VMware vCloud® Director™ 5.1 Evaluation Guide

TECHNICAL WHITE PAPER
V 1.0 / UPDATED OCTOBER 2012

vmware®

Table of Contents

Getting Started

About This Guide

VMware vCloud® Director™ 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 5.1 Evaluation Guide* is designed to provide guided, hands-on evaluation of the most compelling and relevant features of vCloud Director. It walks through a series of procedures, each building upon the previous. When the evaluator has completed the process, they will have a working configuration that illustrates the key concepts that should be understood before deploying a production 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 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:
http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

White papers and other resources:
http://www.vmware.com/products/vsphere/mid-size-and-enterprise-business/resources.html

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, they looked to virtualize applications of low importance, such as those in a preproduction environment. As time passed, they took the next step in the virtualization journey by virtualizing more critical applications in their production environments. They soon realized significant reductions in personnel and hardware costs along with increased utilization of computing resources. 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: the deployment of a private cloud.

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

Simply stated, agility means being able to react more rapidly to business demands. This entails the ability to quickly respond to requirements for environments that routinely change, as well as to similarly enable environments that are commonly viewed as static. This is the main purpose of a private cloud–based infrastructure: to enable agility in the delivery of IT services.

Being virtualized does not equate to the benefits provided by a private cloud. Examining a large number of virtualized datacenters provides 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 VMware vSphere, such as VMware vSphere vMotion®, VMware vSphere High Availability (vSphere HA) and vSphere Distributed Resource Scheduler™ (vSphere DRS).
- The processes utilized to bring new applications and workloads online in a virtualized environment mimic the same processes used in physical environments.

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

An IT organization can see short-duration, high-demand workloads leak to external providers when its own supply of resources is unable to meet the demand of its users. Users that go "outside IT" do so to meet deadlines when they are unwilling or unable to wait out the IT provisioning process. 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—delivered within a secure environment and shielded from risk—to meet user demand. This is the premise of a private cloud: creating a way for companies to securely automate the matching of user demand with available supply. In doing so, companies can realize the benefits of IaaS, where end users can have resources allocated on demand in a self-service model.

An interesting by-product of enabling self-service is the change in end-user behavior in regard to the quantity of resources requested. 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 enabled to get what they need quickly and easily, end users are more likely to make more realistic resource requests and to return the resources when finished.

The transition to virtualization began with specific workloads. The evolution into the cloud also begins in this manner. To start, identify workloads that have a low management or governance need and that are required frequently. A good source for this type of workload is testing and development or preproduction environments.

For example, in a typical development environment, multiple developers often require similar environments for short periods of time. These environments can be hosted in a virtualized environment, though they tend to require refreshes as new product releases are made. This continual need to create environments for the developers and to manage them after they are 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 staff can save considerable time while also using this experience to hone its capabilities to deliver IT as a service (ITaas).

Although the first step in the journey to the cloud might involve low-governance workloads, they are not the ultimate goal. A private cloud solution can meet the needs of many applications and provides users with new ways of looking at how applications and services are provided and utilized.

As an example, consider a typical ERP system, which tends to have long development cycles with fairly minimal changes. A private cloud certainly will help in the development effort by provisioning resources on demand. Because this can be done so quickly, end users can also perform actions that previously were considered difficult. 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, with no trace of the new software.

The agility provided by a private cloud is not solely 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 any more.

The journey to the private cloud mimics the journey to virtualization in another critical way. As companies moved from virtualizing low-impact applications to doing so with more business-critical ones, the capabilities provided by virtualization were changing 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 likely 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 Suite

The VMware vCloud Suite is a combination of products designed to enable an IT organization to build and manage a private cloud based on a vSphere environment. The product suite consists of several components, including the following:

VMware vSphere is the industry-leading virtualization platform and enabler for cloud computing architectures. vSphere enables IT to meet SLAs for the most demanding business-critical applications, at the lowest TCO.

VMware vCloud Director 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 vCloud Networking and Security – Dynamic virtual and cloud infrastructure requires an integrated approach to networking and security. With this goal in mind, VMware offers these capabilities in a single solutioncalled VMware vCloud Networking and Security, which incorporates the capabilities of VMware vShield Edge™ and VMware vShield™ App with Data Security while offering many additional features and enhancements. These include VXLAN; a more flexible load balancer; performance, usability and high-availability enhancements to vShield Edge; and VMware vCloud Ecosystem Framework for third-party integration.

In an effort to ease customer transition from vShield Edge 5.0 to vCloud Networking and Security 5.1 and ensure continuity, the user interface and documentation for vCloud Networking and Security still reference existing vShield product names when discussing capabilities.

VMware vCenter™ Chargeback Manager™ 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.

VMware vCloud Connector™ enables customers to migrate vSphere workloads to private and public clouds. Its comprehensive user interface enables a single view across multiple cloud environments.

VMware vCenter Site Recovery Manager™ Server (SRM Server) enterprise provides for automated disaster recovery planning, testing and execution.

VMware vCenter Infrastructure Navigator™ enables application discovery, dependency mapping and management.

VMware vFabric™ Application Director™ provides a multitier application service catalog publishing and publishing system.

VMware vCenter Operations Enterprise™ enables administrators to monitor the performance of their environment, alerting them to potential issues before they become critical. This is an invaluable tool for capacity planning and optimization of a cloud environment.

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.

The VMware solution ensures flexibility and interoperability for the cloud. Asan enterprise moves to a cloud-based infrastructure, customers can amplify the benefits of virtualization and move selected workloads within their datacenter cloud or to one of the many vCloud-enabled public clouds in the VMware partner ecosystem.

This suite also helps an organization achieve a cloud model that is uniquely theirs—a private, public or hybrid environment precisely aligned with their 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 basic vCloud Director deployment consists of a number of components. These include the following:

vCloud Director

A single instance of vCloud Director is known as a "cell." A cell consists of thevCloud Director components installed on a supported operating system (OS). 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 Database and Microsoft SQL Server for database platforms. In most environments, 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.

VMware 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.

vSphere Hosts

VMware vSphere ESXi™ hosts provide the compute power for vCloud Director. vSphere 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.

vCloud Networking and Security Manager

vCloud Networking and Security 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, vCloud Networking and Security 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 vCloud Networking and Security Edge Gateway in a vCloud Director environment, an instance of vCloud Networking and Security 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.

vCloud Director takes this abstraction to a new level and creates 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 VDCs, corporate IT has the option to offer multiple service-level alternatives 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 of 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 following are the main logical components:

Provider Virtual Datacenter

A provider VDC is a logical grouping of compute and storage resources. The provider VDC groups together a set of vSphere hosts and a set of one or more associated datastores. This logical grouping is then made available for consumption by organizations. Provider VDCs can leverage the Storage Profiles feature of vSphere to provide multiple classes of storage to differing 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 vCloud Director 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 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.

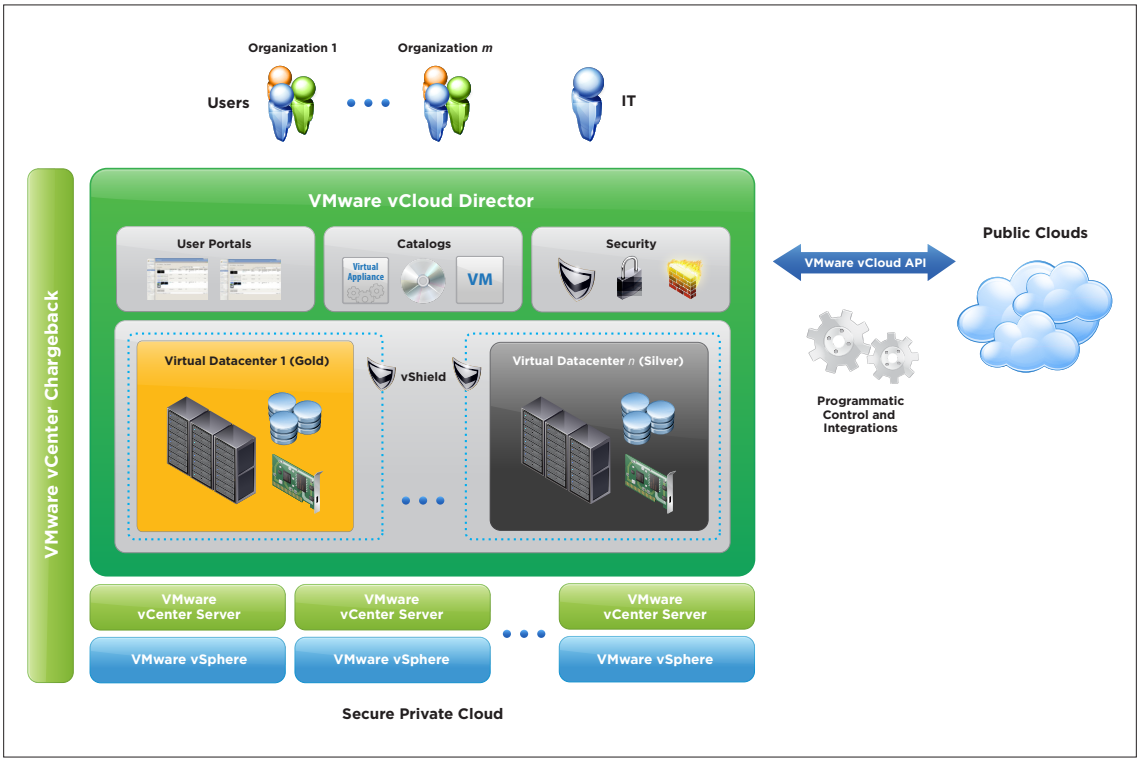
vApps

A VMware vSphere 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 one to be easily redeployed multiple times by an organization's users. These vApp templates can be shared among users in the organization or between organizations.

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

Catalogs

Organizations use catalogs to store vApp templates and media files. The members of an organization that 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 its users.



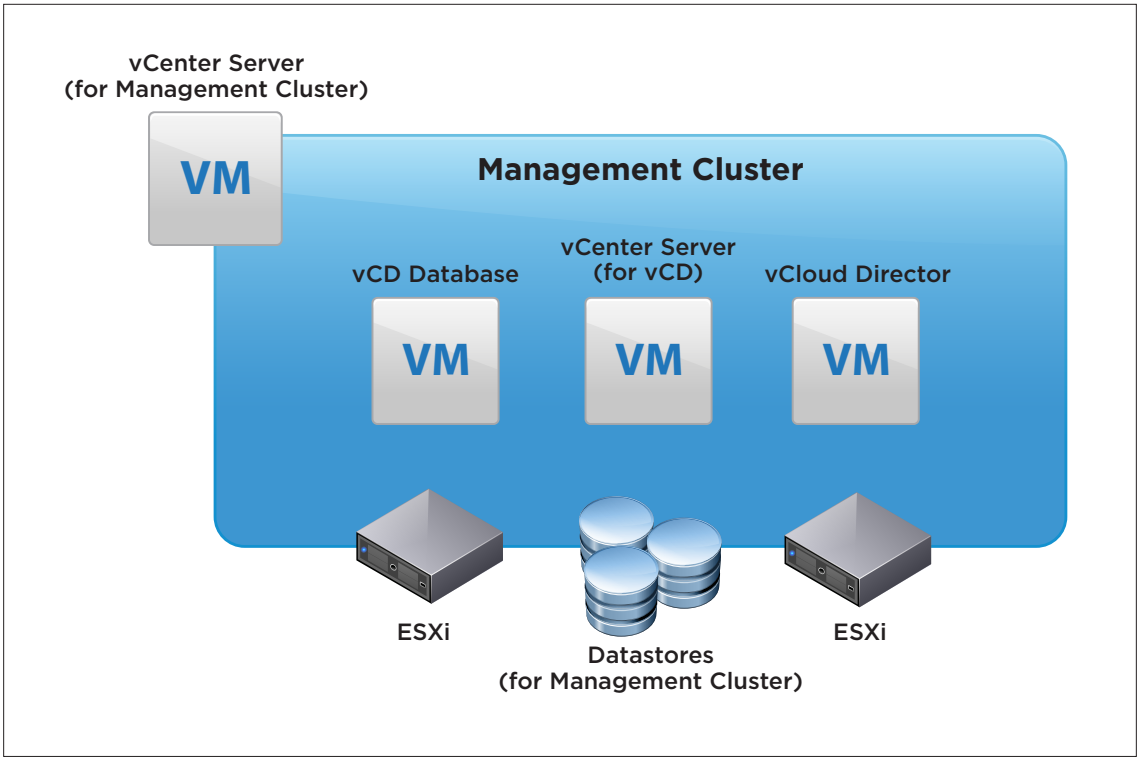
Typical vCloud Director Deployment

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 vSphere hosts, enabling high availability and downtime avoidance. Running within the management cluster are virtual machines hosting vCloud Director, the vCloud Director database, vCloud Networking and Security Manager and one or more vCenter Server instances that are attached to vCloud Director and manage a number of vSphere hosts. Often there also is a single vCenter Server instance inside the management cluster, configured to manage the management cluster.

