VMware vCloud® Director™ 1.5 Evaluation Guide

TECHNICAL WHITE PAPER
V 1.0 / UPDATED NOVEMBER 2011
Table of Contents

Getting Started ............................................................................................................ 4
  About This Guide ...................................................................................................... 4
  Intended Audience ................................................................................................. 4
  Evaluation Help and Support ................................................................................... 4

The Journey to Private Cloud ......................................................................................... 5

Understanding the VMware vCloud Solution ................................................................ 7
  vCloud Director Physical Components .................................................................. 7
  vCloud Director ....................................................................................................... 7
  vCloud Director database ....................................................................................... 7
  vCenter Server ........................................................................................................ 8
  VMware ESXi™ hosts ............................................................................................. 8
  VMware® vShield Manager™ .................................................................................. 8
  vCloud Director Logical Components ..................................................................... 8
  Provider Virtual Datacenter ..................................................................................... 8
  Organizations ........................................................................................................... 9
  Organization Virtual Datacenter ............................................................................. 9
  vApps ....................................................................................................................... 9
  vApp Catalog .......................................................................................................... 9
  Typical vCloud Director Deployment ....................................................................... 10
    Management Cluster ............................................................................................. 10
    Resource Cluster .................................................................................................. 11

Evaluation Lab Configuration Details ............................................................................ 12
  Architecture Overview ............................................................................................ 12
  Compute Hardware Requirements ............................................................................. 13
  Network Requirements ............................................................................................ 14
  Storage Requirements ............................................................................................. 15
  Software and Licensing Requirements ................................................................... 15
  Software Configuration ........................................................................................... 16

Evaluation Procedures ................................................................................................... 17
  Evaluation Scenario ................................................................................................ 17
  Infrastructure Installation ......................................................................................... 17
    Installing vCenter Server ..................................................................................... 18
    Configuring vCenter Server ................................................................................. 26
    Deploying VMware vShield Manager .................................................................... 30
    Installing and Configuring Microsoft SQL Server 2008 R2 Express .................. 37
Deploying the vCloud Director Appliance ........................................ 46
Installing the vCloud Director Binaries ........................................ 50
Generating SSL Certificates ..................................................... 51
vCloud Director Configuration .................................................. 53
vCloud Director Initial Setup .................................................... 56
Attaching to Virtual Center ..................................................... 59
Defining the Provider Virtual Datacenter .................................... 61
  Creating a Provider vDC ......................................................... 61
  Defining an External Network ............................................... 64
Network Pools ........................................................................ 66
Organization Creation .............................................................. 69
  Creating an Organization ....................................................... 69
Allocating Resources to an Organization .................................... 74
Creating an Organization Network ............................................. 79
Creating Another Organization ................................................ 83
Creating a New Organization ................................................... 83
Allocating Resources to an Organization .................................... 84
Creating an Organization Network ............................................. 84
Enabling DHCP for an Organization Network ............................ 85
Accessing an Organization ....................................................... 86
Developing Service Offerings .................................................... 87
  Creating a Catalog ............................................................... 87
Importing Media ..................................................................... 89
Building a vApp ...................................................................... 91
Creating a vApp Template ....................................................... 97
Deploying a vApp from a Template ............................................ 99
Customizing a Virtual Machine ................................................ 102
Cloud Security and Management .............................................. 105
  Site-to-Site VPN ................................................................. 105
Firewall Configuration ............................................................ 110
Blocking Tasks ...................................................................... 113
Conclusion ................................................................. 118
VMware Contact Information ................................................... 118
Feedback .............................................................................. 118
Getting Started

About This Guide
VMware vCloud® Director™ (VCD) enables customers to build a private cloud-based Infrastructure as a Service (IaaS) offering within their organization. By providing a secure, on-demand ability for end users to deploy workloads, companies can realize a level of agility previously thought impossible.

This VMware vCloud Director 1.5 Evaluation Guide is designed to provide a guided, hands-on evaluation of the most compelling and relevant features of vCloud Director. It walks users through a series of procedures, each building upon the previous. When completed, the evaluator will have a working configuration that illustrates the key concepts that should be understood before deploying a production private cloud solution with vCloud Director.

Because this guide is to be leveraged for evaluation purposes, it has been written to require the least amount of hardware resources possible. This enables users who do not have a dedicated test lab to still fully evaluate the capabilities and concepts of vCloud Director. This purpose-built evaluation environment should not be considered as a template for deploying a production environment.

Intended Audience
This guide is intended for IT professionals familiar with VMware vSphere® who are new to vCloud Director. It is expected that the reader is comfortable with common computing and networking topics.

Evaluation Help and Support
This guide is not meant to substitute for product documentation. For detailed information regarding installation, configuration, administration and usage of VMware® products, refer to the online documentation. You can also consult the online VMware knowledge base if you have any additional questions. If you require further assistance, contact a VMware sales representative or channel partner.

The following are some links to online resource, documentation and self-help tools:

**VMware vSphere® and VMware vCenter Server™ resources:**
Product overview:
http://www.vmware.com/products/vsphere/overview.html

Product documentation:

White papers and other resources:

**VMware vCloud Director resources:**
Product overview:
http://www.vmware.com/products/vcloud-director/overview.html

Product documentation:
http://www.vmware.com/support/pubs/vcd_pubs.html

White papers and other resources:
http://www.vmware.com/products/vcloud-director/resources.html
The Journey to Private Cloud

Cloud-based infrastructure environments are a frequent topic of discussion within IT organizations today. This interest stems from several sources. Customers who have broadly adopted virtualization are looking for ways to further increase their agility. Others are interested in achieving a significant reduction in operating costs by deploying a cloud solution. Still others have heard about cloud infrastructure technologies and are trying to understand what benefits it can bring to their organization.

The journey that companies have taken with virtualization started with the need to virtualize applications to reduce server sprawl. Initially, companies looked at applications of low importance to virtualize, such as those in a preproduction environment. As time passed, companies took the next step in the virtualization journey by virtualizing more critical applications in their production environments. Significant reductions in personnel and hardware costs along with increased utilization of the computing resources were soon realized. This led many companies to adopt a “virtualization first” policy, where new applications are considered for deployment in a virtualized environment before a physical one.

With the adoption of virtualization well underway, companies are now looking forward to the next step in their virtualization journey. This step is the deployment of a private cloud.

According to a survey of more than 2,000 CIOs taken by Gartner Executive Programs in January 2011, cloud computing ranked #1 in their technology priorities. It can be inferred that the reason for this is that CIOs are now trying to evolve their current environments into a highly agile infrastructure to improve enterprise efficiency, cost expenditures and the process of implementing or updating business applications.

What does it mean to be agile? Agility simply means being able to respond to the needs of the business faster. This entails the ability to quickly respond to requirements for environments that routinely change. It also means enabling environments commonly viewed as static to rapidly adapt to business needs. This is the main purpose of a private cloud–based infrastructure: to enable agility in the delivery of IT services.

Does being virtualized equate to the benefits provided by a private cloud? Unfortunately, it does not. Examining a large number of virtualized datacenters enables one to observe the following two distinct characteristics:

- A high degree of shared infrastructure. Companies have architected their virtualized environments with storage and network connectivity across large numbers of servers. This enables them to take maximum advantage of the features in vSphere, such as VMware vSphere® vMotion®, vSphere High Availability (vSphere HA), and vSphere Distributed Resource Scheduler (DRS).
- The processes to bring new applications and workloads online in a virtualized environment mimic the same processes used in physical environments.

IT agility is about aligning demand (what users need in order to do the best possible job) with supply (what resources IT can offer). Ideally, a company evolves to provide services as a supply that will meet the demands of users at any given point in time. The risk of not making this evolution is that the demand will find another source of supply.

IT organizations that see short-duration, high-demand workloads leak to external providers are experiencing the issues faced when their supply of resources is unable to meet the demand of users. Users who go “outside IT” do not do so maliciously. Rather, they are just trying to meet their deadlines and are unwilling or unable to wait for the IT provisioning process to occur. In doing so, however, they are exposing the company to unintentional risks.

The easiest way to prevent this is to provide a sufficient supply of IT resources to meet the demands of the users who want to consume them. This supply can be delivered within a secure environment, shielded from risk. This is the premise of a private cloud. A private cloud creates a way for companies to automate the matching of user demand with the available supply in a secure manner. In doing so, companies can realize the benefits of IaaS, where end users are able to have resources allocated on demand in a self-service model.

An interesting by-product of allowing self-service is the change in behavior regarding the quantity of resources requested by end users. When end users must go through a lengthy or difficult process to request servers and applications, they tend to overrequest and are not willing to relinquish what they have obtained.

When allowed to quickly and with minimum effort get what they need, end users are more likely to make more realistic resource requests and return the resources when finished.

How does one get to this point? As the start of the journey into virtualization began with specific workloads, so too does the journey into the cloud. First, identify workloads that have a low management or governance need and that are required frequently. A good source for these types of workloads can be found in testing and development or preproduction environments.

For example, in a typical development organization, multiple developers often require similar environments for short periods of time. Although these development environments are typically hosted on a virtualized infrastructure, they still are high effort because they tend to require refreshes as new product releases are made. This continual need to create environments for the developers and to manage them once created can place a large burden on the IT staff of an organization. By shifting to a self-service model for these workloads, an IT organization can save significant amounts of time while using this experience to hone their capabilities around delivering IT as a service.

Although the first step in the journey to the cloud might start with low-governance workloads, such workloads are not the end of the journey. As you continue down the path, you will quickly realize that the use of a private cloud solution can meet the needs of many applications and will give you new ways of looking at how applications and services are used and provided.

As an example, consider a typical ERP system. These systems tend to have long development cycles with fairly minimal changes. A private cloud will certainly help in the development effort by provisioning resources on demand. Because this can be done so quickly, it enables end users to also perform actions that were considered difficult before. They can quickly test new applications or deploy new analytic packages. If successful, they can examine the feasibility of incorporating them into the ERP solution. If not, it’s a simple matter to destroy the environment and provision a new one, clean of any trace of the new software.

The agility provided by a private cloud is not just about how quickly one can deploy something. It is also about how quickly one can test something and tear it down if it fails. Not trying something simply because it would cost too much in time and personnel resources is not a viable excuse anymore.

