize Hardware Review the hardware of the virtual machine in this vApp. CPU Number of virtual CPUs: 1 Cores per socket: 1 Number of sockets: 1 Number of sockets: 1 Memory			C 0
9 Ru		 Increasing disk size might require configuration of the guest OS after powering on the vApp. Hard disks cannot be made smaller than their template size. Back Next Finish G 	Cancel	•	mware [.]

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

Add to My Cloud			3 😣	
VM Add to My Cloud System Add to My Cloud Select Name and Location Configure Resources Configure Networking Customize Hardware Ready to Complete	Ready to Complete You are about to create a v ^A Name: Description: Owner: Virtual datacenter: Runtime lease: Runtime lease expiration: Storage lease : Storage lease expiration: Networks - 1:	o with these specifications. Review the settings and click Finish. 2entOS 1-10 Vever Expires Vever Vever Expires Vever	• •	Logout Vite
	VMs - 1:	Virtual Machine Guest OS Storage Policy CPUs Memory	Storage	
		CentOS64-64bit CentOS 4/5/6 (6 SSD-Accelerate: 1 1 GB 2) GB	
SI 0.5m		□ Power on vApp after this	wizard is finished.) D

- 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 s shown in the following screenshot:

VMware vCloud Dir	rector				administrator	(System Administrator)	Preferences Help 🗸	Logout
System 1-10 ×								
🛗 Home 🛆 My Cloud 🗐 Ca	talogs 🛛 🍓 Administration							
My Cloud	🚼 vApps							
VApps	+ 🐌 🐄 🖻	000	*		All vApps	• All •		C 😮
Expired Items	Consoles	Name 1	Status	Shar	Owner	Created On	VDC	
Logs	Pending	H CentOS	Creating 11%	-	🔒 system	03/16/2014 2:42 PM	(1 -10	
	•							
							1-1 of 1	
🔹 1 Running 🔮 0 Failed			🛃 VMware vC	Cloud Direc	tor		Powered by VIII	ware [.]

- 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:

VMware vCloud Dir	rector administrator (System Administrator) Preferences Help +	Logout
System 1-10 ×		
🕼 Home 🛆 My Cloud 🗐 Ca	atalogs 🛛 🍓 Administration	
My Cloud	RentOS Stopped	
▼ 器 vApps	vApp Diagram Virtual Machines Networking	
Recent Items	1a 1a 0 0 0 5 🕸	C 🎯
🚰 VMs		
Z Expired Items	CentOS64-64bit	^
🔲 Logs		
	NIC 0: 192.168.109.2	
		×
🗿 0 Running 🔮 0 Failed	Villware vCloud Director Powered by VM	ware [.]

Managing Catalogs and vApps

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:

VMware vCloud Director administrator (System Administrator) Preferences Help + Logout									Logout		
System											
🕼 Home , Manage & Monitor	🖞 Home 🔯 Manage & Monitor 🖏 Administration										
Manage & Monitor Organizations											
Crganizations	+ 🔅	•					All	-			C 💿
Cloud Resources	Name	1 🔺	Enabled	VDCs	Can Publish	Can Publish Externally	Catalogs	vApps	Running VMs	Users	
Provider VDCs	l-05		×	@ 1	-	-	1	25	🗗 22	🔓 3	
Crganization VDCs	left 1-10		×	@ 1	-	-	1	器 1	🗗 0	8 2	_
🥺 Edge Gateways	l-15		×	@ 1	-	-	0	28 o	🗗 0	🔓 3	
		eam	×	@ 0	-	-	0	36 0	🗗 0	🔓 1	
Network Pools		eam	×	@ 0	-	-	⊡ 0	38 0	🗗 0	🔓 0	
VSphere Resources		am	×	@ 1	-	-	⊡ 0	38 o	🗗 0	👗 1	
Resource Pools	Cloud	E	v	(A) 1	-	-	0	器 0	🗗 0	🔓 1	
Hosts	🛆 vmwar			Essenual	×	×	1	36 0	🗗 0	🔓 1	
🗐 Datastores & Datastore (All	ocate Resourc	:es							
Storage Policies	Enable										
Switches & Port Groups	_	Di	sable								
Stranded Items	•	De	lete		1-8 of 8					M	
🐐 0 Running 🔮 0 Failed		No Pr	otty		VMware vCloud Director Powered by VMWare				ware [.]		
🖓 0 Running 🔮 0 Failed		No Pr	otity operties		VMware vCloud Director Powered by VMWAre:					ware [.]	