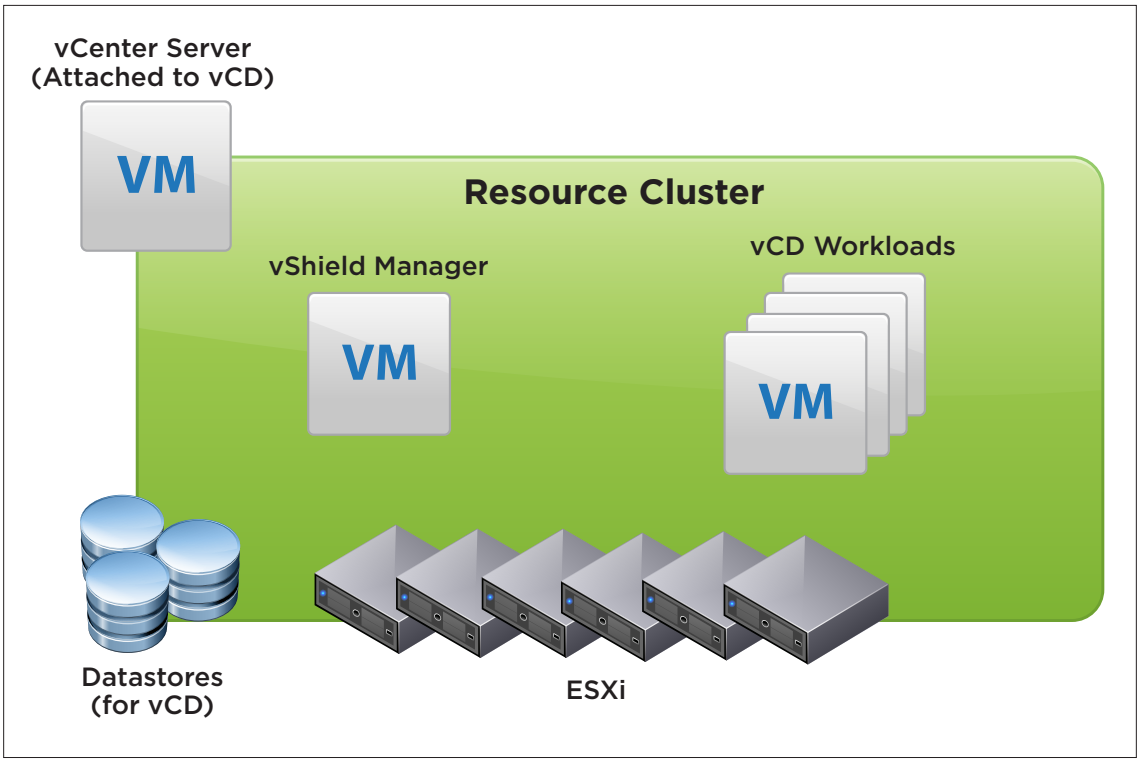
In the following diagram, a simple management cluster with two ESXi hosts is shown. Within this management cluster, virtual machines are configured for vCloud Director, vCloud Director database and two vCenter Server instances. One of the vCenter Server instances provides services for the management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



Resource Cluster

A vCenter Server instance that is attached to a vCloud Director instance manages one or more vSphere hosts. These vSphere hosts provide compute and storage resources that are configured in one or more clusters. These clusters must be configured to use automated vSphere DRS.

The collection of vCenter Server instances that are attached to vCloud Director and the resources (compute and storage) is referred to as a *resource cluster*. It is here that the workloads provisioned from vCloud Director 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 a user might differ from the one in this guide, it is important that all customers understand how the lab used here was constructed and why procedures were done in this way.

Architecture Overview

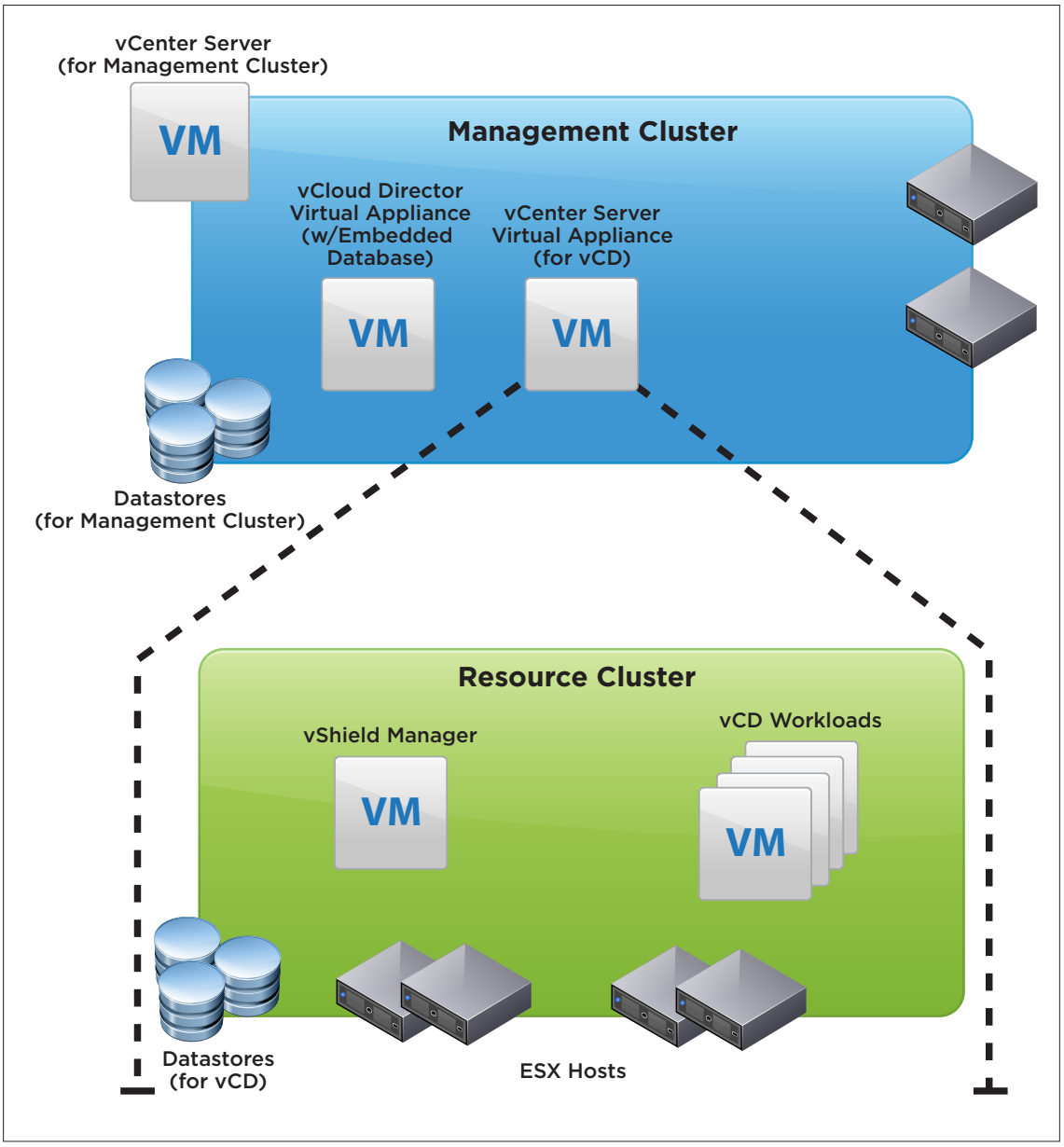
Logically, the environment used for this evaluation guide is split into two parts.

The first logical part is the management cluster, which provides hosting for the vCloud Director infrastructure components. These include the vCloud Director instance, vCloud Director database, vCloud Networking and Security Manager, and vCenter Server instance under 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, because all of the components have been virtualized.

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

To simplify the evaluation process further, this guide leverages the benefits provided by the virtual appliances for both vCenter Server and vCloud Director. Use of these appliances eliminates the need to configure additional databases, because each of the appliances provides an embedded database.

The second logical part of this evaluation environment is the resource cluster. It comprises a set of vSphere hosts that actually host the workloads for vCloud Director. In this evaluation environment, four additional vSphere hosts are used for this purpose. These vSphere hosts are managed by the vCenter Server instance located in the management cluster that is to be attached to the vCloud Director instance.



Compute Hardware Requirements

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

The resource cluster requires four physical hosts of sufficient power to host two standard Linux virtual machines at a minimum.

Network Requirements

One physical network is utilized in this guide. This network must have connectivity to external systems used for testing as well as software download.

The external network must have a pool of IP addresses able to be used for connectivity. It also must have a Dynamic Host Configuration Protocol (DHCP) server located on it that is able to provide DHCP services as needed. In addition, it must support multicast packets.

Four IP addresses are required for each of the main virtual machine components, in addition to the addresses used by the physical hosts themselves. Each address must be resolvable through DNS by a Fully Qualified Domain Name (FQDN). The following table lists the relevant information used for this guide.

FQDN	ROLE	NOTES
vc-l-01a.corp.local	vCenter Server to be attached to vCloud Director	One IP address is required.
vcd-01a.corp.local	vCloud Director	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.
vsm-01a.corp.local	vCloud Networking and Security Manager	One IP address is required.

Storage Requirements

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

To complete the procedures presented in this guide, users must have a minimum of 100GB of storage in a shared datastore accessible by the hosts in the resource cluster. If they want to deploy a highly available management cluster, they also must have shared storage accessible by the hosts in the management cluster.

vCloud Director requires that vSphere DRS be enabled in fully automated mode. This requires that shared storage be attached to all of the hosts, so users must ensure that the storage they employ is visible from all of the hosts in the resource cluster.

Software and Licensing Requirements

Users must have licenses for vCloud Director installation. vCenter Server and vSphere hosts can be run using an evaluation license for a period of time. This enables users to experiment with all the features of the product before deciding on a perpetual license.

Users must have access to the binaries for vCloud Networking and Security Manager, vCenter Server and vCloud Director Appliance. They also must have a copy of a CentOS 6.3 LiveCD .iso image to use for testing.

Software Configuration

It is expected that users have already configured the following management and resource cluster components before beginning the procedures listed in this guide:

Management cluster – A vSphere environment has been created that is managed by an instance of vCenter Server that contains at least one vSphere 5.1 host.

Resource cluster – Four vSphere 5.1 hosts have been installed.

In both cases, it is assumed that the appropriate storage and network connectivity is configured.

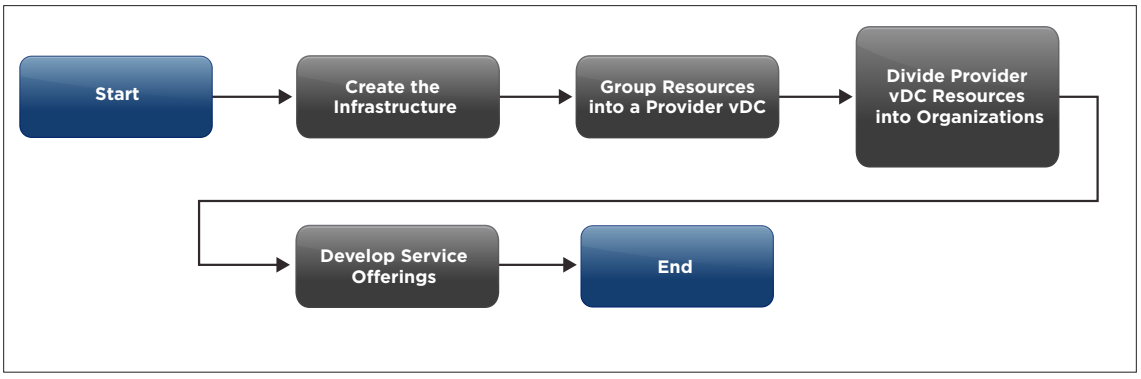
Because vCloud Director fully leverages secure communications between the various components, it is important that the time on all the systems, including the vCloud Director database, is synchronized to a common time source. Configure each virtual machine to use Network Time Protocol (NTP) to maintain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

Security Considerations

The various software components that this guide uses have predefined usernames and passwords. As a best practice, these passwords should be changed from the default settings as soon as possible to enable the most secure environment.

Evaluation Procedures

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



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

This guide also was designed to enable evaluating vCloud Director with limited resources. Accordingly, some of the procedures do not conform to best practices to 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.

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, vCloud Networking and Security Manager, and the vCenter Server instance that will be attached to vCloud Director.