The journey into private cloud mimics the journey into virtualization in another critical way. As companies moved from virtualizing low-impact applications to more business-critical applications, the capabilities that virtualization provided changed the way they deployed and managed applications. The zero-downtime migration capabilities of vMotion and failure handling of vSphere HA meant clustering between multiple running systems no longer made sense. The shift to a more agile infrastructure will drive similar changes. Business applications that might be considered as having a low frequency of change might very well be reexamined in the light of the capabilities of a private cloud. Applications will remain mission critical, but the concept of making routine changes to better support the business will become far less daunting.
Understanding the VMware vCloud Solution

The VMware vCloud® solution is a suite of products designed to enable an IT organization to build a private cloud on top of a vSphere environment. The product suite consists of vCloud Director 1.5, VMware vShield Edge™ 5.0, and VMware vCenter Chargeback™ 1.6.2. A VMware vCloud API is also provided as a programmatic interface to this solution suite.

**VMware vCloud Director 1.5** provides the automation and user portal capabilities needed to enable self-provisioning and management of workloads across one or more vSphere environments. This enables businesses to migrate gradually to cloud computing while continuing to leverage existing vSphere investments.

**VMware vShield Edge 5.0** (included with vCloud Director) provides firewall, VPN, routing, and NAT services for the private cloud. vShield Edge facilitates secure isolation of workloads running in the private cloud from each other as well as from external networks.

**VMware vCenter Chargeback 1.6.2** is an optional add-on for a vCloud environment that provides accurate cost measurement and reporting on virtual machine usage. When it is used as a part of a self-service private cloud environment, business owners can now have complete transparency into, and accountability for, the services they are consuming.

The **VMware vCloud API** ensures compatibility between public and private clouds—it’s the same API published by both private and public clouds. By using the vCloud API, moving from a purely public or purely private cloud to a hybrid cloud is significantly simplified.

With this portfolio of cloud-aware products, VMware amplifies value with cloud computing by reducing IT costs, increasing business agility and preserving IT governance.

This VMware solution ensures flexibility and interoperability for your cloud. As your enterprise moves through the journey to a cloud-based infrastructure, you can amplify the benefits of virtualization and move selected workloads within your datacenter cloud or to one of the many vCloud-enabled public clouds in the VMware partner ecosystem.

This solution also helps your organization achieve a cloud model that is uniquely yours—a private, public or hybrid environment precisely aligned with your individual business goals. When enterprises are able to deploy workloads in the best environment for their business needs, they increase agility without compromising security, reliability or governance.

**vCloud Director Physical Components**

A vCloud Director deployment consists of a number of physical components. These include the following:

**vCloud Director**

A single instance of vCloud Director is known as a “cell.” A cell consists of the vCloud Director components installed on a supported system. In larger implementations, multiple cells can be deployed with a front-end IP load balancer to direct end-user traffic to the correct cell.

**vCloud Director database**

vCloud Director stores information about managed objects, users and other metadata in a database. The current release of vCloud Director supports Oracle and Microsoft SQL Server for database platforms. In most environments, the vCloud Director and database components are installed on separate virtual machines for proper load handling. In cases where multiple vCloud Director cells are deployed, all cells communicate with the same database. Because the database is a critical component of vCloud Director, it is very important that the database be highly available.
vCenter Server
Each vCloud Director cell can connect to one or more vCenter Server instances to access resources for running workloads. Each attached vCenter Server instance provides resources, such as CPU and memory, which can be leveraged by vCloud Director.

VMware ESXi™ hosts
VMware ESXi hosts provide the compute power for vCloud Director. ESXi hosts are placed in groups of resources, such as clusters or resource pools. These groups and their associated storage are then made available to vCloud Director.

VMware® vShield Manager™
VMware vShield Manager provides a central point of control for managing, deploying, reporting, logging and integrating vShield as well as third-party security services. Working in conjunction with vCenter Server, VMware vShield Manager enables role-based access control and separation of duties as part of a unified framework for managing virtualization security. To support the automated management of VMware vShield Edge in a vCloud Director environment, an instance of VMware vShield Manager is required for each vCenter Server attached to vCloud Director.

vCloud Director Logical Components
Server virtualization abstracted away the concept of the physical server. This removed the complexity of specific storage or network interfaces and replaced them with a generalized, abstracted hardware layer that was presented to one or more virtual machines.

VMware vCloud solutions take this abstraction to a new level and create a virtual datacenter. Rather than individually selecting a target vSphere host or cluster, datastore and network port group, users deploy workloads into preallocated containers of compute, storage and networking resources known as virtual datacenters (vDCs). This dramatically simplifies the provisioning process and removes many of the manual configuration steps. To the consumer, these are seemingly infinite and elastic pools of resource that can be expanded quickly and easily.

In creating these virtual datacenters, corporate IT has the option to produce multiple service-level offerings to optimize the use of compute and storage resources. For example, all development users can be placed into a vDC containing resources with performance characteristics lower than those used in a production environment. Meanwhile, UAT/QA users can operate in a vDC with resource performance characteristics much closer to production specifications.

vCloud Director introduces a number of logical components to support the notion of a vDC that is presented to end users. The main logical components consist of the following elements:

Provider Virtual Datacenter
A provider virtual datacenter is a logical grouping of vSphere compute and storage resources. The provider virtual datacenter (provider vDC) groups together a set of ESXi hosts and a set of one or more associated datastores. This logical grouping is then made available for consumption by organizations. Within a provider vDC, compute and storage resources are all considered equal. By this we mean that these resources are considered of equal performance and cost. If an administration team wants to offer groupings of compute and storage resources of different costs or performance, multiple provider vDCs can be created. For example, a group of the most capable ESXi hosts combined with high-performance Fibre Channel (FC) storage might be combined to create a gold-level provider vDC. Another group of less capable ESXi hosts and slower storage might be grouped together as a silver-level provider vDC. In this way, different classes of resources can be offered to different consumer organizations.
Organizations

One of the key capabilities of a vCloud Director private cloud is secure multitenancy. The organization concept is one of the key building blocks of this. A VCD organization is a unit of administration that represents a collection of users and user groups. An organization also serves as a security boundary, because users from a particular organization have visibility only to other users and resources allocated to that organization. Organizations can be as simple as different functional areas inside a business or as complex as unique companies being hosted by a provider.

Organization Virtual Datacenter

An organization virtual datacenter (organization vDC) is a logical grouping of resources from one or more provider vDCs that an organization is allowed to access. Depending on back-end (provider vDC) configuration and needs of the organization, one or more sets of resources backed by different provider vDCs might be present. This enables different performance, SLA or cost options to be available to organization users when deploying a workload.

vApps

A vApp is an abstraction that encapsulates all of the virtual machine and internetworking needs of an application. vApps can be as simple as a single virtual machine or as complex as a multitier business application. Templates can be created from a vApp to enable a vApp to be easily redeployed multiple times by an organization's users. These vApp templates can be shared between other users in the organization or between organizations.

For example, a typical enterprise application might consist of virtual machines hosting a database server, various application servers and several Web servers. These virtual machines will be networked together to facilitate communication between the application components. A vApp encapsulates all of this into a single object. After it is produced, a template can be created of this vApp to facilitate the deployment of other application instances in a standardized manner. An end user who wants to deploy another instance of this application simply deploys another vApp from this template.

vApp Catalog

Organizations use catalogs to store vApp templates and media files. The members of an organization who have access to a catalog can use the catalog's vApp templates and media files to create their own vApps. A system administrator can allow an organization to publish a catalog to make it available to other organizations. Organization administrators can then choose which catalog items to provide to their users.
Typical vCloud Director Deployment

The size and scale of vCloud Director deployments vary greatly. There are, however, several architectural features that are common across most deployments.

Management Cluster

In most implementations, all of the infrastructure components needed for vCloud Director are deployed in a management cluster. The management cluster consists of two or more ESXi hosts, enabling high availability and downtime avoidance. Running within the management cluster will be virtual machines hosting vCloud Director, the vCloud Director database and one or more vCenter Server instances that are attached to vCloud Director and manage a number of ESXi hosts. There often will also be a single vCenter Server instance inside the management cluster, configured to manage the management cluster.

In the following diagram, a simple management cluster with two ESXi hosts is shown. Within this management cluster, virtual machines are configured for vCloud Director, vCloud Director database and two vCenter Server instances. One of the vCenter Server instances provides services for the management cluster by managing the two ESXi hosts and the virtual machines running on them. The other vCenter Server instance is attached to VCD and manages a set of hosts that provide the resources to be consumed by VCD.
**Resource Cluster**

A vCenter Server instance that is attached to a VCD instance manages one or more ESXi hosts. These ESXi hosts provide compute and storage resources, which are configured in one or more clusters. These clusters must be configured to use automated DRS and typically also have HA enabled.

Each vCenter Server instance attached to a vCloud Director instance requires a corresponding VMware vShield Manager. Only one VMware vShield Manager instance is required per vCenter Server, regardless of the number of clusters managed by that vCenter Server instance.

The collection of the vSphere Server instance that is attached to VCD, the associated VMware vShield Manager, and the resources (compute and storage) is referred to as a resource cluster. It is here where the workloads provisioned from VCD are run. This is shown in the following diagram.
Evaluation Lab Configuration Details

In the creation of this guide, an attempt was made to simplify the environment as much as possible. Although the evaluation environment available to you might differ from the one used in the creation of this guide, it is important that you understand how the lab used here was constructed. Doing so will help you understand why some procedures were done the way they were.

Architecture Overview

Logically, the evaluation environment used for this guide is split into two parts.

The first part is the management cluster. This provides hosting for the vCloud Director infrastructure components. These include the vCloud Director instance, vCloud Director database and the vCenter Server instance under the control of the vCloud Director that manages hosts in the resource cluster. An additional vCenter Server instance is used to provide management for the management cluster, as all of the components have been virtualized.

In this evaluation guide, the management cluster comprises two ESXi hosts, which enables the use of vSphere HA, providing availability services for the virtual machines within the management cluster. If two ESXi hosts are not available for the management cluster, the management components detailed in this evaluation guide can be run on a single host. This will, of course, limit the ability to enable HA.