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



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

VMware vCloud Dir	ector				administr	ator (System Administra	ator) Prefere	nces Help - Logout			
System vCloud-Essent ×											
🚮 Home 🛆 My Cloud 🗄 Ca	talogs 🖓 Administrati	DN									
Catalogs	🔢 My Organizatio	on's Catalogs									
My Organization's Catalogs	Catalogs vApp Templates Media & Other										
Public Catalogs	+ ⊗ -				All Catalogs 🔍 🗸 All			C 0			
	NI Add Catalog	n Status	Shar	Exter	Owner	Created On	vApp Templat	Media & Other			
		-									
							0-0 01				
🐐 0 Running 🔮 0 Failed			Mw VMw	are vCloud	Director			Powered by VmWare			

- 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:

VMware vCl	New Catalog		۶ ۵	s Help + Logout
System vCloud-Essent	Name this Catalog	Name this Cat A catalog allow catalog for vAp	alog s you to share vApp templates and media with other users in your organization. You can also have a private templates and media that you frequently use.	
E My Organization's Ca	Share this Catalog	Name	vCloud-Essential-Catalog *	
Public Catalogs	Publish Settings	Description		
	Ready to Complete			C 😡
		Subscribed Ca	talog	Media & Other
		Subscribed ca	and use if a read-only copy of an external published catalog and cannot be modified.	
		Subscribe to	na external catalon	
		Subscription U	RL *	
		Password:		
		Automatical	by download the content from external catalog.	
🖏 0 Running 🔮 0			Back Next Finish Cancel	owered by vm ware

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

VMware vCl	New Catalog		2 😣	
System vCloud-Essent	Name this Catalog	Select Storage Type		
Catalogs	Add Storage Share this Catalog Publish Settings Ready to Complete	Use any storage available in the organization Choose this option if you do not need to store catalog items on a specific storage. Pre-provision on specific storage policy Choose this option if you want to store catalog items on a specific VDC storage policy. - vApp templates in this catalog will be fast provisioned on selected VDC storage policy. - instanting a vApp from fast provisioned vapa template stark - A VDC storage policy selected will cause the vApp template size to count against your catalog storage quota. Endstanting a vapa from the vapa template size to count against your catalog storage quota.		C @
📲 0 Running 🔮 0		Back Next Finish Ca	incel	owered by VmWare

- 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:

VMware vCl	New Catalog		Share With Organizations		s Help - Logout
System vCloud-Essent	Name this Catalog Add Storage Share this Catalog	Share this Cat With which me Add Memt	Share with: All organizations Specific organizations	e	
Public Catalogs	Publish Settings		Organization Name	1 🔺	
	Ready to Complete		1-05	<u> </u>	CO
			1-10 1-15 VCDTeam-001 Add Remove I A 1-5 of 7 Organization Name		Medis & Other
🖏 0 Running 🞱 0			• • • •	K Cancel cel	owered by VIIIWare

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

VMware vCl	New Catalog	Share With Organizations	🥥 🙁 🕽 🛞 s Help - Logout
System vCloud-Essent	Name this Catalog Add Storage	t All organizations • Specific organizations	C
I My Organization's Ca	Publish Settings Ready to Complete	Organization Name 1-10 1-05 VCDTeam-001 VCDTeam1-001	LA CONTRACTOR A Other
		Organization Name	
🗿 0 Running 오 (Access level: Read Only	OK Cancel overed by VITIWare

- 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:

VMware vCl	New Catalog	g 8	s Help v Logout
VMware vClu System vCloud-Essent Home My Cloud Catalogs My Organizations C: Public Catalogs	New Catalog Name this Catalog Add Storage Share this Catalog Publish Settings Ready to Complete	Publish Settings External publishing allows creation of catalog for consumption by external organizations Enable Publishing After creating this catalog, you can find the subscription URL on the catalog's Publish/Subscribe Settings page. Password: Supply an optional password to access the catalog. Only ASCII characters are allowed in a valid password. Confirm Password: Enable early catalog export to optimize synchronization. If this option is selected, extra storage is required to store the published catalogs at the transfer server storage location. If this option is selected, extra storage is required to store the published catalogs at the transfer server storage location. Horsenve identity information heture RBO URDs and MAC addresses in the downloaded OVF package. This limits portability of the package and should only be used when necessary.	s Heip ~ Logout
a Running 🔮 (Back Nett Finish Cancel	owered by VmWare