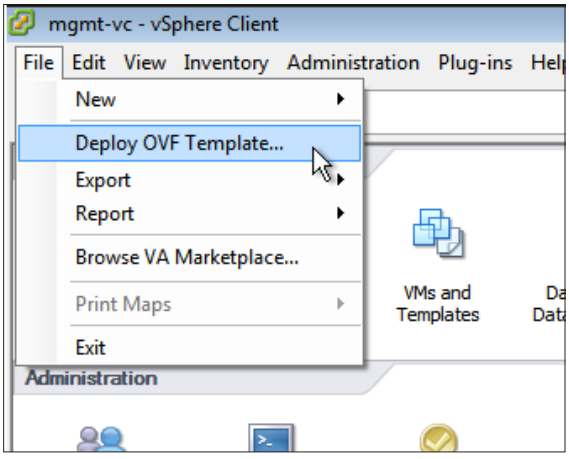
In this guide, the vCloud Director and vCenter Server appliances are used. This enables you to quickly get an environment for evaluation purposes up and running.

The vCloud Director Appliance uses SUSE Linux Enterprise Server for VMware, based upon SUSE Linux Enterprise Server 11 Service Pack 2. Although thevCloud Director Appliance supports the use of an external Microsoft SQL Serveror Oracle Database as the vCloud Director database, it also includes an internal Oracle Database Express Edition 11*g* Release 2 (Oracle Database XE) that can be used. This guide leverages the benefits of the internal database. You can obtain more information about the supported external databases by accessing theVMware Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?

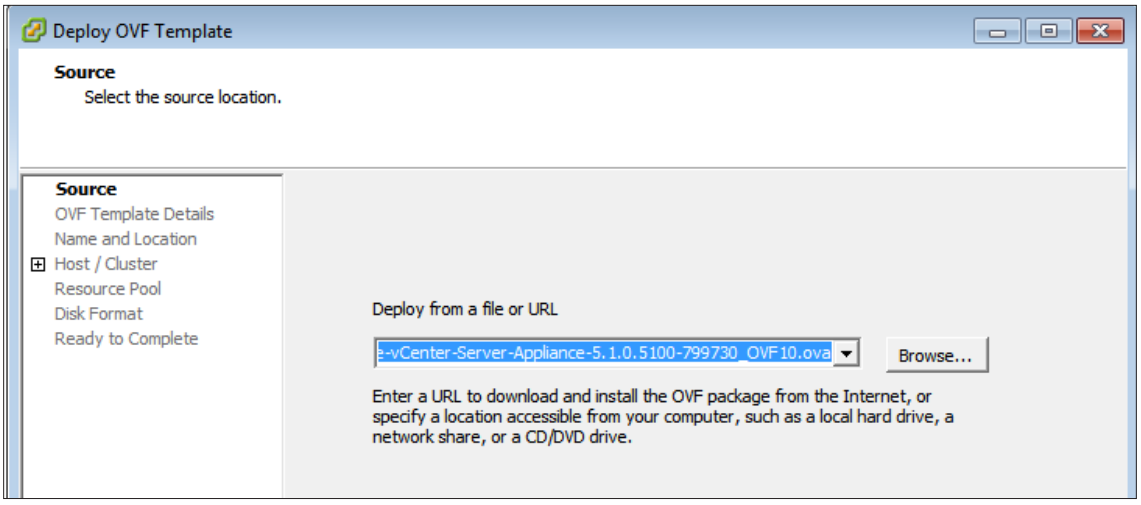
Installing the vCenter Server Appliance

The first step in building an environment to evaluate vCloud Director is to install the vCenter Server instance that will be associated with vCloud Director. This vCenter Server instance and the resources it maintains will become the foundation of resources used within vCloud Director.

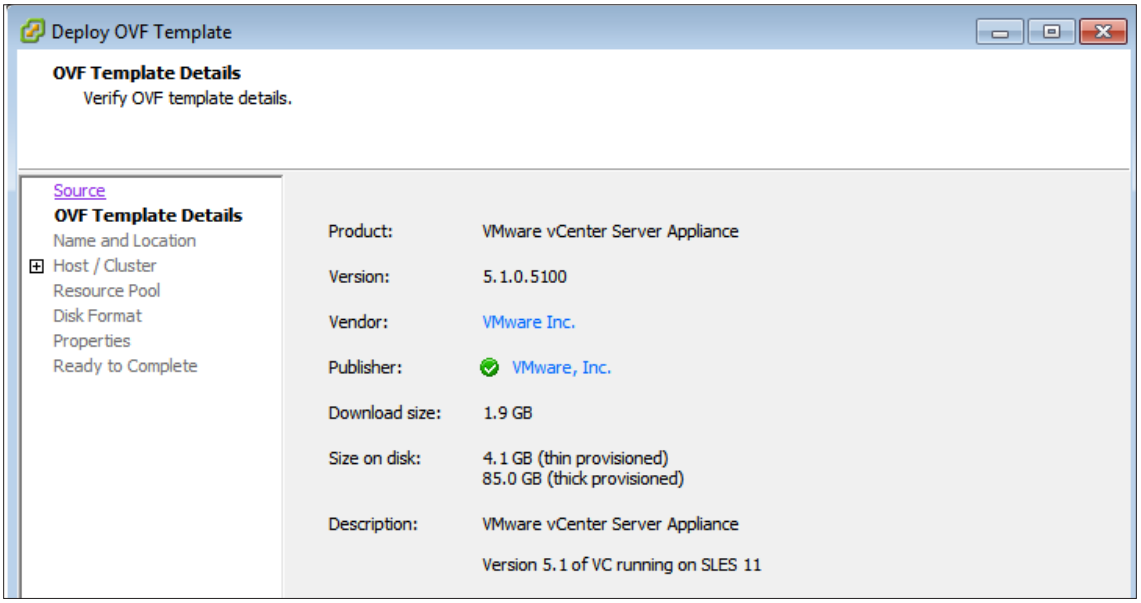
In this guide, we utilize the VMware vCenter Server Appliance™ for this purpose. Using the vCenter Server Appliance eliminates the complexity of deploying a complete solution. It will be deployed as a virtual machine that resides within the management cluster configured.



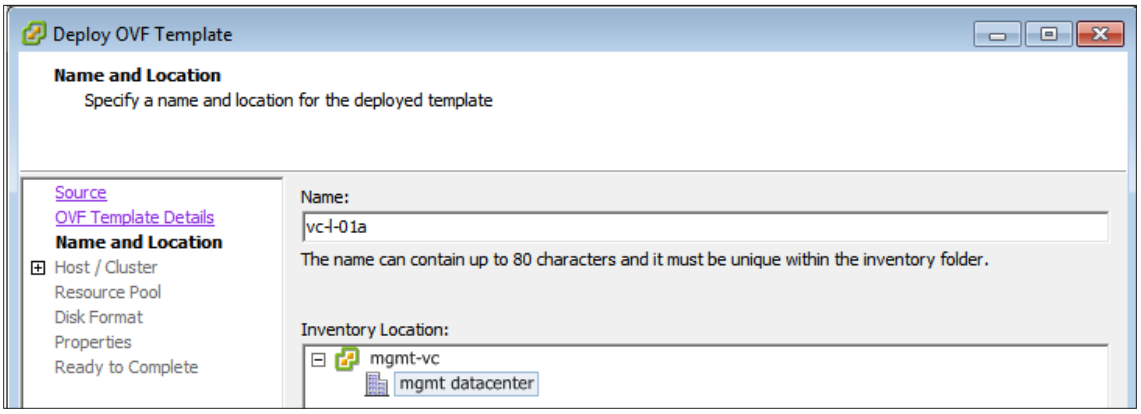
To begin, utilize the VMware vSphere Client™ connected to the vCenter Server instance for the management cluster and select the **Deploy OVF Template** option.



You will be prompted for the file to deploy. Select the **vCenter Server Appliance.ova** file and click **Next** to continue.

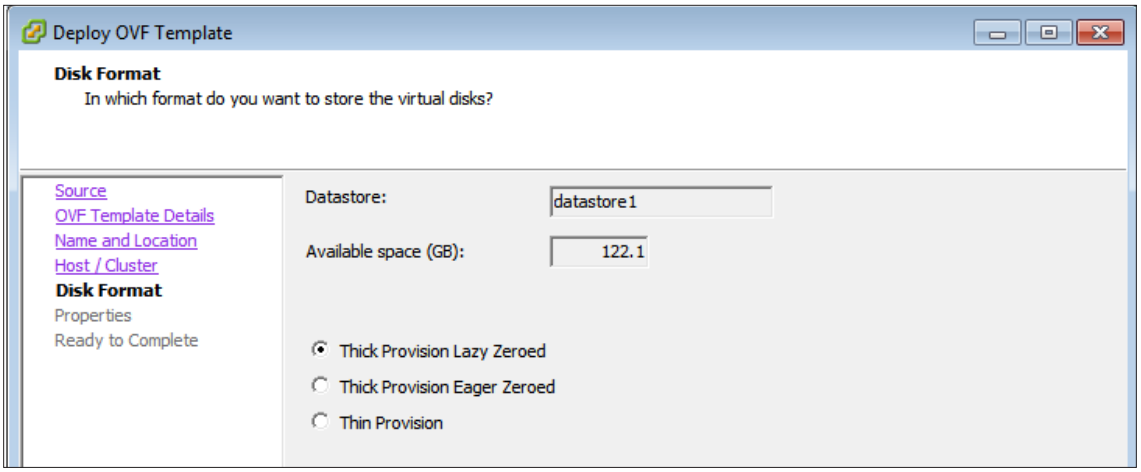


The next screen gives you some information about the virtual machine template you are about to deploy for the vCenter Server Appliance. Click **Next** to continue.

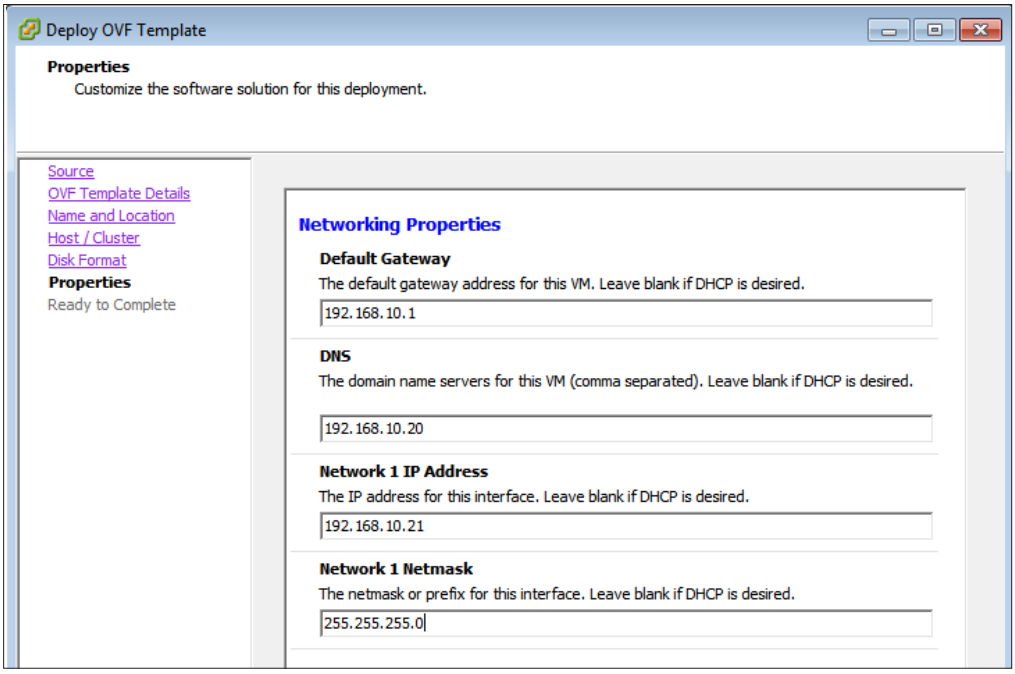


The OVF deployment wizard then prompts you for the name of the vCenter Server Appliance to be deployed. In this guide, we name it **vc-l-01a**.

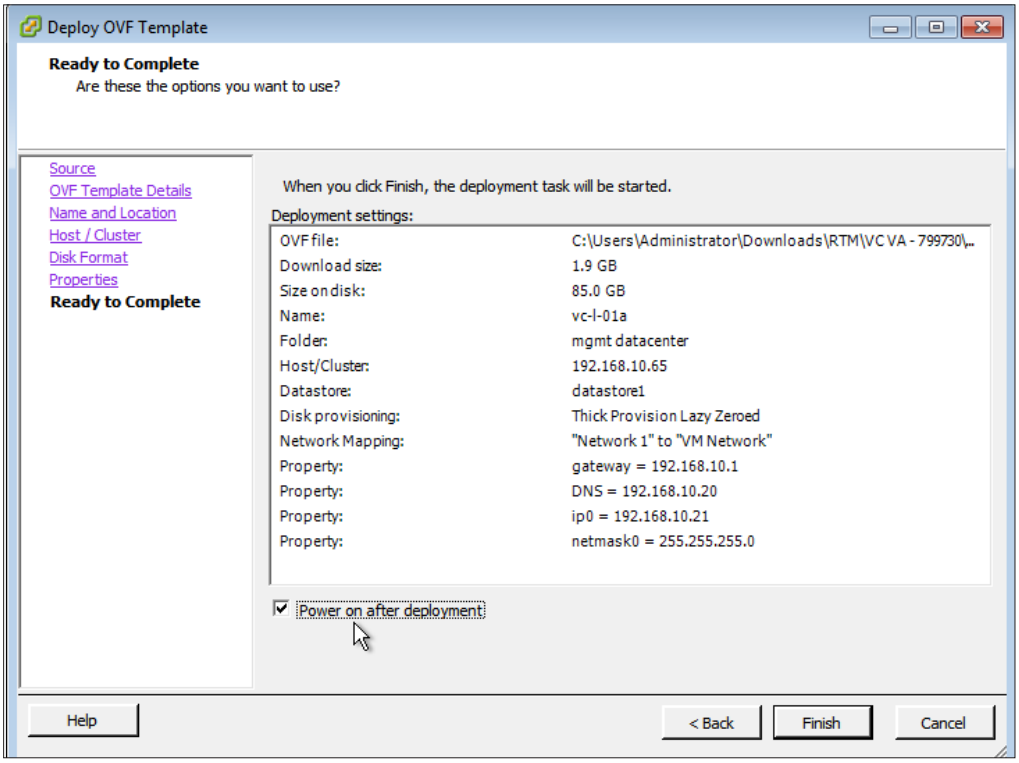
Click **Next** to continue. You will be asked to select the host or cluster within the management cluster to deploy the appliance to. Select the appropriate option and click **Next** to continue.