Two methods of deploying the management cluster are presented in this guide. One method will utilize the VMware vCloud Director Appliance 1.5.

The vCloud Director Appliance provides the required components of a vCloud Director in a prepackaged and preconfigured manner. It comprises a virtual machine based on CentOS 5.6. This virtual machine hosts the vCloud Director binaries in addition to an embedded Oracle Database 11g R2 Express Edition (XE). Use of the vCloud Director Appliance is limited to evaluation environments that conform to the following:

- One vCloud Director cell
- Two vCenter Servers
- 10 organization vDCs
- 100 virtual machines
- Up to 11GB of information stored in the embedded database

The other method involves deploying vCloud Director and a Microsoft SQL Server database, to mimic the process to be performed if you were to deploy a production environment. With this method, the vCloud Director database is configured on the same virtual machine that hosts the vCenter Server instance, to minimize resource requirements. This method is depicted in the diagram on the following page.

The second logical part of this evaluation environment is the resource cluster. This comprises a set of ESXi hosts that will actually host the workloads for VCD. In this evaluation environment, two additional ESXi hosts are used for this purpose. These ESXi hosts are managed by the vCenter Server instance located in the management cluster that is to be attached to the VCD instance. A virtual machine for the VMware vShield Manager instance is also running on these ESXi hosts.
Compute Hardware Requirements

The management cluster requires at least one physical host powerful enough to host the two virtual machines that will be built. Two ESXi hosts were used for redundancy in the creation of this guide.

The resource cluster requires two physical hosts of sufficient power to host at least two standard Linux virtual machines.
In the environment used for this guide, all of the physical ESXi hosts are configured identically. Each host has two Intel Xeon Processor (“Nehalem” quad-core) CPUs running at 2.40GHz with 48GB of memory available. All of the physical hosts are running ESXi 5.0.

**Network Requirements**

One physical network is utilized within this guide. This network needs connectivity to external systems used for testing as well as software download. In our test lab environment, each ESXi host has two 10GB network adaptors attached to the physical network to provide redundant networking. As a minimum, you will require each host to have at least one 1GB network adaptor connected to the physical network.

The environment that was used in the creation of this evaluation guide has a network that was segmented through the use of several VLANs. The initial configuration of each host is shown in the following diagram. We use a total of three VLANs to separate “production” (externally routed) traffic, ESXi management network traffic, and vMotion traffic. We also have an additional VLAN (VLAN ID 3003) reserved for use later in the evaluation guide.

A pool of IP addresses able to be used on the external routed (Production02) network for external network connectivity is required. This guide has 20 such IP addresses allocated, but the minimum number needed is 10.
Four IPs are required for each of the main virtual machine components, in addition to the IPs used by the physical hosts themselves. Each of these IP addresses must be resolvable through DNS by a FQDN. The following table lists the relevant information used for this guide.

<table>
<thead>
<tr>
<th>FQDN</th>
<th>ROLE</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>vc-01.tmsb.local</td>
<td>vCenter Server to be attached to VCD</td>
<td>One IP address is required.</td>
</tr>
<tr>
<td>vcd-01.tmsb.local</td>
<td>vCloud Director</td>
<td>vCloud Director requires two network interfaces. One is used for HTTP traffic; the other is used for the console proxy traffic. The FQDN name should resolve to the HTTP interface.</td>
</tr>
<tr>
<td>vsm-01.tmsb.local</td>
<td>VMware vShield Manager</td>
<td>One IP address is required.</td>
</tr>
</tbody>
</table>

**Storage Requirements**

The environment used for this guide has several datastores available. There are three datastores, each 100GB in size, for a total of 300GB of available storage. These datastores are configured as shared datastores that are available to all the hosts used in the evaluation environment. Differing types of storage, including SSD and SAS disks, back these datastores. Although it is not required to have different types of storage available, it would enable you to create multiple tiers of service offerings based upon the storage type.

To complete the procedures presented within this guide, you will need a minimum of 100GB of storage in a shared datastore accessible by the hosts in the resource cluster. Additionally you will need shared storage accessible by the hosts in the management cluster if you choose to deploy a highly available management cluster.

vCloud Director requires that DRS be enabled in fully automated mode. Automated DRS requires that shared storage be attached to all of the hosts. Ensure that the storage you use is visible from all of the hosts used in the resource cluster.

**Software and Licensing Requirements**

You will need software and licenses for an operating system that is supported by VCD as well as one that is supported for vCenter Server. Refer to the supported operating systems in the respective product documentation. In this evaluation guide, a Windows 2008 R2 64-bit operating system (OS) was utilized for vCenter Server, and a Red Hat Enterprise Linux (RHEL) 5.6 server 64-bit image is used for the vApps created within the private cloud. The vCloud Director instance used in this guide also uses an RHEL 5.6 64-bit image, if not using the vCloud Director Appliance.

This guide uses vSphere 5.0 in Evaluation Mode. This enables all of the features of vSphere and does not require a license until the end of the evaluation period.

You will also need an evaluation license for vCloud Director as well as the binaries for VCD, vCenter Server, VMware vShield Manager available. The license keys can be obtained when you download the binaries from VMware.
To assist you in preparing for this evaluation, the following table provides a list of the software you will need before you begin.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>QUANTITY</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere 5.0</td>
<td>1</td>
<td>No license needed, run in Evaluation Mode. Downloadable when you download vCloud Director from VMware.</td>
</tr>
<tr>
<td>vCloud Director 1.5</td>
<td>1</td>
<td>Obtain license when you download the binaries from VMware.</td>
</tr>
<tr>
<td>VMware vShield Manager</td>
<td>1</td>
<td>Downloadable when you download vCloud Director from VMware.</td>
</tr>
<tr>
<td>Windows 2008 R2</td>
<td>2</td>
<td>Use 64-bit version. To be used for the vCenter Server instance.</td>
</tr>
<tr>
<td>RHEL 5.6</td>
<td>3+</td>
<td>Use 64-bit version. Used for the virtual machines to be built within vCloud Director. Can also be used for the vCloud Director instance if the vCloud Director Appliance is not used.</td>
</tr>
<tr>
<td>ESXi</td>
<td>3-4</td>
<td>Downloadable when you download vCloud Director from VMware. Licensed as part of setting up vSphere in Evaluation Mode.</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 Express</td>
<td>1</td>
<td>Use 64-bit version. Downloadable from Microsoft.</td>
</tr>
<tr>
<td>vCloud Director Appliance*</td>
<td>1</td>
<td>Downloadable from VMware. After registering for the download, a license will be provided.</td>
</tr>
</tbody>
</table>

*NOTE: If using the vCloud Director Appliance, you will not need Microsoft SQL Server or the vCloud Director binaries, because the vCloud Director Appliance includes vCloud Director and an embedded Oracle Database 11g R2 XE. Use of the vCloud Director Appliance will also decrease the number of RHEL 5.6 licenses needed.

### Software Configuration

Before beginning the procedures listed in this guide, it is expected that some of the management and resource cluster components have already been configured. For the management cluster, this means that you have created a vSphere environment managed by an instance of vCenter Server that contains at least one ESXi 5.0 host. One virtual machine with a Windows 2008 R2 64-bit OS is required to be running within this environment. If you are not going to use the vCloud Director Appliance, one additional virtual machine is required. This virtual machine will be configured with an RHEL 5.6 64-bit operating system and will be used for vCloud Director.

The following chart contains information specific to the two virtual machines used in the management cluster, assuming the vCloud Director Appliance is not used:

<table>
<thead>
<tr>
<th>VIRTUAL MACHINE</th>
<th>CPU</th>
<th>MEMORY</th>
<th>OS DISK SIZE</th>
<th>OS</th>
<th>NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Director</td>
<td>Two vCPUs</td>
<td>2G</td>
<td>25G</td>
<td>RHEL 5.6</td>
<td>Two network interfaces</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Two vCPUs</td>
<td>4G</td>
<td>35G</td>
<td>Windows 2008 R2</td>
<td>One network interface</td>
</tr>
</tbody>
</table>
If you are using the vCloud Director Appliance, the virtual machine for vCloud Director shown in the preceding chart is not required. However, the vCloud Director Appliance will require approximately 30GB of disk space—assuming thick provisioning is used—and also the IP information to associate with the two network adaptors it will use.

For the resource cluster, it is assumed that you have two hosts with ESXi 5.0 installed. It is also assumed that the appropriate storage and network connectivity is configured.

Because vCloud Director fully leverages secure communications between the various components, it is important that the time on all the systems, including the VCD database, are synchronized to a common time source. Configure each virtual machine to use NTP to maintain the clock within a 2-second drift of each other.

### Evaluation Procedures

The evaluation is divided into five sections. Each section presents a series of tasks to be completed. Completion of these tasks will enable you to evaluate the core functionality of vCloud Director.

![Evaluation Procedures Diagram](image)

Because this guide is intended to walk you through an evaluation of vCloud Director, the procedures given build upon each other. Due to this, the procedures are to be performed in the order presented unless otherwise noted.

This guide was also designed to enable evaluating vCloud Director with limited resources. A result of this is that some of the procedures do not conform to best practices that should be followed when deploying vCloud Director in a production environment. Whenever possible, procedures that directly conflict with best practices are called out. In short, the procedures listed here are for evaluation purposes only.

**Evaluation Scenario**

To facilitate the procedures performed within this guide, it helps to have a story that explains the reason for performing the procedures. The following is the basic scenario that we will be using throughout this guide:

You are the IT administrator for a software development company that produces a widget based upon a LAMP stack. You are deploying vCloud Director to provide a secure, self-service, private cloud for use by your software development and quality assurance teams. Because this is mostly for development, this environment is considered by your company to be for preproduction use only.

Each of the teams resides in different physical locations in the world, but they tend to utilize the same types of system configurations.

**Infrastructure Installation**

In this section, you will install and configure the components that will provide the foundation upon which you will build a private cloud. This includes installation of vCloud Director, the VCD database, and the vCenter Server instance that will be attached to VCD.