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

VMware vCl	New Catalog			3 0	<u>ه</u>	Help -	Logout
System vCloud-Essent	Name this Catalog	Ready to Complet	e				
Home My Cloud Catalogs My Organization's C: My Public Catalogs	Name this Catalog Add Storage Share this Catalog Publish Settings Ready to Complete	Name Description Shared: Publish Settings Organization: Storage Policy:	VCloud_Essential_catalog Yes Publish externally Do not allow early catalog export to optimize synchronization Identity information is not preserved. VCloud-Essential Use any storage available in the organization			Media & Oth] ℃ ◎
🗿 O Running 🔮 O			Back Next Finish Ca	incel	D	wered by VN	Nware [.]

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:

VMware vCloud Director administrator (System Administrator)	Preferences Help - Logout
System vCloud-Essent X	
🚹 Home 🖾 My Cloud 🗐 Catalogs 🖏 Administration	
here a set up this organization	Organizations
Quick Access	💣 Org Settings
To start a vApp, click Start. To use a powered on vApp, click on its thumbnail.	A Manage VDCs
💠 Add vApp from Catalog 🛯 🐐 Add vApp from OVF 🛛 🕌 Build New vApp 🛛 📴 Import from vSphere C 🔮 🎯	Content
	Hanage vApps Add vApp Add vApp Add vApp from OVF Build New vApp Image Catalogs New Catalog Users & Groups Administer Users Notify Users
Image: Second and Second an	Powered by VMWare

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

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

VMware vCloud Dir	rector			admir	nistrator (System Adminis	trator)	Preferences	Help 🗕 Logout
System vCloud-Essent ×								
付 Home 🛆 My Cloud 🗎 Ca	italogs 🖓 Administra	tion						
Catalogs	🔢 My Organizat	ion's Catalogs						
My Organization's Catalogs Rublic Octobers	Catalogs vApp	Templates Media & Othe	er					
E Public Catalogs	1 😰 🖄	₩ ₩		All Catalogs	▼ AI	•		C 3
	Name 1 A V Import	from vSphere	Catalog Owner	Created On	Last Successful Sync	VDC	Storage Us	Shadow VMs
								_
							0-0 of 0	
👬 0 Running 🔮 0 Failed			VMware vCl	oud Director			Powe	red by VMWare

- 9. 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**.
- 10. Click on **OK** as is shown in the following screenshot:

VMware vClou	Import VM as a vApp Te	mplate	2	×	ces Help 🗸 Logout
System VCloud Essent			All 👻 🤇	*	
Violate Social	VM 1 Memory	Storage CPUs	Path		
Home My Cloud	468548 4.00 GB	40.00 GB 1	[VPC1-LUN2] 468548f8-71ac-48cc-8ec1-1e68ca904346/468548f8-71ac-48cc-8ec1		
Catalogs	ESXi 16.00 GB	128.00 GB 4	[VPC1-LUN0] ESXI/ESXI.vmx		
I My Organization's Cata	vCVA55 8.00 GB	125.00 GB 2	[VPC1-LUN0] vCVA55/vCVA55.vmx		
Public Catalogs	VSAN N 4.00 GB	62.00 GB 2	[VPC1-LUN0] VSAN Nested ESXi VM/VSAN Nested ESXi VM.vmx		C @
			1-4 of 4		Shadow VMs
	Destination				
	vApp template name:	vCVA-Template	1	*	
	Description:			::	
	Catalog:	vCloud_Essential_catalo	pg v		
	Copy or move:	Copy VM O Move VM			
	Gold Master:	💿 No 🔘 Yes			
	After the import is co Guest customization You can review Cust	mplete, check the VMware Tools v requires at least version 7299. tomize VM Settings option on the v	version that is installed on the VM. App template properties page.	•	
🗿 0 Running 🔮 0 F			OK Cancel		Powered by VMWare