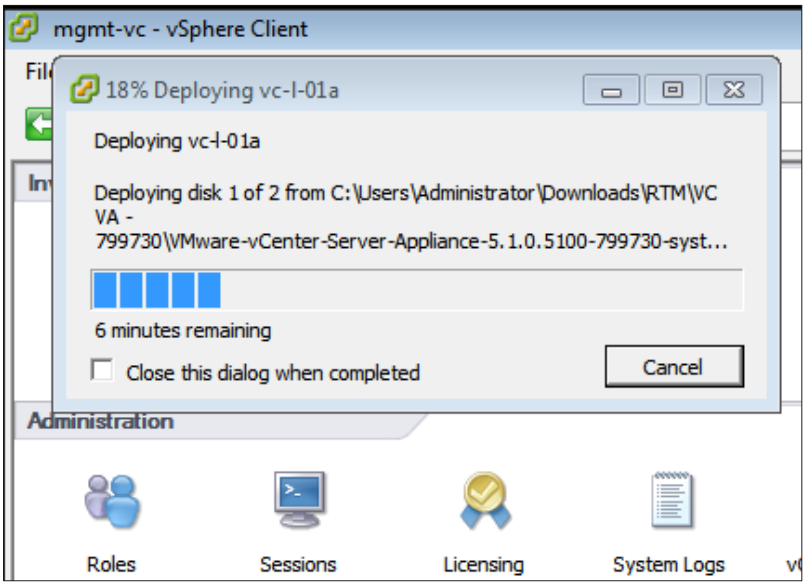
Next, define the datastore in the management where the deployed appliance will reside and select a provisioning method. Click **Next** to continue.



Next, define the network configuration for the appliance. These values must match the network configuration that is present in your environment. The preceding example represents what is used in this guide.



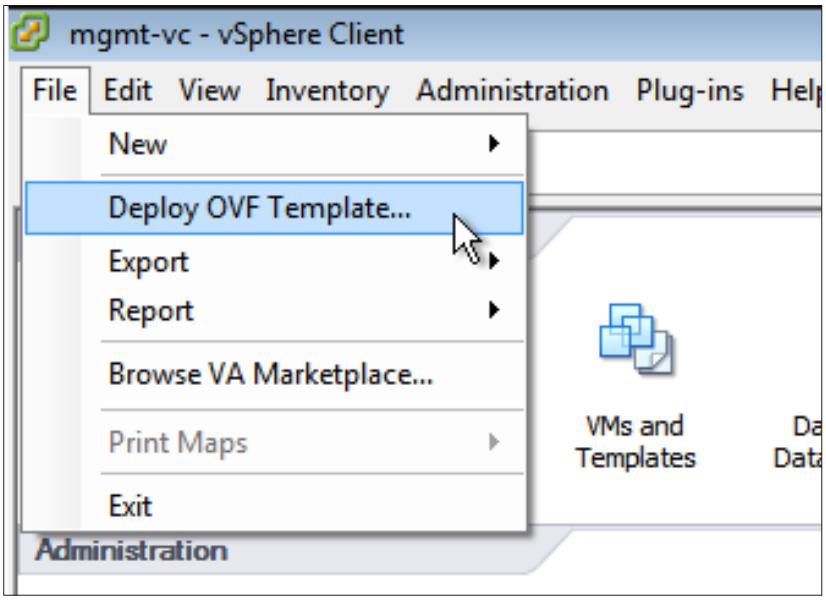
On the summary page, review the information to ensure that it is correct. Select the **Power on after deployment** check box to power on the appliance after the deployment has completed. Click **Finish** to start the deployment.



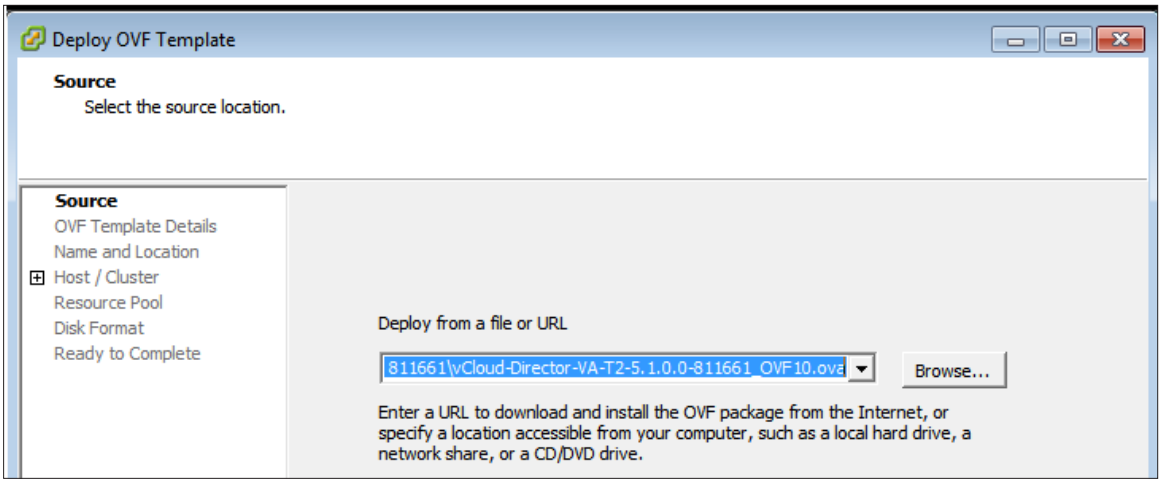
A window will be displayed that shows the progress of the appliance deployment. Wait until this is complete before continuing.

Installing the vCloud Director Appliance

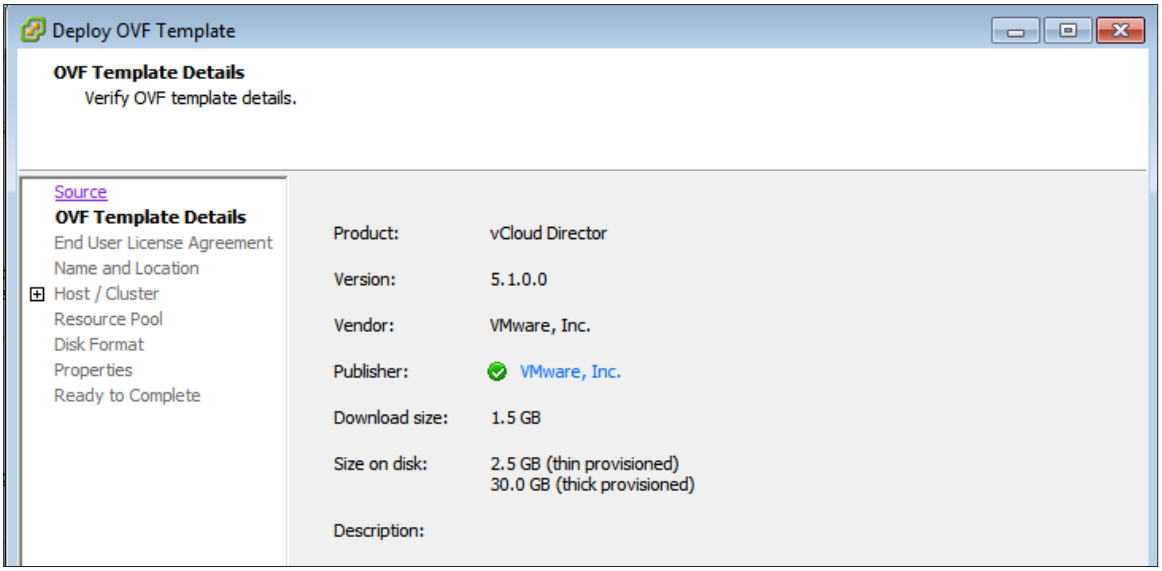
In this guide, we use the vCloud Director Appliance. As with the vCenter Server Appliance, using the vCloud Director Appliance reduces the complexity that would be involved with a production deployment. The vCloud Director Appliance is not supported for production environments. For the PoC environments that the vCloud Director Appliance is targeted at, it's expected to be used on a limited infrastructure scale. As a result, the vCloud Director Appliance has been verified in single-cell deployments with two attached vCenter Servers and 100 virtual machines. This will be more than adequate for the purposes of this guide.



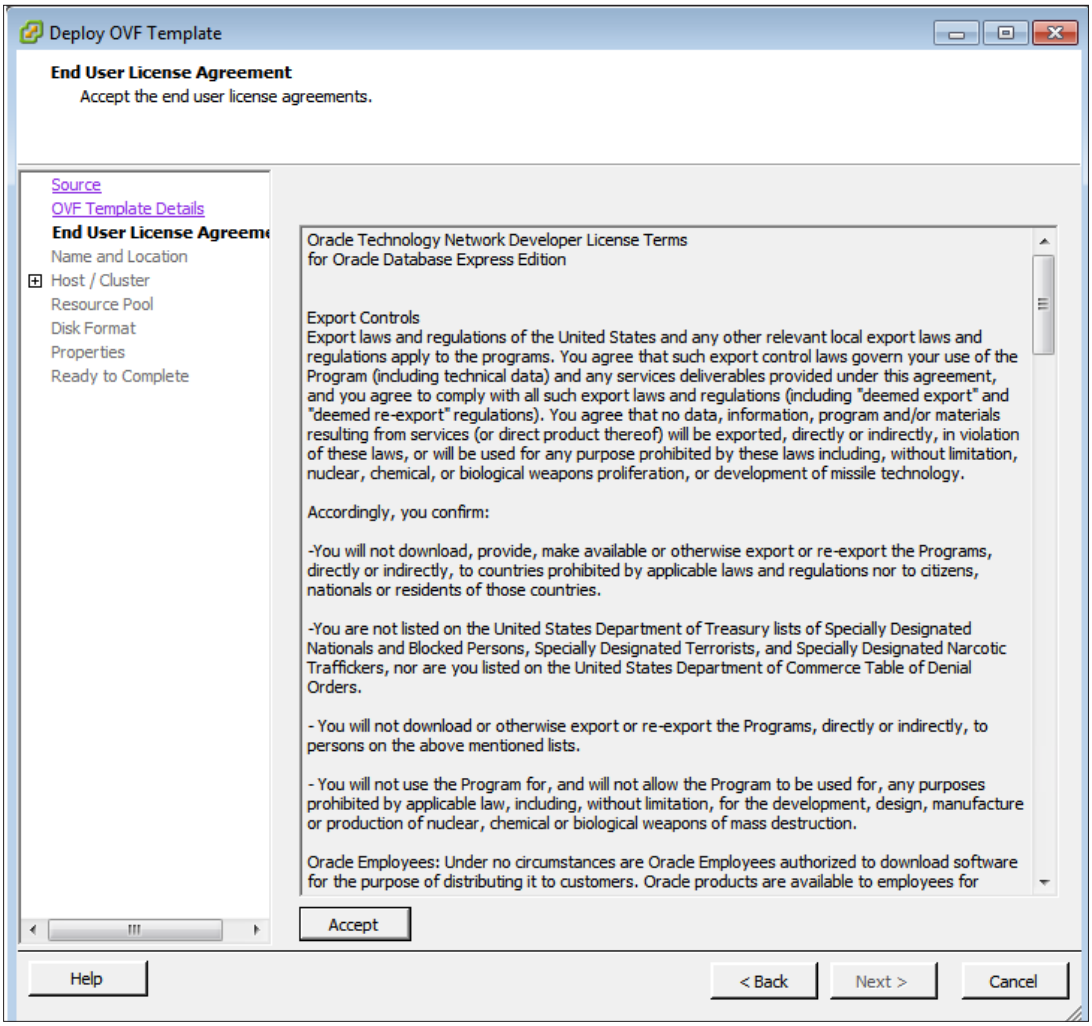
As with the vCenter Server Appliance, deploying the vCloud Director Appliance starts with selecting the **Deploy OVF Template**... from the vSphere Client connected to the management vCenter Server.