In this guide, there are two methods shown for installing the vCloud Director components. One is through the use of the vCloud Director Appliance. This virtual appliance consists of a virtual machine that is preconfigured with vCloud Director and an embedded Oracle Database 11g R2 XE. The other method involves the installation of vCloud Director and a Microsoft SQL Server 2008 R2 Express database.
The vCloud Director Appliance is perfect for performing quick evaluations of the vCloud Director product and functionality. Because it comes preconfigured, deployment of the virtual appliance takes minutes, after which you can use and evaluate all the features and functionality of vCloud Director. The vCloud Director is specifically designed for evaluation environments only and is not for production deployments.

It is understood that some people who want to evaluate vCloud Director also want to evaluate the procedures that they would have to actually perform in the event of a production deployment. For this reason, both of these methods are shown in this guide.

As a result of demonstrating these two methods, there are some procedures in this section that are not applicable when using a given method. The processes that are affected by this are noted. Pay attention to this as you progress through this evaluation guide.

**Installing vCenter Server**

The first step in building an environment to evaluate vCloud Director is to install the vCenter Server instance that will be associated to vCloud Director. This vCenter Server instance and the resources that it maintains will become the foundation of resources used within vCloud Director. You will install this vCenter Server instance on the virtual machine you configured previously in the management cluster that is running the Windows 2008 R2 64-bit OS.

To begin, make the media for the vSphere 5.0 installation available on the Windows virtual machine and start the installer.

After starting the VMware vSphere installer, the above screen is shown. This interface enables you to start the installation of several different components. One of these is vCenter Server. Select this component and click the **Install** button.
After selecting the appropriate language you want to use, you will be prompted to begin the installation of VMware vCenter Server.

Acknowledge the End-User Patent Agreement and click Next to continue.
After reading and agreeing to the license agreement terms, click **Next** to continue.

On the next screen, you will be prompted to enter your customer information. For the purposes of this guide, leave the **License key** field blank in order to install vCenter Server in Evaluation Mode. This will enable all of the features of vCenter for 60 days. Enter the appropriate information and click **Next** to continue.
vCenter Server requires a database to store its information. During this evaluation, we will have a very small deployment. As such, it is sufficient to use the Microsoft SQL Server 2008 R2 Express instance for vCenter Server.

After entering the fully qualified domain name for the vCenter Server system, click **Next** to continue. If you have not done so before this, ensure that the name entered here is resolvable through DNS.
Accept the default file locations and click **Next** to continue.

This guide will use only one vCenter Server instance for vCloud Director. As a result, there will be no other vCenter Servers that are available to be connected to in Linked Mode. vCloud Director can connect to multiple vCenter servers in either standalone mode or Linked Mode. Ensure that the **standalone mode** option is checked and click **Next** to continue.
Accept the defaults for the port assignments and click **Next** to continue.

Accept the defaults for the Inventory Service and click **Next** to continue.
The **Small** size will be sufficient for our purposes. Select this option and click **Next** to continue.

At this point, you have answered all the information required to install vCenter Server. Click **Install** to begin the installation.
The installation will take a couple of minutes. During this time, you will see various screens displayed as the vCenter Server components are being installed. Wait until the installation completes.

When the installation is completed successfully, click **Finish** to exit the installer.
Configuring vCenter Server
After vCenter Server has been installed, we can move forward with configuring that vCenter Server instance for use with vCloud Director.

Using the VMware vSphere® Client™, connect to the vCenter Server instance after specifying the appropriate security information.

After logging into the vCenter Server instance, create a new datacenter called EvalDatacenter. After the datacenter has been created, create a cluster. In this guide, the cluster name created is cluster-01. This cluster
will act as the resource pool that will be abstracted by vCloud Director and made available to users of the private cloud later. When creating the cluster, ensure that you enable DRS in **Fully automated** mode. To do this, select the **Turn on vSphere DRS** checkbox when creating the cluster.

As you continue through the cluster creation wizard, ensure that the automation level for DRS is set to **Fully automated**.

After completing the cluster creation wizard, you are now ready to add hosts to that cluster. During this evaluation, two hosts will be added to the cluster configuration. These hosts will provide the resources that will be consumed by vCloud Director as users create workloads in the private cloud. These two hosts are the two ESXi 5.0 hosts for the resource cluster that you previously configured.
After the addition of the two hosts to the cluster, your view from the vCenter Client should resemble the above picture.

In the configuration used by this guide, selecting a host’s networking configuration shows that there are several port groups defined as part of a vSphere standard switch. These port groups were created automatically based upon the existing configuration of the underlying infrastructure. Your particular display might vary slightly from this. At a minimum, however, all of the ESXi hosts used by vCloud Director must contain at least one vSphere standard switch that has a standard virtual machine port group.
It is important to notice here that there is a port group called Production02 that has a VLAN ID of 3001. This VLAN is the same VLAN that we will use for our external network.

vCloud Director is best deployed with a vNetwork distributed switch (vDS). This allows vCloud Director to enable vCloud Director Network Isolation and the use of dynamically created networks. Because a vDS is not created by the default installation of vCenter Server, you must add one to the environment. Accept the default name and options when creating the vDS.

Either during the creation of the distributed switch or afterward, create a port group called External Network. If assigning a VLAN ID in your environment is required as it is in this guide, ensure that it is completed as well. After the distributed switch and external network port group have been created, your display of the vSphere distributed switch should look similar to the above diagram. In this example, we have used the same VLAN ID (3001) that is used by the Production02 port group on the vSphere standard switch.

This concludes all the configuration tasks required to be performed on vCenter Server.
Deploying VMware vShield Manager

VMware vShield Manager provides the network services to vCloud Director and to vCenter. It must be installed under the vCenter Server instance that is to be used by vCloud Director. Each vCenter Server that is associated with a vCloud Director must have a unique instance of VMware vShield Manager associated with it.

The quickest and easiest method to deploy VMware vShield Manager is by using the VMware vShield Manager OVF template. To do this, select the Deploy OVF Template option from within the vSphere Client.

When prompted, enter the location for the OVF file to be deployed and click Next to continue.
The OVF deployment wizard will show the information associated with the OVF file that you are to deploy. Click **Next** to continue.

After accepting the license agreement, click **Next** to continue.
In the space provided, type in the name of the VMware vShield Manager virtual machine to be created. This guide will use the name vsm-01. Click Next to continue.

Select the location where you want to store the VMware vShield Manager virtual machine to be created. Click Next to continue.
The next screen enables you to select a disk format for the virtual machine. Choose an option and click **Next** to continue.

The following page enables you to select the network mapping for the VMware vShield Manager virtual machine. In this guide, we will accept the default selection because this provides a mapping to the Production02 port group on the standard switch on our vCenter Server instance. Click **Next** to continue.
A summary of the deployment is shown on the next screen. Check **Power on after deployment**. Click **Finish** to begin the VMware vShield Manager deployment.

It will take a couple of minutes for the VMware vShield Manager to be deployed. Wait until the process completes and the VMware vShield Manager virtual machine is in the powered-on state.
After the VMware vShield Manager has been deployed successfully, use the vSphere Client to access the console for the virtual machine.
After you are connected to the console, you will be prompted to log in. The default user is **admin** and the default password is **default**. After you log in, enter the command

```
enable
```

followed by the command

```
setup
```

to access the VMware vShield Manager configuration dialog.

The configuration dialog will lead you through a series of prompts to enter the IP information for the VMware vShield Manager. Enter the relevant information and save the configuration. Log out of VMware vShield Manager and close the console.
Installing and Configuring Microsoft SQL Server 2008 R2 Express

vCloud Director requires a database to store its information. As of vCloud Director 1.5, both Microsoft SQL Server and Oracle Database are supported. For specific database versions supported, refer to the vCloud Director Installation Guide.

Because the vCloud Director Appliance includes a database, this procedure is not required when using the appliance.

If you are not using the vCloud Director Appliance, this procedure demonstrates how to install and configure Microsoft SQL Server 2008 R2 Express—available as a free download from Microsoft—for use as the vCloud Director database.

We will be installing this database on the same system that we are using for the vCenter Server instance installed earlier. Although this satisfies the requirements for this evaluation, it is important to remember that this would not be a recommended configuration for a production deployment.

Access the Microsoft Web site to download Microsoft SQL Server 2008 R2 Express. Select the 64-bit version that includes the database tools. Download it to a location available to the vCenter Server instance installed earlier.

On the vCenter Server system, start the Microsoft SQL Server 2008 R2 Express installation by double-clicking the file you downloaded earlier. Select New installation or add features to an existing installation.
Select **New installation or add features to an existing installation**. Because we are performing this installation on the same system where we installed vCenter Server, you’ll notice that the installer automatically detects the vCenter Server database, which also used Microsoft SQL Server Express. We will not be affecting the vCenter Server database instance, but it is important to note the name used to avoid confusion later.

Accept the license agreement and click **Next** to continue.
The default selection for the features to install is sufficient for our purposes. Click Next to continue.

When prompted, enter a name for the database instance to be created. Use VCD_SQLEXP for this purpose and click Next to continue.
Accept the defaults to the Server Configuration page and click Next to continue.

When using Microsoft SQL Server as the vCloud Director database, it is required that it be configured to use Mixed Mode authentication. Select this mode and enter a password for the SQL Server system administrators account in the spaces provided. click Next to continue.
Click **Next** to continue past the Error Reporting page.

At this point, the installation process will begin. Wait until it completes.
After the installation has completed successfully, you will see a dialog similar to the one above. Click Close to continue.
Before the Microsoft SQL Server database is usable, we must first create a database for vCloud Director. Open a command prompt on the system to access the “sqlcmd” command. This can be done by typing “cmd” into the search box in the start menu and selecting “cmd.exe executable.” Through the use of this command, enter the following to create the vCloud database and a user that will enable access to it. Refer to the picture on the preceding page for an example of the use of the “sqlcmd” command.

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
USE [vcloud]
GO
ALTER DATABASE [vcloud]
SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud]
SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud]
SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE = [vcloud],
DEFAULT_LANGUAGE = [us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

**NOTE:** The settings specified for the database are purely for use in this evaluation environment. When creating this database in a production environment, you must evaluate what database settings will provide you with the best performance.
To allow access to the vCloud database, we must enable network communication to it. The SQL Server Configuration Manager tool enables us to configure the network communication for the database.
Under the **SQL Server Network Configuration**, select **Protocols for VCD_SQLEXP** on the left-hand navigation pane. Double-click **TCP/IP** and change **Enabled** to **Yes**.