- 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:

VMware vCloud Dir	rector				
System vCloud-Essent ×					
🚮 Home 🖾 My Cloud 🗎 Ca	talogs 🖓 Administration				
Catalogs	🔝 My Organization's Cata	logs			
My Organization's Catalogs Dublic Octobers	Catalogs vApp Templates	Media & Other			
Public Catalogs	🏡 🖻 🖄 💀 🐲		All Catalogs	• Al •	C' 😮
	Name Upload) Status	Gold Mas Catalog	Owner Created On	Last Successful Sync VDC	Storage Us Shadow VMs
					0-0 of 0
0 Running 🔮 0 Failed		🛃 VMv	vare vCloud Director		Powered by VMWare

- 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**.

Managing Catalogs and vApps

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: vcloud.vcloud. 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.

Managing Security

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
```

7. 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.



8. 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.

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.

Managing Security

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

Managing Security

This is shown in the following screenshot:

VMware vCloud Dire	ector	ad	Iministrator	(System Administrator)	Preferences	Help +	Logout
System VDC-11442-12 ×							
🚮 Home 🛆 My Cloud 📋 Cat	talogs 🍇 Administration						
Administration	@ LDAP						
	LDAP Options Custom LDA	q					
Wirtual Datacenters							-
Users							(2)
👸 Groups	Synchronize LDAP Test LI	DAP Settings					::
🛔 Lost & Found							
✓ Settings	Connection						
@ Email	Server:	10.	*				
de LDA₽	Port:	389					
Policies		Default port number 389 for LDA	P / 636 for LD	APS.			
Guest Personalization Federation	Base distinguished name:	dc=vcap,dc=local	*				
@ Metadata		Example: dc=example,dc=com					
	SSL:	Use SSL					
		Accept all certificates					
	SSI Certificate:				A	pply Re	vert
🗿 0 Running 🥝 0 Failed		VMware vCloud E	irector		Po	wered by VIII	ware [.]

- 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.

VMware vCloud D						
System VDC-11442-12 ×	LDAP Settings	Test Results	_	_	3	0
🕼 Home 🛆 My Cloud 🗐	Connecte	d				
Administration	User name to	search for:	:t			
Wernhore	LDAP user se	arch test results:				-
& Users		Attribute		Attribute V	Result	©
a Groups		Unique identifier		objectGuid	\1B\AA\C2\42\3	
a Lost & Found	~	User name		sAMAccountNa	Administrator	
✓ Settings	0	Email		mail		
i General	0	Display name		displayName		
i Email	0	Given name		givenName		
de LDAP	0	Surname		sn		
Policies	0	Telephone		telephoneNum		
Guest Personalization	×	Group name		cn	Administrators	
@ Metadata	×	Group unique identifier		objectGuid	IDCICCIEF115	
					ОК	Apply Revert
0 Running 🔮 0 Failed		🛂 VMware vCloud Di	irector			Powered by VMWare

-[166]-

- 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:

VMware vCloud E			administrato			
System VDC-11442-12 ×	LDAP Settings	Test Results	_	_	3	0
🚮 Home la My Cloud 🗐	Connecte	d				
Administration	User name to	search for: vcap				
- Cloud Resources		arch toot requite:				
Members	LDAF user se	architest results.				
Lusers	~	Attribute		Attribute V	Hesult	S
📇 Groups	~	User name		sAMAccountNa	vcap	
🔒 Lost & Found	0	Email		mail		
✓ Settings Ø General	4	Display name		displayName	vcap	
a Email	×	Given name		givenName	vcap	
de LDAP	0	Surname		sn		
Policies	0	Telephone		telephoneNum		
Pederation	×	Group name		cn	Administrators	
a Metadata	×	Group unique identifier		objectGuid	IDCICCIEF115	
						-
					ОК	Apply Revert
0 Running 🔮 0 Failed		🛃 VMware	vCloud Director			Powered by VMWare

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

VMware vCloud Dir	ector	а	dministrator	(System Administrator)	Preferences	Help + L	.ogout
System VDC-11442-12 ×							
付 Home 🛆 My Cloud 🗐 Cat	talogs 🖓 Administration						
Administration	💣 LDAP						
 Cloud Resources Virtual Datacenters 	LDAP Options Custom LDA	(P					
✓ Members							3
📇 Users 🎇 Groups	Synchronize LDAP Test LI	DAP Settings					