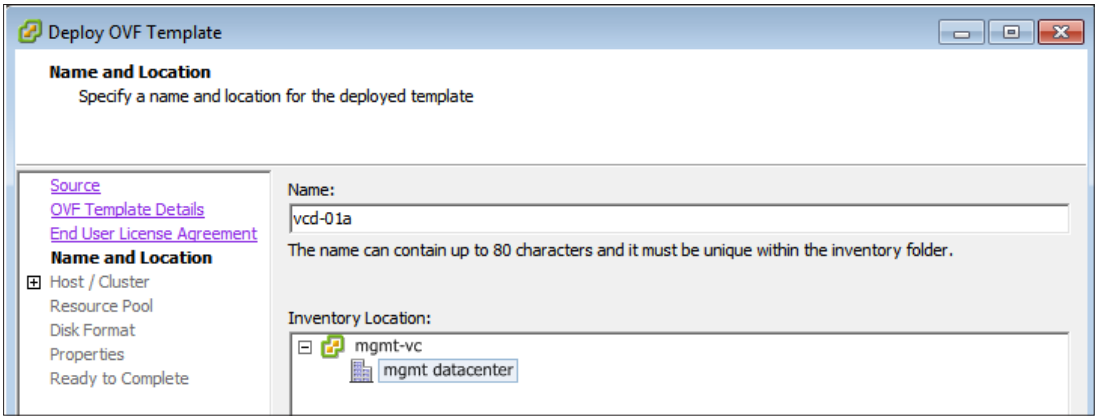
After specifying the location for the vCloud Director Appliance file, click **Next** to continue.



A summary of the appliance is displayed. Click **Next** to continue.

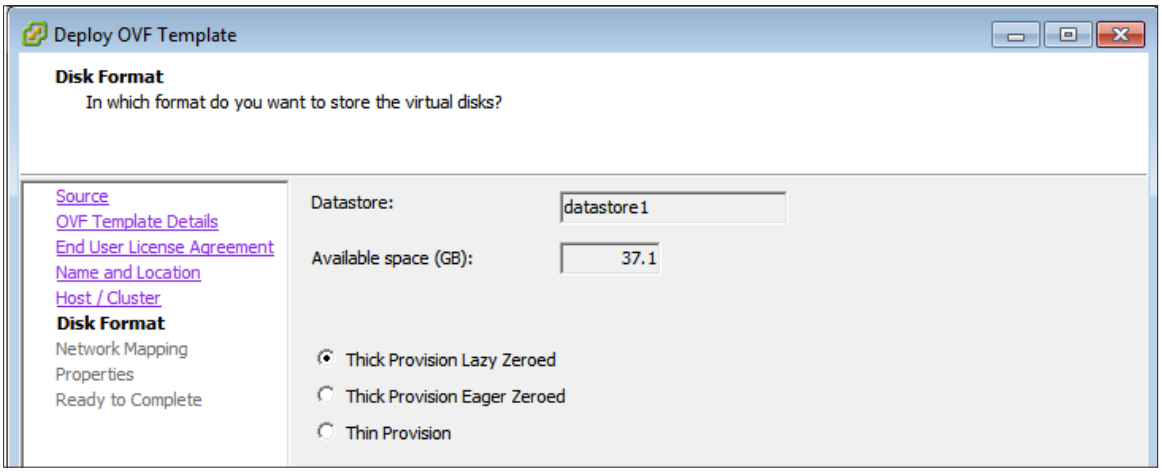


You then are presented with an End User License Agreement (EULA) that you must accept before continuing. This EULA is specific to the embedded Oracle Database XE that is packaged with the vCloud Director Appliance. After clicking the **Accept** button, click **Next** to continue.

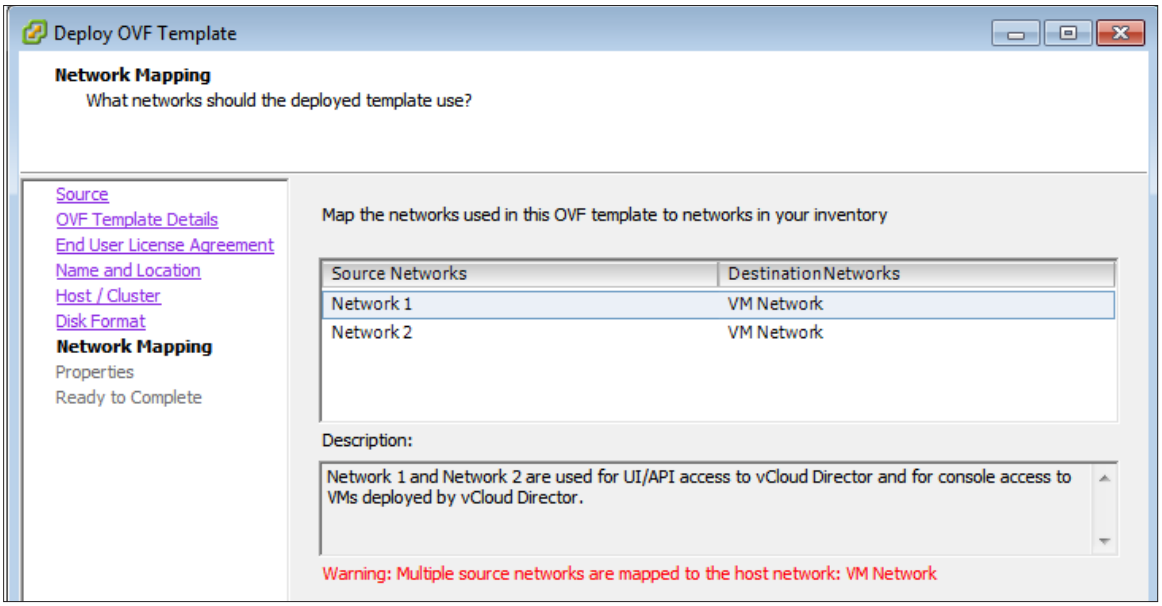


The next step is to name the vCloud Director Appliance. In this guide, we use the name vcd-01a. Choose a name and location to place the vCloud Director Appliance. Click **Next** to continue.

The next screen prompts you to define the host and/or cluster to deploy the appliance to within the management cluster. Select the appropriate value and click **Next** to continue.



The next step is to define the format that you want to use to store the virtual disks of the appliance. Select an option and click **Next** to continue.

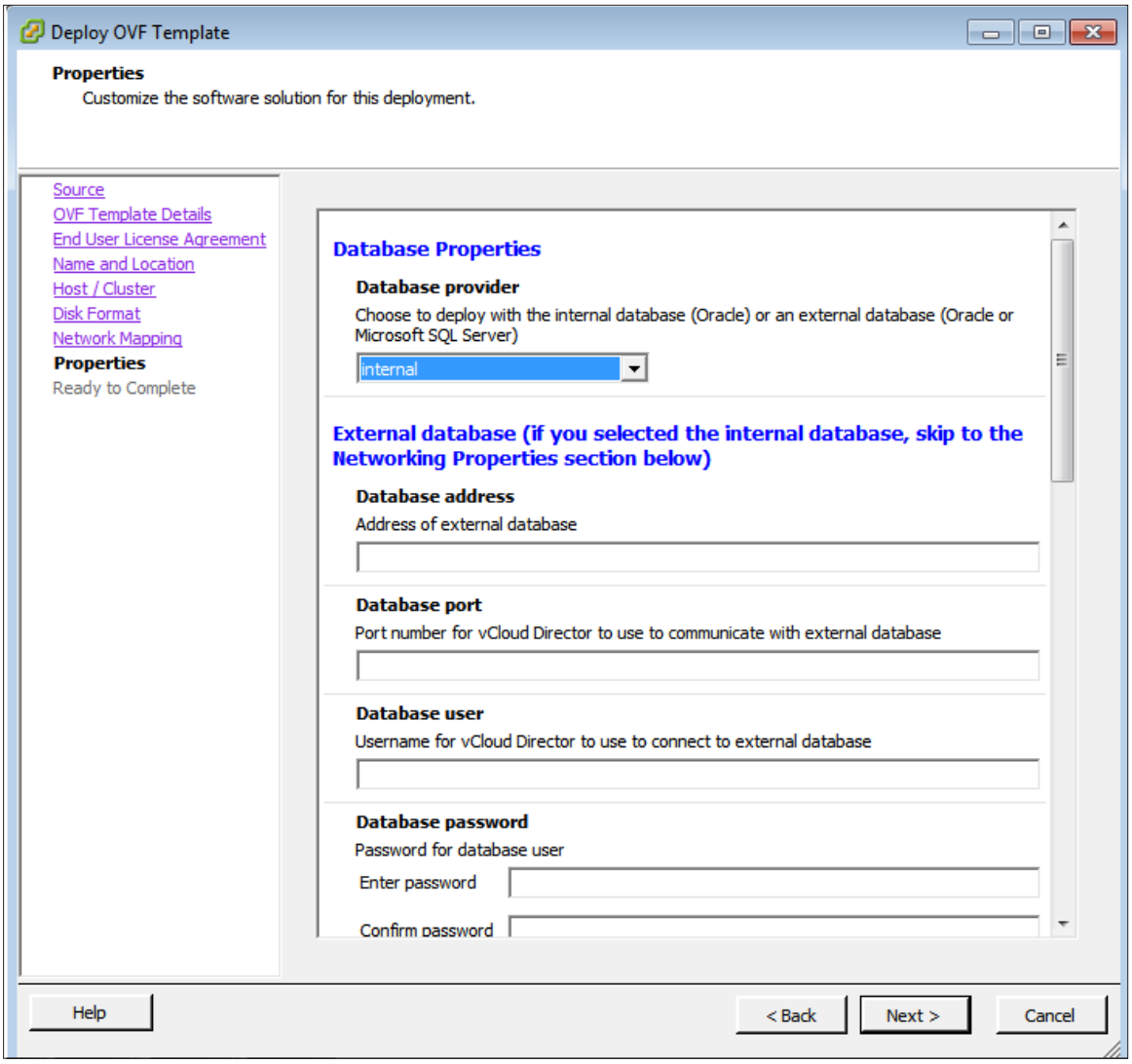


Next, define the network mapping. Each vCloud Director installation requires two IP addresses. One is used for HTTP traffic and to connect to the vCloud Director user interface. The other is for the console proxy connection that is used for all VMware Remote Console (VMRC) connections and traffic.

In a production environment, these IP addresses are configured in different networks. This enables the user to separate the public-facing network that uses the HTTP IP address from the private network that uses the console proxy IP address.

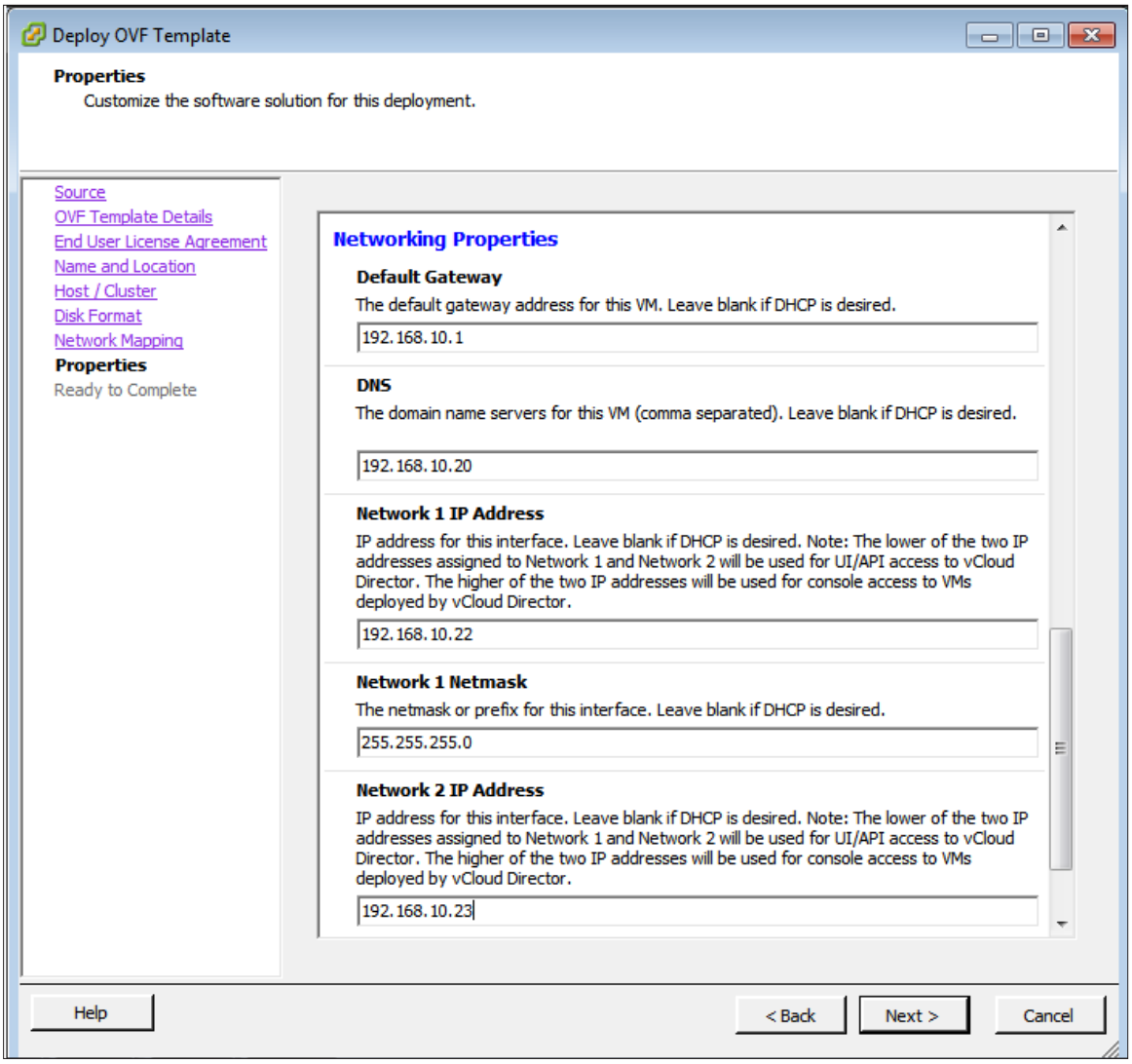
Using this screen, you can map the two network interfaces of the vCloud Director Appliance to specific networks defined in your management cluster. In the preceding example, both of the vCloud Director network interfaces are mapped to the same network on the management cluster. Because this is not a best practice for a production environment, a warning is generated.