After applying the changes, a pop-up dialog message box will appear, informing you that the database instance must be restarted for the changes to take effect. Acknowledge the dialog and click **OK** to continue.

Under **SQL Server Services**, right-click **SQL Server (VCD_SQLEXP)** and click **Restart**. Wait until the restart completes and then close the **SQL Server Configuration Manager** utility.
Deploying the vCloud Director Appliance

If you are not using the vCloud Director Appliance, you can skip ahead to the next procedure, entitled “Installing the vCloud Director Binaries”; otherwise, this procedure will demonstrate how to deploy the vCloud Director Appliance.

To begin, ensure that either the OVF template files or the OVA file for the vCloud Director Appliance is accessible from the vCenter Server instance that manages the management cluster components. You will deploy the vCloud Director Appliance on the ESXi host(s) within your management cluster, using this vCenter Server instance.

Under File, select Deploy OVF Template... from the vCenter Server Client connected to the vCenter Server instance for management cluster.

When prompted, select the location of the vCloud Director Appliance OVA file and click Next to continue.

The wizard will display some general information about the vCloud Director Appliance. Click Next to continue.
On the next screen, you will be prompted to enter a name for the virtual machine that will be the vCloud Director Appliance. Enter an appropriate name and click **Next** to continue.

Next, select the cluster where the VMware vCloud Director Appliance will reside. Click **Next** to continue.

On the next screen, you will be asked to select a host within the management cluster to be assigned to the virtual machine to be created. Select one of the hosts in your management cluster and click **Next** to continue.
You will then be prompted to select a storage location to store the virtual machine files. Select an appropriate location and click **Next** to continue.

On the next screen, select the type of format you’d like to use to store the virtual disks of the virtual machine. Click **Next** to continue.

The next screen enables you to select the networks that you want to use for the vCloud Director instance. Each vCloud Director instance requires two network connections, one for the HTTPS service that provides access to the API and the user interface, and one for the console proxy services that provide access to the deployed virtual
machine consoles. Ideally, these would be two separate networks to enable the greatest level of security. In this guide, we will use the same physical network and will assign different IP addresses to each of the interfaces, with the understanding that this is only for an evaluation environment and not a best practice. As a result, in this example both of the source networks for the vCloud Director Appliance are mapped to the same destination network, Production02. This displays a warning message that we can safely ignore. Select Next to continue.

The next screen displayed by the wizard enables you to enter the network-specific information for the vCloud Director Appliance. As mentioned earlier, you will need two IP addresses, which are associated with the HTTPS service and the console proxy service. The vCloud Director Appliance will automatically use the lower IP address—as determined through a string comparison—to be used for the HTTPS service.

For example, if you were to define an IP address of 192.168.10.1 for the network 1 IP address and an IP address of 10.10.10.1 for the network 2 IP address, the 10.10.10.1 address would be used for the HTTPS service and the 192.168.10.1 address would be used for the console access.

Configure this information as applicable to your environment and click Next to continue.

Finally, you will be presented with a summary screen that displays the information you selected from within the wizard. Verify that this information is correct and click the checkbox to start the virtual machine when deployment is completed. Click Next to start the process of deploying the OVF template.

After it is deployed, the virtual machine is started automatically. You can then skip to the procedure entitled “vCloud Director Initial Setup.”
Installing the vCloud Director Binaries

The next task is to install the vCloud Director binaries. This procedure is required only if you are not using the vCloud Director Appliance. Only the binaries will be installed at this time. This is to enable us to leverage the Java Runtime Environment Version 6 binaries installed with vCloud Director, to generate the SSL certificates required as part of the vCloud Director configuration later.

Copy the vCloud Director binary to a location accessible from the vCloud Director guest OS. Ensure that the binary is executable by using the following command:

```
chmod +x <vCloud Director binary>
```

Execute the binary to start the installation process.

```
./<vCloud Director binary>
```

When prompted, answer No to running the vCloud Director configuration script.
Generating SSL Certificates

vCloud Director requires that secure communications be utilized, which means SSL certificates must be configured. For the purposes of this evaluation guide, we will be creating a pair of self-signed SSL certificates. One will be used for the vCloud Director IP address used for HTTP traffic; the other will be used for the console proxy traffic.

This procedure is required only if you are not using the vCloud Director Appliance.

In a production environment, best practice would be to use signed SSL certificates instead.

In a terminal window, change directories to the /opt/vmware/vcloud-director/jre/bin directory.

```bash
cd /opt/vmware/vcloud-director/jre/bin
```

From here, execute the following command to generate a self-signed SSL certificate for the HTTP traffic:

```bash
keytool -keystore /certificates.ks -storetype JCEKS -storepass password -genkey -keyalg RSA - alias http
```

This will create a key file called certificates.ks under the root (/) directory. In the case of an evaluation, we are placing the file here to keep the procedure as simple as possible. If you store this file in a different location—as would be recommended for a production environment—keep in mind that the vCloud Director configuration script will not run as a privileged user. This means that the certificates.ks file you create must reside in a location accessible by all users.

The password for the keystore file is set to “password” with the above command. In a production environment, you would want to set this to a password of better quality.
Use the keytool command again to generate a self-signed SSL certificate for the console proxy traffic.

```bash
keytool -keystore /certificates.ks -storetype JCEKS -storepass password -genkey -keyalg RSA - alias consoleproxy
```

As we did with the SSL certificate for the HTTP traffic, we are storing the console proxy SSL certificate in the certificates.ks keystore file under the root (/) directory.

Verify that the keystore contains the two SSL certificates by using the following command. The output should resemble the screenshot above.

```bash
keytool -storetype JCEKS -storepass password -keystore /certificates.ks -list
```
vCloud Director Configuration

After the SSL certificates have been created, the vCloud Director configuration script that we did not run after the installation of the VCD binaries can be started. Again, this procedure is relevant only if you are not using the vCloud Director Appliance.

The configuration script prompts you for the IP addresses to be used for the HTTP service and the remote console proxy. As mentioned earlier, the system used for VCD requires two IP addresses, one for the HTTP traffic and one for the console proxy traffic. In this configuration, the VCD system has two network adaptors, each configured with an IP address on the same network. In a production environment, you likely would have two different networks used for the same purpose.

Select the appropriate IP addresses and then provide the configuration script to the location for the SSL certificate key store created earlier.

For the purposes of this guide, press Enter when prompted, to skip the configuration of a remote syslog host.
Select the option for using a Microsoft SQL Server as the vCloud Director database. Enter the name for the host where the vCloud Director database was installed. In this case, the server name is the same as our vCenter Server (vc-01.tmsb.local).

Accept the default port (1433) for the database. When prompted, enter the information for the vCloud Director database, including the database name, the database instance name, and the database user.

This guide used the database instance name of VCD_SQL. During the configuration of the vCloud database earlier, we also created a user (vcloud) and assigned the password of "vcloudpass" to this user.
After entering the correct password, several messages will be displayed as the vCloud Director configuration script communicates to the Microsoft SQL Server database and configures it for use.

When prompted, start the vCloud Director process and allow the vCloud Director configuration script to complete. Notice that the configuration script displays the URL for accessing the vCloud Director user interface.
vCloud Director Initial Setup

Before you can start using vCloud Director, you must complete the initial installation that is presented the first time you log in to the VMware vCloud Director interface.

Using the URL of https://<VCD HTTP IP address>, connect to the vCloud Director instance.

Upon the initial connection, a screen summarizes the steps that are required to be preformed. Click Next to continue.

Accept the terms of the license agreement and click Next to continue.
On the next screen, enter a valid license key for vCloud Director and click **Next** to continue.

Next, create an administrator account by specifying the desired user name, password, and contact information. Continue by clicking **Next**.
The next screen enables one to define the name of the vCloud Director instance to be installed. It also enables you to specify an ID unique to this vCloud Director installation. This ID is used to seed selection of MAC addresses. In a production environment, it must be unique—that is, different from any other vCloud Director installations—to avoid MAC conflicts.

Click **Next** to continue.

Review the setup information. If it is correct, click **Finish** to finalize the vCloud Director setup process.
After the setup is completed, log in to vCloud Director using the administrator account defined earlier.

At this point, you have vCloud Director up and running. If you are using the vCloud Director Appliance, you might need to obtain access to the virtual machine or the Oracle Database 11g R2 XE instance installed. This might be required, for example, in the event that you must modify the IP addresses used by vCloud Director. The following are the default username and password for each:

VMware vCloud Director Appliance virtual machine:
username = root
password = Default0

VMware vCloud Director Appliance/Oracle Database 11g R2 XE instance:
username = vcloud
password = VCloud

**Attaching to Virtual Center**

With vCloud Director up and running now, the first step in building a private cloud environment is to attach the vCloud Director to the vCenter Server instance created earlier. This will provide vCloud Director with the resources that it will abstract later for use by the end users.

After you log in to vCloud Director, you’ll notice a **Quick Start** section. This provides an easy accessible list of the tasks that must be accomplished. Select the first item on the list: **Attach a vCenter**.
After making the selection, a wizard pops up to guide you through the process of attaching a vCenter Server. Enter the appropriate information in the spaces provided and select Next to continue.

The next screen prompts you to provide the information for the VMware vShield Manager instance that is associated with the vCenter Server that is being attached. In this example, we have not changed the default user name and the password for VMware vShield Manager. Although this is not a best practice, it enables one to specify the default User name (admin) and Password (default) here.
Review the summary and click Finish.

At this point, you have finished the configuration of the infrastructure components required to start building a private cloud. This involved the installation vCloud Director, a database for VCD, VMware vShield Manager, and a vCenter Server instance that is attached to vCloud Director.

**Defining the Provider Virtual Datacenter**

In this section, you will start the process of configuring vCloud Director and defining the resources that will be consumed by the organizations.

**Creating a Provider vDC**

After a vCenter Server has been attached to vCloud Director, the resources that it offers can be added to a provider vDC. Having the ability for multiple vCenter Servers to be connected to vCloud Director, a provider vDC creates a layer of abstraction for all of these resources.