🔓 Lost & Found	Synchronization with LDAP has	started.					- 14
✓ Settings	Connection						-11
🖉 Email	Server:	10.	*				- 11
d LDAP	Port	389	*				- 11
Policies	Base distinguished name:	Default port number 389 for LD	AP / 636 for LD	APS.			
Federation Metadata	base distinguished name.	Example: dc=example,dc=com					
-	SSL:	Use SSL					- 11
		Accept all certificates					
	SSI Cenneare.				Ар	ply Revert	
0 Running 🔮 0 Failed		VMware vCloud I	Director		Pow	vered by VM	are [.]

-[167]-
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:

VMware vCloud D	Import Users	0	*		
System VDC-11442-12 ×	Source: LDAP -	vcap Sear	ch		
🚮 Home 🛆 My Cloud 🗐 C	User Name	Full Name			
Administration	vcap	vcap			
				-	୯ ଉ
Mirtual Datacenters				All VMs/Quota	Running VMs/Quote
✓ Members				0 / unlimited	
Lusers				0 / unlimited	0 / unlimited
l ost & Found				0 / unlimited	0 / unlimited
➡ Settings				0 / unlimited	0 / unlimited
General				0 / unlimited	0 / unlimited
i Email		Add		0 / unlimited	0 / unlimited
PLDAP	Selected:			0 / unimited	o / unlimited ::
Policies	vcap			07 uniimited	07 uniimitea
Guest Personalization				0 / unlimited	0 / unlimited
Federation				0 / unlimited	0 / unlimited
🖓 Metadata			_	0 / unlimited	0 / unlimited
	You can type the user names of the users yo user names (for example: user1;user2;user3	ou want to import. Use a semicolon to sepa b).	rate	0 / unlimited	0 / unlimited
	Assign role: Organization Administrator	-		0 / unlimited	0 / unlimited
				1-13 0	f 395
🗿 0 Running 🔮 0 Failed		OK Canc	el		Powered by VmWare

-[168]-

- 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:

VMware vCloud Director	Import Groups
System VDC-11442-12 ×	Source: LDAP domain users Search Results
Administration Image: Cloud Resources Image: Wintual Datacenters Image: Cloud Resources Members Image: Cloud Resources Image: Cloud Resources I	Domain Users
🖏 0 Running 🔮 0 Failed	OK Cancel Powered by VIIIWARE

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:

♦ VMware vCloud Dire	New Role		3	×	System Administrator) Preferences Help 🗕 Logout
System	Name:	Custom Role	*	^	
🕼 Home 😡 Manage & Monitor	Description:				
Administration					
	Rights for this	Role			
🆧 Users					Description
🕌 Groups	→ 🔳 🖨 All R	ights			
🚾 Roles	▶ <u> </u>	atalog			er who creates and publishes new catalogs
🎉 Lost & Found	▶ 🗌 🧰 C	atalog Item			er who can only view virtual machine state and properties and use
		isk			inistrator
🇬 General	▶ 🗹 🛄 G	ateway			
🇬 Email	▶ 🗌 🛄 G	eneral			ninistering an organization
LDAP	▶ 🗹 🛄 0	rganization VDC Network			
Password Policy	▶ 🗹 🛄 0	rganization			Inistrator
License	D 🔤 🔽 (rganization VDC			ninistering this installation
💣 Branding) 🕞 🖂 U	ser			er who uses catalogs and creates vApps
Public Addresses	► 🗌 🛄 W	\pp			er who uses vApps created by others
Extensibility					
Federation					
-					
				•	1-11 of 11
0 Running 🔮 0 Failed			OK Canc	el	Powered by VMWare

- 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:

VMware vCloud Direct	User Properties: vcap	•	ator) Prefer	rences Help -	Logout
System VDC-11442-12 ×	Credentials				
Administration	Type: LDAP				
	In sync with LDAP: Yes				C O
Virtual Datacenters	Password: *		VMs/Quota	Running VMs/Quota	
Users	Confirm password: *		limited	0 / unlimited	-
🖧 Groups 🔓	Polo		limited	0 / unlimited	
🔓 Lost & Found 🖁 🖁	Nie		limited	0 / unlimited	
▼ Settings	Use group roles instead of user role		limited	0 / unlimited	
General	User role in organization: VDC-11442-12494-684		limited	0 / unlimited	
AP Email	Custom Role 💌		limited	0 / unlimited	
Policies	Group roles in organization: VDC-11442-12494-684		limited	0 / unlimited	
Guest Personalization	Member Of Role		limited	0 / unlimited	
Federation			limited	0 / unlimited	
Metadata 🖁	Contact Info		limited	0 / unlimited	
8	Full name: vcap		limited	0 / unlimited	
8	Email address:		limited	0 / unlimited	
	Phone:		1-14 0	of 396	
🕅 0 Running 🔮 0 Failed	OK Can	cel		Powered by VII	ware [.]