Click **Next** to continue.



On the properties page, you can specify attributes for a vCloud Director Appliance deployment. It is divided into sections denoted by blue headers. The first section for **Database Properties** enables you to choose what type of database vCloud Director will use. You can specify an internal or external database. If you select an external database, you can continue to the next section and define the properties for the Microsoft SQL Server or Oracle Database to be used. By selecting the internal database, you utilize Oracle Database XE, which comes bundled with the vCloud Director Appliance.

This guide uses the internal database option. For this reason, you can skip the section for the external database properties. Use the scroll bar to scroll to the **Networking Properties** section.

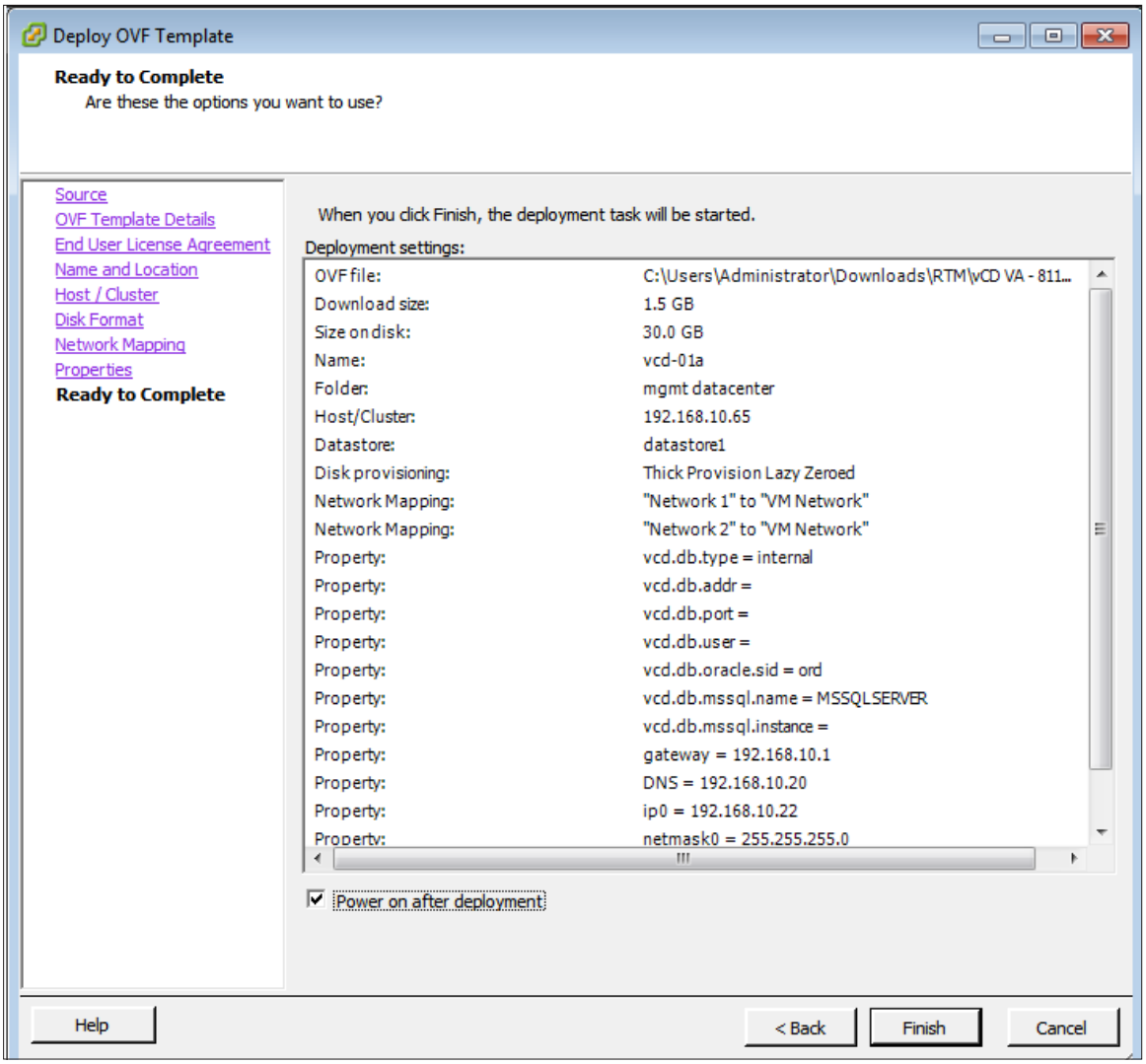


In the **Networking Properties** section, you define the values to configure the networking services on the vCloud Director Appliance. These include the default gateway addresses, DNS servers and IP addresses used with the associated netmasks.

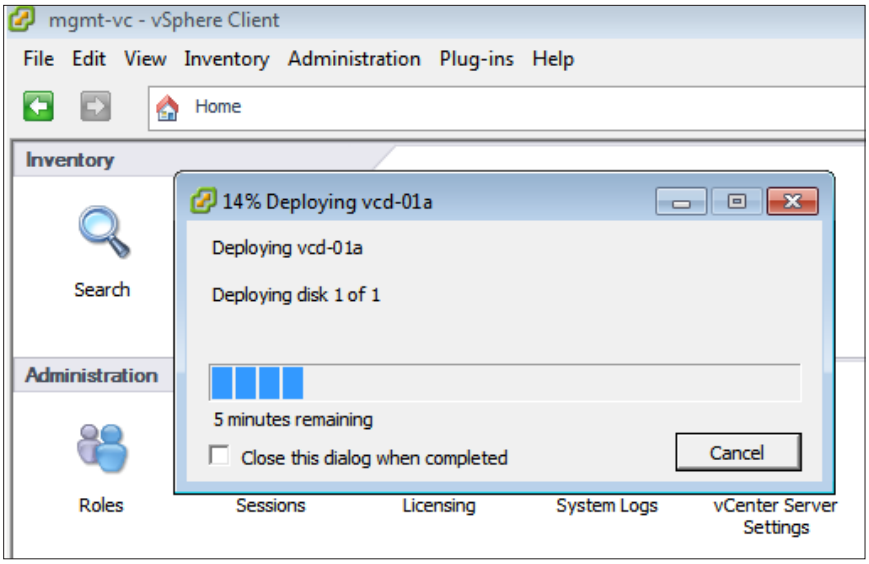
There are two IP addresses that must be defined, as previously mentioned. These are specified as **Network 1 IP Address** and **Network 2 IP Address**.

NOTE: The vCloud Director Appliance automatically chooses the lower of the two IP addresses to use for HTTP traffic. In other words, the lower of the two IP addresses is the IP address that you use to access the vCloud Director Web interface.

Provide the values for the **Networking Properties** section and then click **Next** to continue.



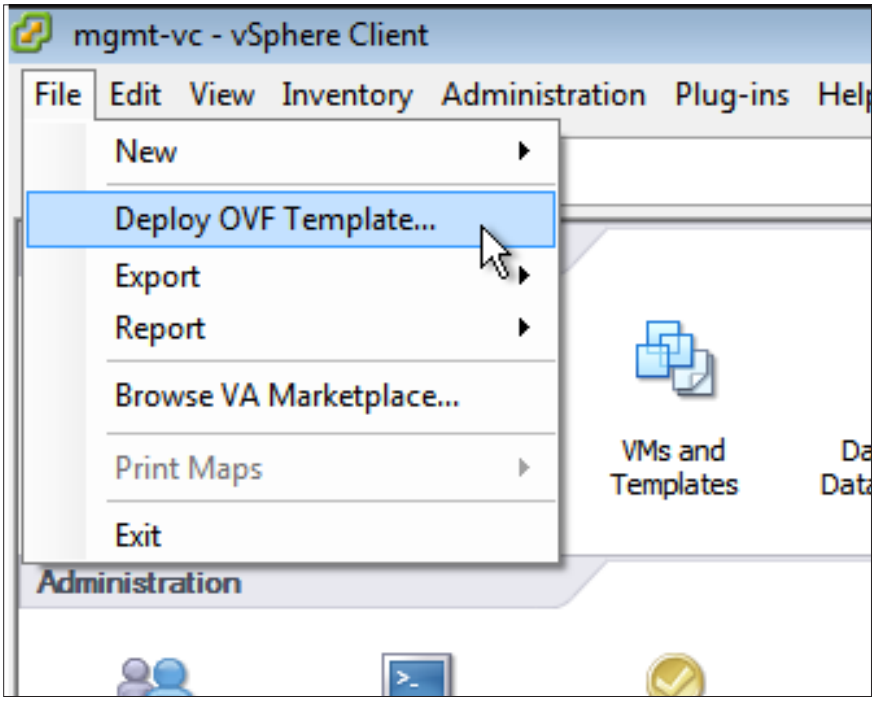
At this point, you are presented with a summary screen to review the information that you provided. Verify that the information is correct and select the **Power on after deployment** option. Click **Finish** to start the deployment.



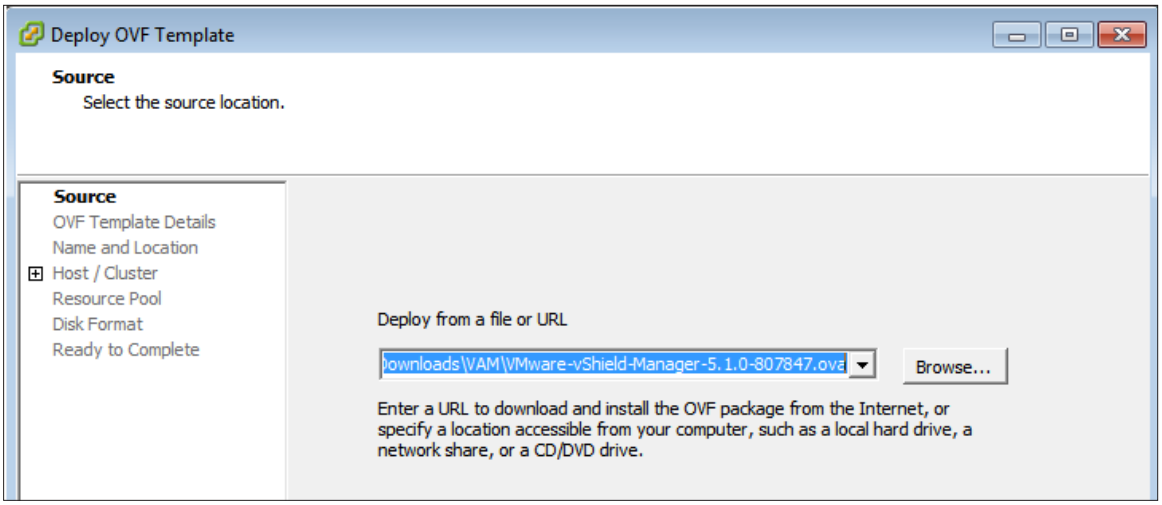
Observe the status provided and wait for the deployment to finish.