One way to think about this is that provider vDCs represent the pools of resources that will later get divided up between the various organizations within your vCloud Director environment. In other words, the resources that make up a provider vDC define, in essence, an offering available to your consumers.

On the home screen for vCloud Director, click the **Quick Start** link for creating a provider vDC.
This brings up a wizard that will walk you through the process of creating a provider vDC. The first part of this process is to name the provider vDC to be created. In this guide, the scenario is that this is being built for a company's private cloud in their preproduction environment. Because of this, we will name the provider vDC in such a manner as to enable easy distinction between it and other environments (such as a production environment) that would be added later.

Because we will be using this provider vDC, ensure that the Enabled checkbox is selected.

With all the hosts in this environment being ESXi 5.0 hosts, we can safely select hardware version 8 to be used. If we had a mix between VMware ESX® 5 and ESX 4.1, we might want to select hardware version 7, or even 4, to ensure compatibility. Click Next to continue.

Selecting a resource pool is the next step. In this example, the resource pool that will be utilized is the root resource pool of the cluster (cluster-01) that we created previously on the vCenter Server. Select this from the attached vCenter Server and click Next to continue.
The wizard then enables you to add datastores that are available to the attached vCenter Server as a pool of space to be used in the provider vDC. Select each of the datastores that you want and click Add to populate the bottom table.

Click Next to continue.

Each of the hosts within the resource pool selected must be prepared for use with vCloud Director. This step will install and configure the vCloud Director agent on each of the hosts. To do this, vCloud Director must be configured with the administrative (root) user name and password for each of the ESXi hosts.

Enter the appropriate information here and click Next to continue.
After reviewing the summary information, click **Finish** to complete the process of creating a provider vDC.

**Defining an External Network**

An external network is one that enables virtual machines in your cloud to connect outside of your cloud environment. You can use this external network to provide access to a corporation's intranet or to the Internet, or even to establish an IPSec VPN connection to another external network or another organization.

To start, click the **Create an external network** link on the Quick Start section of the **Home** screen.
The wizard that is brought up enables you to select a port group that is managed by an attached vCenter Server for use as an external network. Earlier, we created a port group on a vDS called **External Network**. Select this port group name from the attached vCenter Server and click **Next** to continue.

The next screen enables you to specify the network settings for use with the external network. At a minimum, you must specify the netmask and the default gateway values. In this guide, we also will specify the DNS information because this external network has its own DNS servers that we want to use.
This screen also enables you to configure a pool of IP addresses that can be dynamically allocated to objects within the vCloud Director environment that need access to this external network. These addresses must be reserved for use with vCloud Director, preventing an IP conflict with another device on the external network.

Enter the relevant information and click Next to continue.

Last, we must provide a name for this external network. Because this network is for use solely in our preproduction cloud environment, we will use the name “Pre-Prod External Network.”

Review the summary information provided and click Next to complete the process of adding an external network.

**Network Pools**

Network pools provide a collection of undifferentiated networks that are then consumed by organizations to provide connectivity within the cloud environment. vSphere network resources such as VLAN IDs and port groups back a network pool or cloud isolated networks. These network pools are used by VCD to create NAT-routed and internal organization networks and all vApp networks.
Creating a network pool starts by clicking Create a network pool in the Quick Start section of the Home screen.

There are different options for creating network pools. Each of these methods enables different ways to segment the networks used by vCloud Director from each other. These include the following:

- **VLAN-backed**
  These network pools enable you to register vSphere VLAN IDs for vCloud Director to use. vCloud Director creates networks as needed, assigning each network a VLAN ID. To use this kind of network pool, the ESX servers must be connected to a trunk port that provides the VLAN IDs reserved in the preceding dialog.

- **Network isolation-backed**
  A cloud isolated network spans hosts, provides traffic isolation from other networks and is the best source for vApp networks. An isolation-backed network pool does not require preexisting port groups in vSphere.

- **vSphere port group-backed**
  This option enables you to register vSphere port groups for vCloud Director to use. Unlike other types of network pools, a network pool that is backed by port groups does not require a vSphere distributed switch. It does, however, require port groups to be manually preconfigured.

For both the VLAN- and port group-backed network pool options, care must be taken to ensure that the networks used are properly isolated at the Layer 2 levels. Refer to the vCloud Director 1.5 Administrator’s Guide for more information.

For our evaluation purposes, we are going to choose to create the network isolation-backed option. This option will automatically create and delete port groups on the vDS we created earlier, as networks are consumed. All of these networks are completely isolated from each other.
After selecting the type of network pool, we proceed to configure the network pool properties. Because this is a small evaluation deployment, we’ll specify a small number of isolated networks (20) that we want to have. The environment used for this guide had a VLAN reserved for this purpose, as explained earlier. We will use a VLAN ID of 3003 to carry traffic for the isolated networks.

After defining the network pool properties, select the attached vCenter Server instance and the distributed switch created earlier.

The name for this network pool will be defined as “Pre-Prod Pool.” This will help us distinguish it later if we decide to add more network pools for environments such as a production environment.
Review the action summary and click **Finish** to complete the network pool wizard.

Now you have completed the configuration of a provider vDC and the resources that can be allocated to organizations. You’ve defined the networks and the network pools that can be used, as well as the datastores that will be consumed.

**Organization Creation**

Now it is time to create the organizations that will consume the resources previously configured in the provider vDC. You will create two organizations in this section. One will be for the development organization; the other is for the QA organization. These two organizations will leverage the resources in the provider VCD for the workloads they create.

**Creating an Organization**

Having completed the process of creating a provider vDC, we are ready to define the organizations that will consume resources within our cloud. An organization is a primary building block of your cloud environment. It is here where users are defined and given the ability to create vApps.

Start the process of creating an organization by clicking **Create a new organization** in the **Quick Start** section on the vCloud Director **Home** screen.
The first organization that we will create is for preproduction developers. Populate the text fields with the information shown above and click Next to continue.

vCloud Director makes it easy to obtain user and group information from an LDAP-based user authentication source. For this evaluation, we have not created an LDAP server. Instead, we will manually define the organization users and the privileges that are associated with them.

The next screen enables us to manually define the users of this organization. To add a new user, click Add.
You are then prompted for the information required for the user to be created. The first user that we will create will be the `dev_mgr` user. This user is the manager of this organization. Because this user will need full access to modify this organization, ensure that the role associated to this user is that of an organization administrator.

After creating the `dev_mgr` user, add another user called `dev_user`. This user is a consumer of the resources of the organization. As such, we can simply assign the role of `vApp User` for this user account. If this user were to have additional responsibilities, such as creating vApps, then we would assign the user the `vApp Author` role.
Catalogs are a collection of vApps, vApp templates, and media. An organization can create multiple catalogs. For example, an organization might choose to create a catalog of vApps that contain a set of builds for a QA team to test. The same organization might have another catalog that would contain .iso image files for the OS installation media they use. At times, different organizations might find that they would create catalogs that contained many of the same items.

In this case, it is more efficient from a storage and management standpoint for an organization to share the contents of a catalog with other organizations in the cloud.

On this screen, you can enable the ability of an organization to share or not share their catalogs with others. Allow the publishing of catalogs and click Next to continue.

The wizard then prompts us to enter the notification settings chosen for the organization. Click Next to continue.
You are then enabled to set the policies for the organization. This includes setting the length of time that vApps can run, when vApps are automatically deleted, and so on.

By utilizing this mechanism, you can automatically reclaim resources so they can be allocated for another purpose later.

The defaults are sufficient for this evaluation, so click **Next** to continue.

Review the summary screen and click **Finish** to complete the organization creation process.
Allocating Resources to an Organization

After an organization has been defined, you can then allocate resources from the provider vDC to create an organization vDC. This gives you the ability to allow different organizations access to resources offered by provider vDCs in differing quantities.

Using organization vDCs offers the cloud administrator the ability to establish leases and quotas on the workloads to be created. It also provides different types of allocation models that are useful when determining how to best allocate resources.

From the Quick Start section on the Home screen, select the option to allocate resources to an organization.

The wizard then brings up a list of organizations that have been defined. Because we have only one Organization created at this time, select the Dev organization and click Next to continue.
The wizard then enables you to select the provider vDC that you want to consume resources from in the creation of the organization vDC. Select the **Pre-Production** vDC and click **Next** to continue.
The following three methods are available for you to choose how to control the quality of service and the costs associated with the resources that you will be allocating:

- **Allocation Pool**
  Only a percentage of the resources you allocate are committed to the organization vDC. You can specify the percentage, which enables you (the provider) to overcommit resources across multiple vDCs to different organizations.

- **Pay-As-You-Go**
  Resources are committed only when users create vApps in the organization vDC. You can specify a percentage of resources to guarantee, which enables you (the provider) to overcommit resources. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC.

- **Reservation Pool**
  All of the resources you allocate are immediately committed to the organization vDC. In this case, control of overcommitment passes to the users in the organization, who can control overcommitment by specifying reservation, limit and priority settings for individual virtual machines.

In this guide, we will be using the Pay-As-You-Go model of resource allocation. Select the Pay-As-You-Go model and click **Next** to continue.

Because we’ve selected the Pay-As-You-Go model, the wizard then displays a screen that enables us to adjust the allocation of resources. For our purposes, the default settings will provide ample ability to support the number of resources we will be using. Click **Next** to continue.
You are then prompted to define how to allocate storage within the organization vDC. You can set limits on how much storage can be used and choose whether you want to enable the use of thin or fast provisioning.

Fast provisioning drastically reduces the provisioning time for vApps by using linked clones for virtual machine provisioning operations.

A linked clone is a duplicate of a virtual machine. It uses the same base disk as the original, with a chain of delta disks that keep track of the differences between the original and the clone. If fast provisioning is disabled, all provisioning operations result in full clones.

Because all the hosts in our environment are ESXi 5.0 hosts, we can have fast provisioning enabled. Accept the defaults and click Next to continue.

The next step is to define the network pool to use. Here we can select the network pool created earlier (“Pre-Prod Pool”) and, if we choose to do so, assign quotas. Click Next to continue.
Last, we must name the organization vDC. Because this is for the development organization, we will name it **Dev** accordingly.