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.

Managing Security

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:

VMware vCloud Dire	ector	administrator	(System Administrator)	Preferences Help 🕶 Logout
System				
付 Home 😡 Manage & Monitor	🍇 Administration			
Administration	Federation			
 ✓ System Administrators & Roles 	vSphere Services vSphere Lookup Service Regis Regis	gister tering with vSphere Lookup Service enables vi	Cloud Director to discover othe	•
같[LAP @ Password Policy @ License @ Branding @ Public Addresses @ Extensibility c? Federation	Use vSphere Single Sign-On Your vSphere identity provider is u	used to authenticate System users.		
🗿 0 Running 🕥 0 Failed		VMware vCloud Director		Apply Revert Powered by VmWare

- 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:

VMware vCloud Dire	administrator (System Administrator) Preferences	Help 🗸 Logout
System		
Home Manage & Monitor	R Administration	
Administration	Pederation	
	Register With Lookup Service	
🏖 Users	Lookup Septica LIPI	
📇 Groups		
Roles	Example: https://hostname:/444//ookupservice/sdk	
🎎 Lost & Found	SSO Admin User Name root *	
	The vSphere Single Sign-On user with Administrative privileges.	other services
i General	SSO Admin User Password ****** *	
i Email	vCloud Director URL https://10. /cloud *	
i LDAP	The base URL identifying this vCloud Director instance (e.g.	
Password Policy	https://example.com/cloud).	
💣 License		
Pranding 🌮		
Public Addresses		
Extensibility		
Federation		
	Apply	Revert
🗿 0 Running 🔮 0 Failed	🕌 VMware vCloud Director Powered	by vm ware

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:

VMware vCloud Dire	ector administrator (System Administrator) Preferences Help + Log	out
System		
Home 😡 Manage & Monitor	Contraction Administration	
Administration	I Federation	
 ✓ System Administrators & Roles 2 Users 2 Groups 2 Roles 2 Lost & Found ✓ System Settings 2 General 2 Email 	vSphere Services vSphere Lookup Service Register Registering with vSphere Lookup Service enables vCloud Director to discover other services, and allows other services	-
الله LDAP الله Password Policy الله Picense الله Branding الله Public Addresses الله Extensibility P Federation	Identity Provider Use vSphere Single Sign-On Your vSphere identity provider is used to authenticate System users.	-
資 0 Running 🔮 0 Failed	Apply Revert VMware vCloud Director Powered by VMWare	9 .

- 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:

Chapter 6

VMware vCloud Director	Import Users 🕑 🛞) Preferences Help √ Logout
VMware vCloud Director System VDC-11442-1 × Manage & Monitor & A Administration System Administrators & Roles Course Groups Roles Lost & Found System Settings General Email Cuerse Password Policy Etcanse Branding Public Addresses Etcansibility Federation	Import Users Import Source: Source: Sphere SSO Enter user names to import: admin_test_user1@marvet.net	P Preferences Help + Logout Image: Type Type Cal
	Role: System Administrator	1-1 of 1
0 Running 🔮 0 Failed	OK Cancel	Powered by VMWare

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

Α

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 89 allocation pool model 88 archived basic reports managing 28, 29

С

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

Ε

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

Μ

managed by property 32 maximum transmission unit (MTU) 73

Ν

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

0

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

Ρ

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

Т

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 (vmnic) 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

Υ

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.

[PACKT] Open source



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.

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