Installing the vCloud Networking and Security Manager

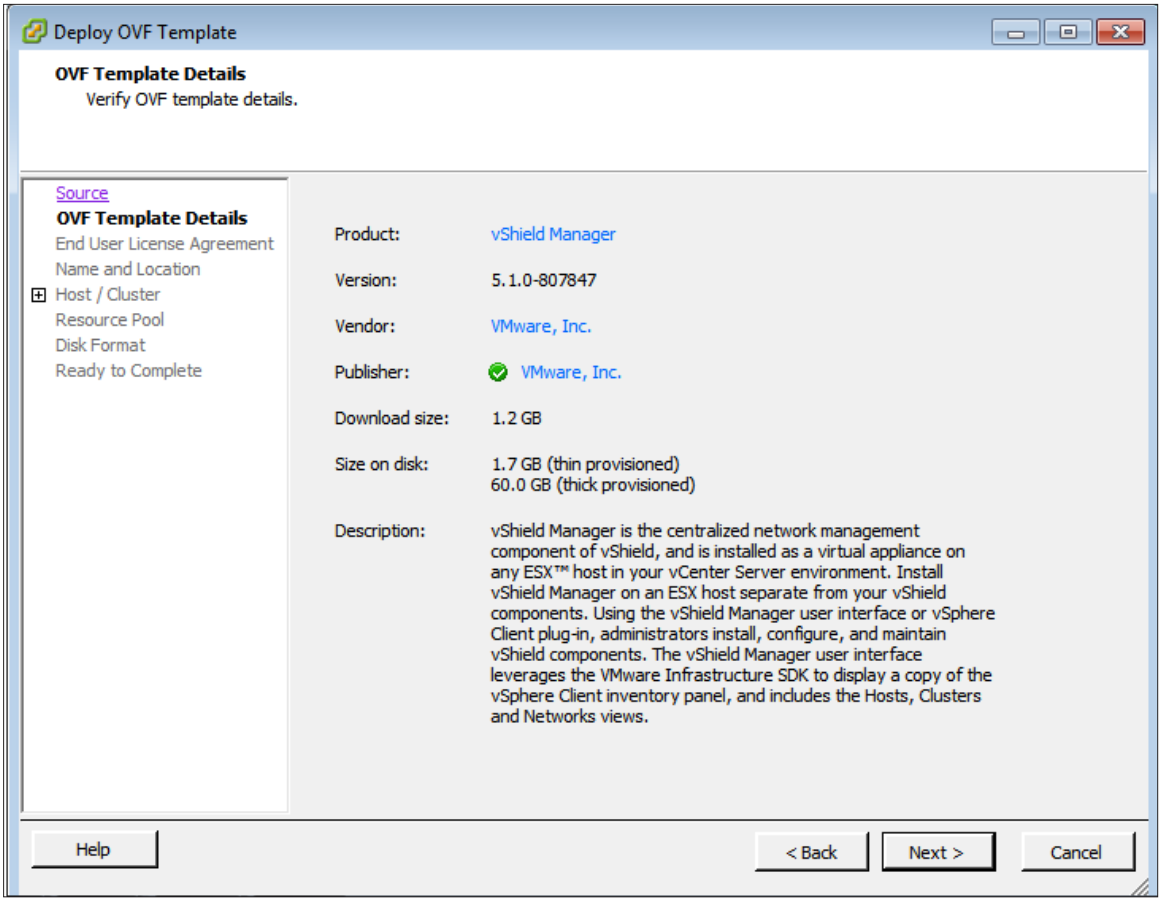
vCloud Networking and Security Manager provides network services to vCloud Director and to vCenter Server. A unique instance must be installed for each vCenter Server instance used by vCloud Director.



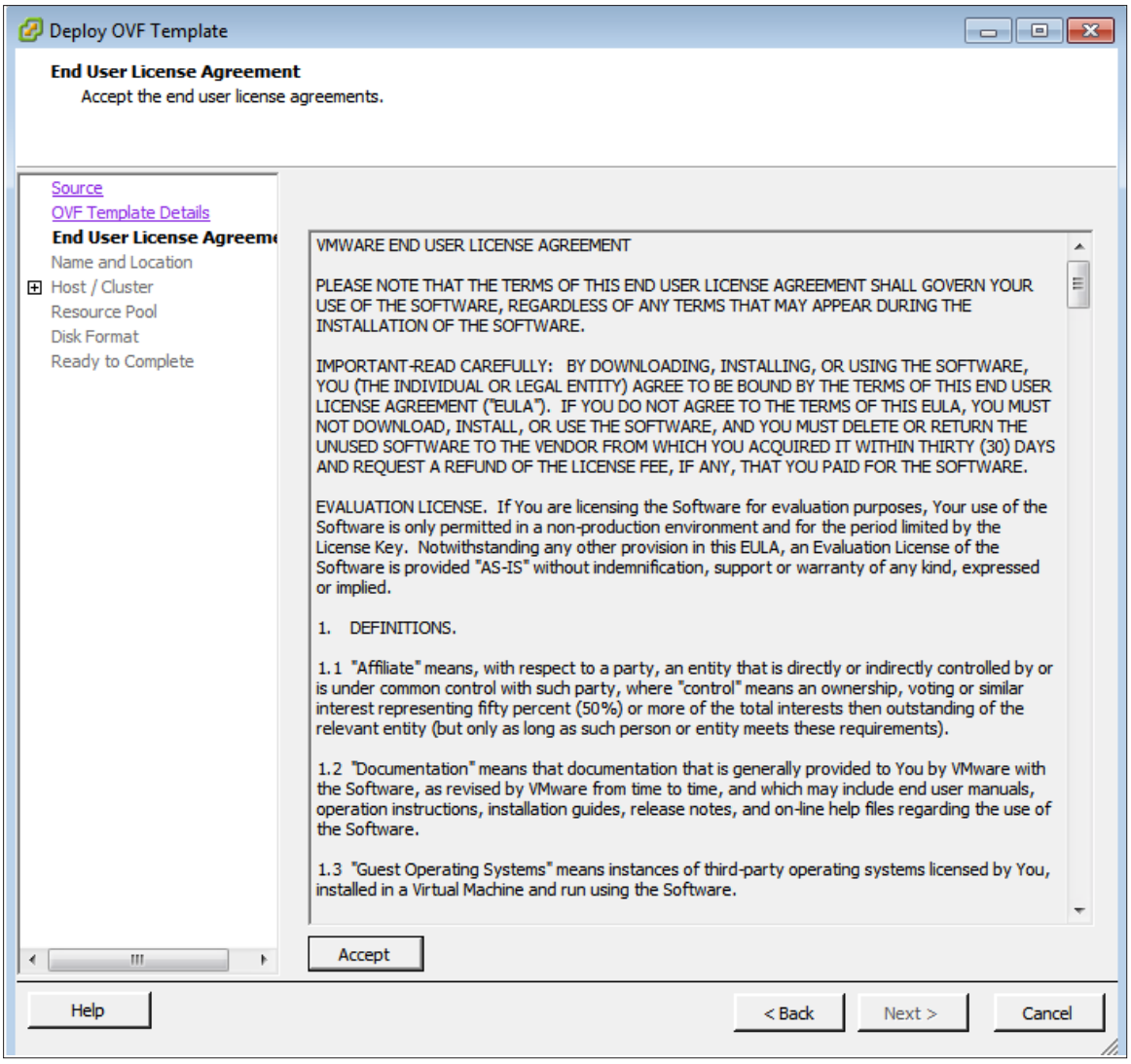
Deploy the vCloud Networking and Security Manager by selecting the **Deploy OVF Template...** option from a vSphere Client connected to the vCenter Server managing the management cluster.



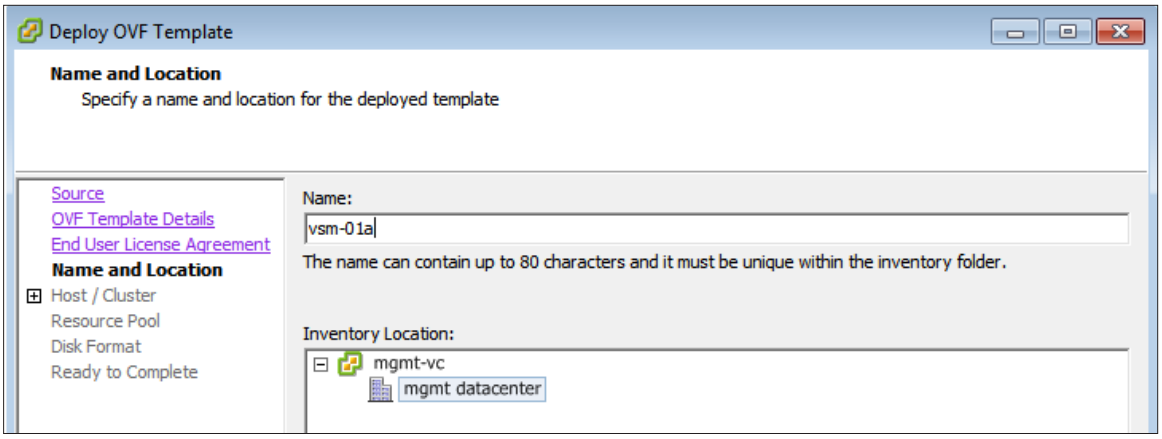
As you have done previously for the other components, select the appropriate file for the vCloud Networking and Security Manager and click **Next** to continue.



You then are presented with an information screen that displays details about the template to be deployed. Click **Next** to continue.

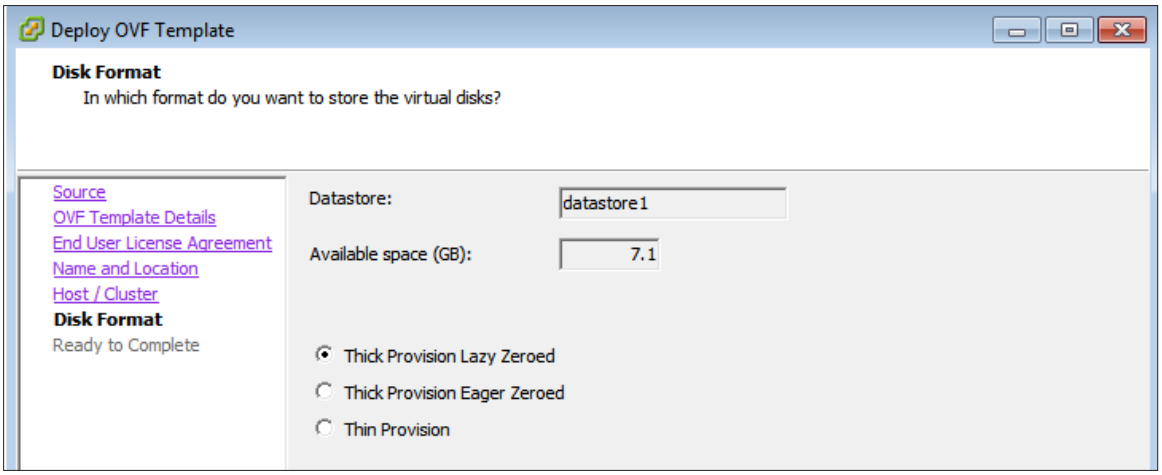


Next you are presented with a EULA from VMware. After clicking the **Accept** button, click the **Next** button to continue.

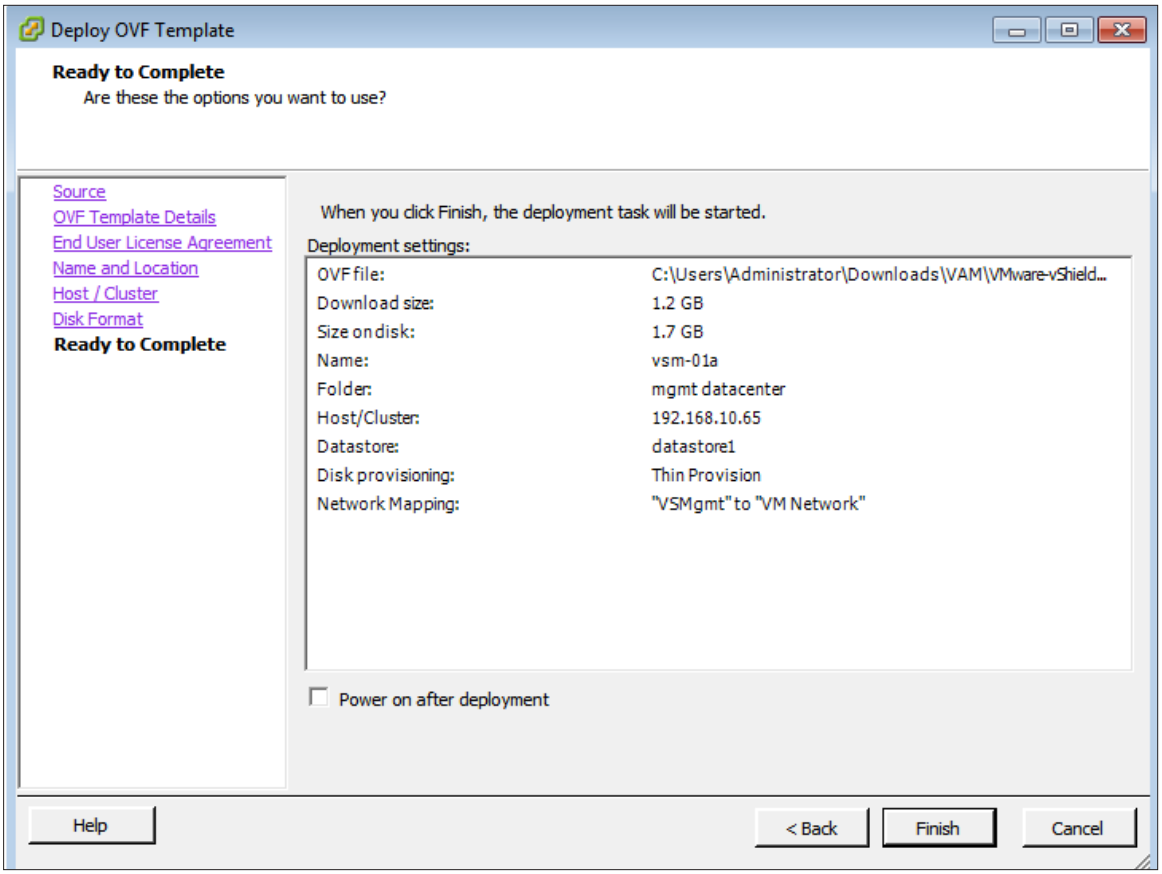


The next screen enables you to specify a name for the vCloud Networking and Security Manager and a location where it will be stored. This guide uses the name **vsm-01a** for the vCloud Networking and Security Manager. Enter your chosen name and click **Next** to continue.