Review the summary information presented. If it is correct, click **Finish** to complete the process of creating the organization vDC for **Dev**.
Creating an Organization Network

With the organization vDC created, we can now define networks that will be available to vApps created within that organization vDC.

After selecting the Add a network to an organization link in the Quick Link section of the Home screen, a wizard is presented that will ask what type of network you want to create. By default, it will create two networks. One network will be a network strictly for communication between the vApps in an organization. The other network will be created to communicate to systems external to the vApp, such as the Internet.

There are multiple ways an external network can be defined. The first is a direct connection. This has no firewall or other protection in place. As a result, it depends on the security of the external network it is connected to. The second is a routed network that leverages the ability for vCloud Director to provide a firewalled external connection.

For the purposes of this guide, we will be accepting the default settings of creating an internal network as well as a routed external network.

The next couple of screens will walk you through the configuration steps required for the internal network. First, under Network Pool, you must select the one to use for the internal network. Select the Pre-Prod Pool that you created earlier and click Next to continue.
Next, you will be prompted to enter the IP settings for the internal network. We will opt to configure this network as a 192.168.1.0/24 network. Keep in mind that these networks are isolated from each other and are specific to an organization. This means that when we define other internal networks for other organizations (or this organization), we can use the same IP address information.

We will leave the DNS information blank for now. If we wanted to deploy a DNS server within the organization on this network, we might use that to provide DNS services.

By default, a range of 100 IPs will be set for use as static IPs for this network.

Next, we simply must provide a name for this internal network. We will call this the **Dev Internal Network**. By being descriptive here, we can avoid confusion later when we create more organizations. It will enable us to differentiate easily between our external and internal networks.
The wizard then will begin the process of asking us to define the external network settings. Select the **Pre-Prod External Network** and **Pre-Prod Pool** that we created earlier.

You’ll notice that the wizard will present a different network to be used by the external network than was used with the internal network. As a refresher, the internal network was 192.168.1.0/24; now the wizard is showing a 192.168.0.0/24 for the external network.
Because it is an external routed network, we will leverage the DNS settings used in our external network. Accept the defaults for the static IP range and click **Next** to continue.

We will name this external network **Dev Ext Routed Network**. This name enables us to determine the network type at a glance.

After you have reviewed the summary information, select **Finish** to complete the process of creating an organization network.
Creating Another Organization

To facilitate some of the activities presented later in this guide, we must create another organization and associate resources to it.

This new organization in our scenario will be for the QA organization. The steps to create this QA organization are the same as performed earlier for the development organization. The only changes are in the information specified. As such, we will forgo the step-by-step procedures and instead provide you with the information required so you can repeat the process.

The following will provide you with the requisite information and highlight any specific changes required. The information is presented in sections that correspond to the major sections in this guide and to the actions you performed earlier. It is advisable to go back to the associated section as you progress through the process of creating the QA organization with this information.

Creating a New Organization

When you create the QA organization, add two users (qa_mgr and qa_user) with the same privileges as you did with the users in the development organization.

The above is the summary screen from the New Organization wizard. Your summary should resemble the output here.
Allocating Resources to an Organization

The screen above shows the summary page that should resemble yours when you complete the process of creating the QA organization vDC.

Creating an Organization Network

When you create the QA Ext Routed Network, be sure to use a different network than the one specified for the Dev Ext Routed Network. In this example, we used the network of 192.168.7.0/24 for the QA Ext Routed Network. Later in this guide, we will tie these networks together. To do this, the external routed networks for QA and development must be different.
Enabling DHCP for an Organization Network

The use of DHCP in an environment greatly reduces the management demands on an administrator. vCloud Director provides the ability for a DHCP server to be used in each network. In this section, we will enable that functionality for external networks of the QA and development organizations.

Navigate to the Organization Networks table under the Manage & Monitor tab. Select the Dev Ext Routed Network and right-click to bring up the Network Menu. Select Configure Services…

You'll then be brought to a screen where you can configure the DHCP server for this network. After checking the Enable DHCP checkbox, ensure that the information is correct and click OK.

Repeat this process on the QA Ext Routed Network.
Accessing an Organization
Each of the organizations we have created is accessible through a portal specific to that organization. It is through this interface that organization users will create and use vApps within their respective organization datacenter.

To access the Organizations portal, select the organization under the Manage & Monitor tab. Right-click the organization and click Open.

You will then see a new tab displayed that is specific to that organization.

In completing this section, you have learned how to create an organization, assign networking and storage resources to it, and configure users with various privileges in the organization. You’ve also learned how each organization has its own portal and how to access it.
Developing Service Offerings

After the organizations have been created, you can now create catalogs for the content that can be readily consumed by members of the organizations. In this section, you will configure a vApp and learn how to make a vApp template as well as how to perform other tasks to help populate your private cloud catalogs.

Creating a Catalog

A catalog is a collection of vApps, vApp templates, and media that an organization uses.

To create a catalog, navigate to the Catalogs tab under the organization and click Add Catalog.

You will be prompted to enter the name of the catalog you want to create. Create a catalog called Dev OS Images and click Next to continue.

You then can specify whom you want to share this catalog with. You can share with individual users or groups or everyone in the organization. Click Add Members... to add some members of the organization to share this catalog with.
You’ll see how you can select individual users or groups. For the purposes of this guide, select **Everyone in the organization**.

After you have selected the members of the organization to share the catalog with, you can continue by clicking **Next**.
You will recall from the previous steps that we provided the ability for the organization to publish its catalogs so that they could be used by other organizations. We want to reduce the amount of waste incurred by multiple organizations' building catalogs of similar material. With this catalog's being used for OS images, it is a perfect candidate to be shared between organizations.

Select **Publish to all organizations**.

Review the summary page and click **Finish** to complete the wizard.

**Importing Media**

After a catalog has been made, we can add items to it so users can use them. To start, let’s add a media file.

Under the development organization’s **Catalogs** tab, select the **Media** tab. Here we can store ISO or FLP files that we will use later for installing applications or operating systems.
There are several methods that can be used to upload the media. You can upload it from your desktop, or you can import it from a datastore that is accessible by an attached vCenter Server instance.

For this example, we are going to upload an RHEL 5.6 ISO image by importing it from vCenter Server. If you happen to have this ISO image on your desktop, you can use that method as well.

After selecting the import from vCenter, a window pops up that asks for the relevant information. This includes the name of the media, where it can be found for uploading, and where to upload it.

Select the information appropriate for you and click OK to begin the upload process.

After the upload process has completed, you will see the media listed as being part of the catalog you selected.
Building a vApp

At this point, everything is in place for us to build our first vApp. A vApp is a collection of one or more virtual machines that run within an organization.

From the Dev portal, select Build New vApp from the Home screen.

Next, provide the wizard with the information about the name of the vApp. In our scenario, this will be a vApp that contains a virtual machine that is configured to run as a LAMP stack.
The next screen enables you to add virtual machines to this vApp. Because this is a new vApp, we have no virtual machines already defined. Click New Virtual Machine... to add one to the vApp.

You will then be given the ability to specify the virtual machine settings. Notice the settings used above and configure your environment similarly.
You will now see the virtual machine you specified listed in the **Virtual Machines** table. We will be adding only one virtual machine to this vApp. Click **Next** to continue.

Now the wizard will enable you to select the organization vDC where this vApp will be stored. Ensure that the Development vDC is selected.

This page also enables you to select the networks that will be used by this vApp. Select **Dev Ext Routed Network** so the virtual machines in the environment will be able to get external access to the network. Leave the IP assignment as **Static – IP Pool** so the virtual machines in this vApp will be assigned an IP address from the static IP pool we previously defined for the **Dev Ext Routed Network**.

The last wizard screen enables you to select from various options on how the network is used. This includes the ability to **Fence vApp** and the related difficulties of the IP assignment. Select **Always use assigned IP addresses until this vApp or associated networks are deleted** and click **Next** to continue.
To complete the process of creating your vApp, review the changes and click **Finish** if correct.

Although we now have a virtual machine listed under our newly created vApp, it is of little use until we have installed an operating system. To do this, we will connect the ISO image of the RHEL OS that we previously stored in our catalog to the CD-ROM device for the virtual machine.
Right-click the virtual machine and select this option from the context menu.

You’ll then see a list of all the media in the catalogs available to you. Select the RHEL 5.6 media that we added to our catalog earlier.

Now you are ready to power on the virtual machine and start the process of installing the operating system.
Right-click the virtual machine and select the **Popout Console** option. This will enable you to access the console of the virtual machine from within your Web browser.

To use the pop-up console, you might be asked to install a plug-in for your Web browser. If so, install the plug-in as needed.

Proceed with installing the OS as you normally would. Ensure that when asked for the network configuration, you specify that the OS should obtain its IP information from DHCP. This will enable you to take advantage of the DHCP server we configured earlier for this network.
After the OS has been installed, access it and test to see if you have network connectivity with the outside world. Everything should work, including DNS lookups.

**Creating a vApp Template**

A vApp template enables users in an organization to quickly deploy vApps that have already been configured. Creating a collection of vApp templates can enable users to avoid the time required to set up and configure an environment for use. It also can enable you as the administrator to define standardized versions of the vApps you want users to deploy.

Because vApp templates can use fast provisioning (if enabled), provisioning of new vApps from a template is very fast. The use of fast provisioning with a vApp template might also cause you to see an object called a “shadow virtual machine.” This is due to the fact that a linked clone cannot exist on a different vCenter datacenter or datastore than the original virtual machine. If this occurs, vCloud Director automatically creates and manages shadow virtual machines to support linked clone creation across vCenter datacenters and datastores for virtual machines associated with a vApp template. These shadow virtual machines are exact copies of the original virtual machine created on the datacenter and datastore where the linked clone is created.

To create a vApp template, we will use the vApp that you just created.

From the Dev portal, select the vApp that you want to create a template from. Before creating a template from a vApp, ensure that the vApp is stopped.
Right-click the vApp and select Add to Catalog...

In the window that is displayed next, enter the information for the vApp template. When finished, click OK to start creating the template.
After the template has been created, you will see it listed under the **vApp Templates** tab for the **Dev** organization.

**Deploying a vApp from a Template**

Creating future vApps from a template is a great way for users to provision their own environments quickly and easily. This is the foundation of IaaS.

Open the portal for the QA environment that you created previously. In this environment, we have not yet created any vApps. Select **Add vApp from Catalog** from the QA portal’s **Home** page.

The QA environment currently does not have any catalogs. However, previously we shared the catalog we created for the development organization with all other organizations. We will now leverage this published catalog in our QA organization. From the drop-down menu, select **Public catalogs**.
Now we can see the vApp template created earlier in the development organization. Select this vApp template and click **Next** to continue.

In our scenario, QA is going to use the template created for the LAMP stack to deploy a new vApp that will be used to perform application stress testing. As such, we will name this vApp **LAMP Stress Test**.

As we did previously when creating the vApp in **Dev**, we can now associate the networks that we want to be used by this vApp. Select **QA Ext Routed Network** and leave the IP assignment to use the static IP pool created for this network.
As before, select the option to always use the assigned IP address and click **Next** to continue.

Review the summary information and click **Finish** to create the vApp.
On the QA organization’s portal Home page, you will now see the vApp that was created. We will now enable the capacity to automatically customize the virtual machines within this vApp.

**Customizing a Virtual Machine**

The ability to customize a virtual machine is a powerful way to ensure that the virtual machine gets reconfigured when it gets powered on the first time. This customization can be used to set the name of the guest OS, AD domain information, and other required parameters. The customization can also be triggered after the first boot of a virtual machine, if needed.

As a side note, the guest OS used for the virtual machine to be customized in this guide is RHEL 5.6.

Customization of Windows-based guest operating systems might require the installation of the Microsoft Sysprep binaries into vCloud Director, depending on the version of Windows used. VMware knowledge base article 1005593 (http://kb.vmware.com/kb/1005593) provides information on how to obtain the required Sysprep files.

After you have the files, you must copy them to a location on each VCD instance you have. Then, execute the following command as the root user:

```
# $VCLLOUD_HOME/deploymentPackageCreator/
createSysprepPackage.sh <directory>
```

Here, `<directory>` equates to the directory where you have placed the files. After this, you must restart the VCD instance by using the following command:

```
# service vmware-vcd restart
```
Select the virtual machine in the LAMP Stress Test vApp you created for the QA organization. Right-click it and select **Properties** from the context menu.

In the **Properties** window, select the **Guest OS Customization** tab. Check the **Enable guest customization** box. By default, the customization process will generate a random password for the local administrator account. Enable this option and the ability to specify a password. Type in a new password for the administrator (root) account for this virtual machine so you can verify the customization later. Click **OK** to close the **Properties** window.
Now, start the vApp to power on the vApp and the virtual machine contained in it.

After the vApp has been started, use the pop-up console to gain access to the virtual machine. You might notice that the virtual machine will power on, perform the customization and then restart. After the virtual machine is fully powered on, log in as the root user with the password you specified during the customization.
You can then see that the guest OS was customized with the name of the virtual machine you specified for the vApp. It also has an IP address that was assigned from the static IP pool from the QA Ext Routed Network as we specified earlier. A test of the external connectivity should also show that you have external access.

By now you have been exposed to the basics of building a catalog of services that can be consumed by members of your private cloud. You’ve created a vApp, made vApp templates, populated a catalog with media and learned how to customize a vApp.

Cloud Security and Management

In this section, you will be exposed to some of the security features included with vCloud Director as well as some of the features that can assist you in managing the environment.

Site-to-Site VPN

One of the new features in vCloud Director 1.5 is the ability to establish a site-to-site VPN. You can enable a site-to-site VPN for an organization network and then create a secure tunnel to another network. This site-to-site VPN can connect organization networks in the same organization, organization networks in different organizations (including organization networks in different instances of vCloud Director) and remote networks. This is especially useful when configuring hybrid cloud configurations.

This functionally enables organizations to establish a secure communications path themselves without the need to involve a third entity (such as a service provider). This helps to streamline the process and further enable the users in an organization.

In the scenario for this guide, we mentioned that the QA and development organizations were situated in different physical locations. Using this as a premise, we will now create a site-to-site VPN tunnel between the two organizations.

VPN connections can be made only with routed networks. Select QA Ext Routed Network and right-click to bring up the context menu. Select Configure Services...
Under the Site-to-Site VPN tab, check Enable site-to-site VPN. Then click Add... to add a new network tunnel.

On the window that is displayed, enter the name for the VPN tunnel. We will create a tunnel that connects the QA and development organizations in this example. Again, we are doing this purely for evaluation. In a production environment, the organizations would exist under different provider vDCs. To do so, select Tunnel to: a network in another organization.
To add the tunnel, you must click **Connect to another organization** and specify the URL for the vCloud Director that manages the organization you are connecting to. In this case, we are connecting to the **Dev** organization. The vCloud Director instance is the same as the one used by the QA organization.

You also must specify the name of the organization (**Dev**) and the username and password for a user who has administrative access in that organization. Use the username for the dev_mgr user that you created earlier and click **Connect**.

Leave the rest of the settings at the default settings and click **OK** to add the VPN connection.
You’ll notice that the VPN tunnel is now shown under the **Site-to-Site VPN** tab. **Status** will show as **Connecting** for at least 2 minutes. In our case, it will continue to stay in the connecting state because we have not enabled the development organization’s VPN ability.

To do this, go to the development organization, select **Dev Ext Routed Network** and then select **Configure Services...**
Under the **Site-to-Site VPN** tab, you will see that the tunnel has been configured but the VPN service is not enabled. This will prevent the VPN tunnel from becoming active.

Check **Enable site-to-site VPN**.
After approximately 2 minutes, you will see the **Status** of the VPN connection change to a **green check mark** that denotes the VPN tunnel is active.

**Firewall Configuration**

To test the VPN connection, we must change the firewall settings. With vCloud Director 1.5, a 5-tuple firewall is enabled automatically to protect your routed external organization networks.

To verify the need to change the firewall settings, you can access a terminal session from the virtual machine in the vApp created in the QA environment. Before we modify the firewall, you can notice that we can ping the peer gateway (the VMware vShield Edge) of the VPN connection we just created, but we cannot ping the virtual machines in the development organization.
Access the Services screen for the Dev Ext Routed Network and select the Firewall tab. You’ll notice that the firewall is currently configured to allow only outgoing traffic. By clicking Add, we will add a new firewall rule to allow ICMP packets, enabling us to test the VPN functionality.

On this screen, you can select many different options for the firewall rule that you are about to create. Notice that you can use the firewall to filter traffic based on the source IP, the source port, the destination IP, the destination port and the protocol.

For our purposes here, configure the settings to allow ICMP packets from any host to any host on any port and click OK.
The new firewall rule is now in place.

Follow the same process to add a firewall rule on the QA Ext Routed Network, so we can ping from both directions.

Now you should be able to go to the virtual machine in either the development or QA organization and ping the system in the other organization through the established VPN tunnel.
If you perform a continuous ping and then disable the VPN functionality from one of the organizations, you can also verify that the traffic is going through the VPN tunnel. After the VPN functionality is disabled, you will notice that your pings fail to return.

**Blocking Tasks**

Blocking tasks enable the cloud administrator to pause tasks within vCloud Director so prerequisites can be completed. For example, an administrator can use this functionality to ensure that any media that has been uploaded to a catalog has been scanned for viruses before it is made available for others to use.

To demonstrate this ability, go to the **Administration** tab for vCloud Director. Select **Blocking Tasks** from the left-hand navigation pane and then click **Modify Media Name and Description** in the list of tasks available to block.
Notice under the Settings tab that you have several options, including sending notifications to an AMQP broker. Refer to the vCloud Director Administrator’s Guide for more information on configuring an AMQP broker. Although we are not going to modify any of the default settings in this guide, it is important that you know the options available to you.

Go to the Dev portal and select the properties for the media we uploaded to the catalog earlier.
Change the name as you want and click **OK**.

You will see that the status of the media has now changed to **Pending processing...**

Going back to the blocking tasks for vCloud Director, you'll see that the task is now listed as being blocked.
By right-clicking the blocked task, you can choose to allow the task to complete, abort it, or fail it. For the sake of illustration, select Fail.

Under Enter a reason for failing, type in a message that you want logged.
Back in the Dev portal, you'll see that the media status has changed again, to Ready. In addition, Cannot update is mentioned. Clicking the provided link will display more information.

Here you will see the reason you entered previously for why you failed the task.

By now, you should have a good feel for some of the security features included with vCloud Director. These include the ability to establish a VPN between organizations and other clouds and the ability to configure a firewall with VCD. You've also seen how you can use Blocking Tasks to provide notification or other actions on activities within your private cloud.
Conclusion

With VMware vCloud Director, you can:

• Increase business agility by empowering users to deploy preconfigured services or build a complete application stack with a few clicks.

• Maintain security and control over a multitenant environment with policy-based user controls and VMware vShield security technologies.

• Reduce expenditures by efficiently delivering resources to internal organizations as virtual datacenters, enabling decreased costs through increased resource pooling and automation.

• Follow an evolutionary path to the cloud by leveraging existing investments and open standards, for interoperability and application portability between clouds.

In this paper, we have shown how you can use VMware vCloud Director to transform your vSphere environment into a cloud environment. Refer to the VMware vCloud Director User’s Guide for more details.

To gain cost visibility into your VMware vCloud Director–based private cloud, download and evaluate VMware vCenter Chargeback™ 1.5. For details, refer to the VMware vCenter Chargeback Manager 1.5 Evaluation Guide.

VMware Contact Information

For additional information or to purchase VMware vCloud Director, the VMware global network of solutions providers is ready to assist. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5000 outside North America) or email sales@vmware.com. When emailing, include the state, country and company name from which you are inquiring. You can also visit http://www.vmware.com/vmwarestore/ to purchase VMware vCloud Director online.

Feedback

We appreciate your feedback on the material included in this guide. In particular, we would be grateful for any guidance on the following topics:

• How useful was the information in this guide?

• What other specific topics would you like to see covered?

• Overall, how would you rate this guide?

Please send your feedback to the following address: tmdocfeedback@vmware.com, with “VMware vCloud Director 1.5 Evaluation Guide” in the subject line. Thank you for your help in making this evaluation guide a valuable resource.