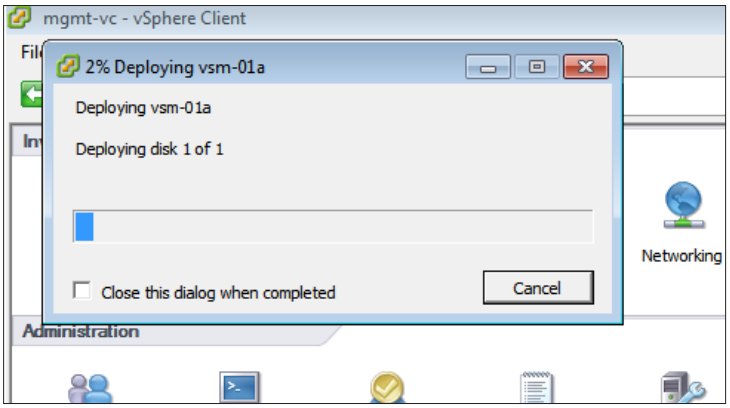
At the next screen, select the host or cluster on which to run the vCloud Networking and Security Manager. Click **Next** to continue.



At the next screen, select a disk format option and click **Next** to continue.



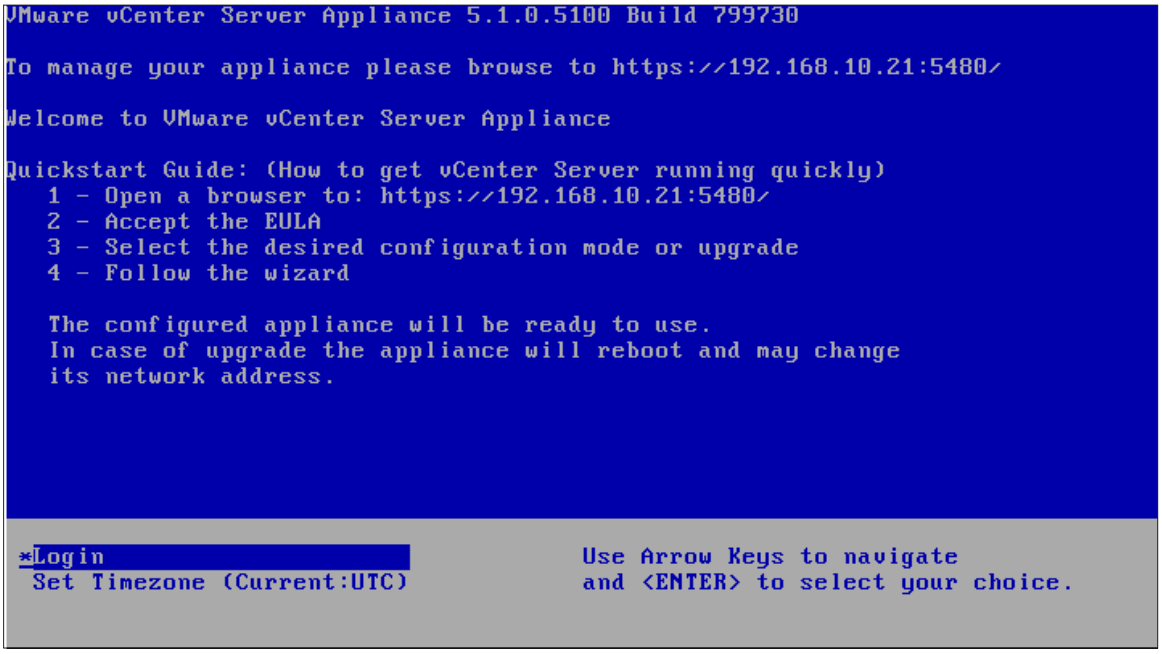
On the summary page, select the **Power on after deployment** option and review the information presented. If satisfied, click **Finish** to start the deployment of the vCloud Networking and Security Manager.



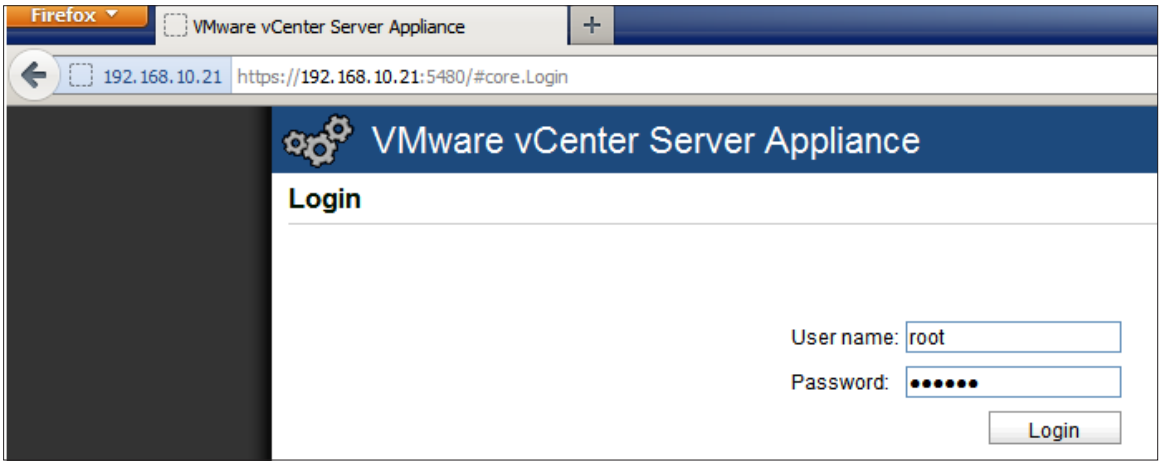
Observe the deployment process and wait until it finishes.

Configuring the vCenter Server Appliance

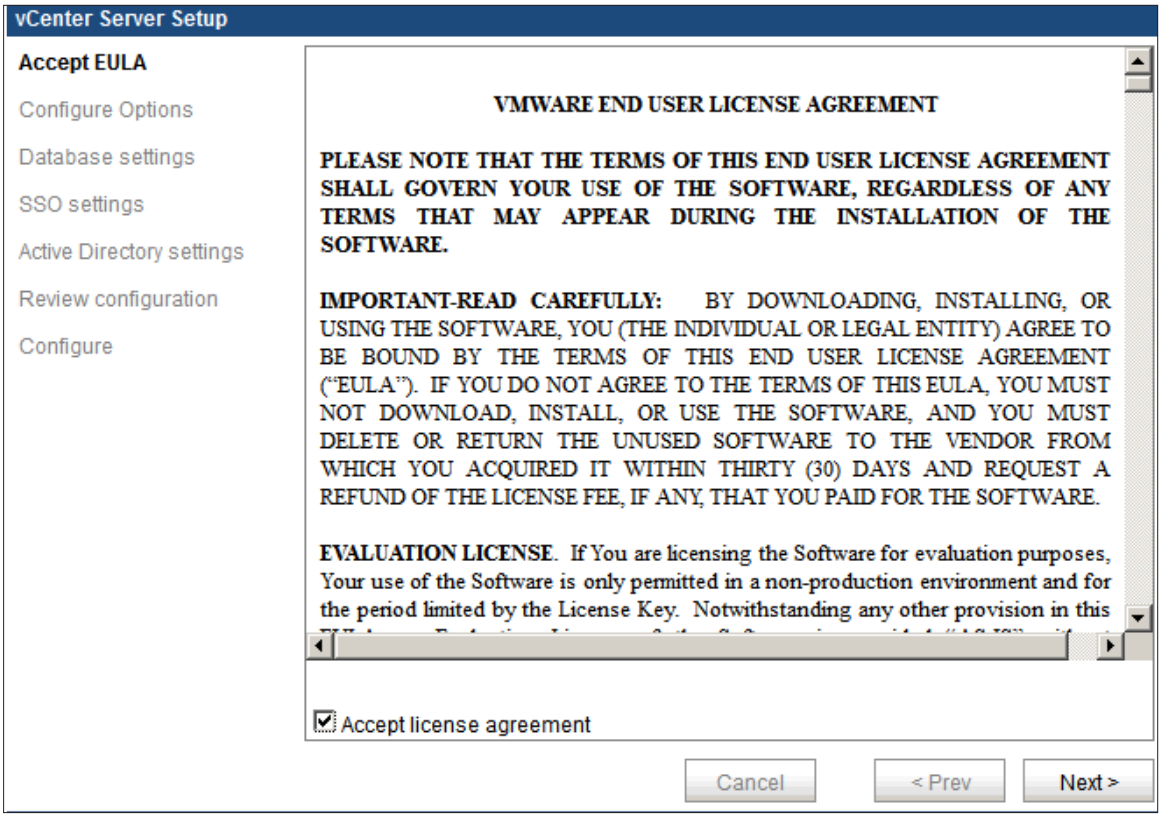
To utilize the vCenter Server Appliance after the initial deployment, you must complete the initial configuration.



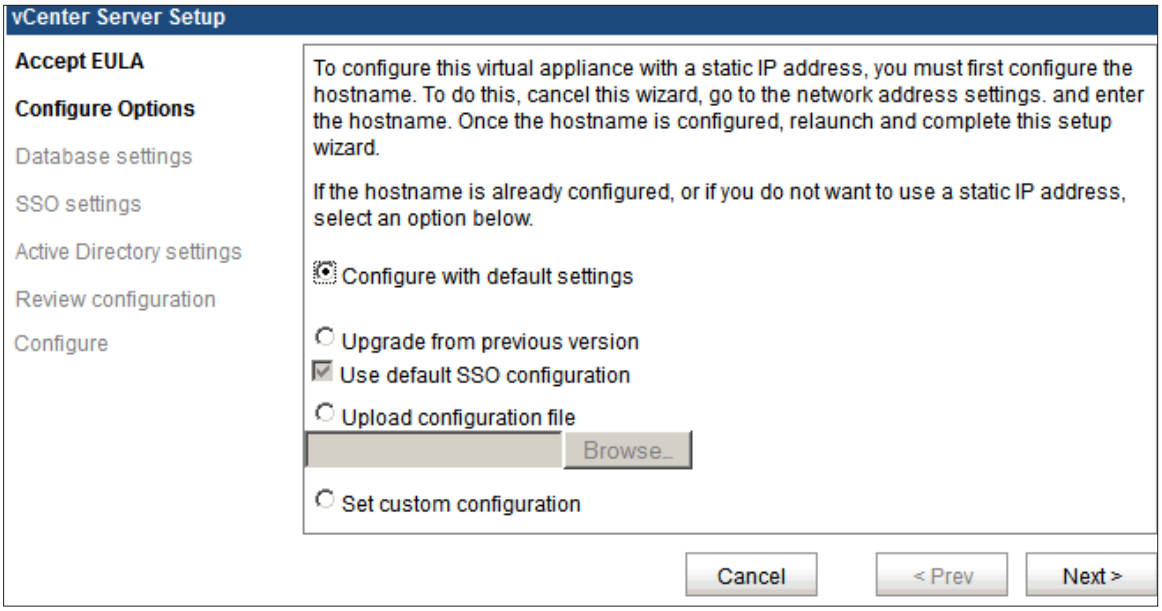
To do this, you must use a Web browser and point it to the address you used for the vCenter Server Appliance. In case you didn't note it previously, you can open a console window to the appliance. This will display the URL that you can use to connect to it.



After you enter the URL into the browser of your choice, you are presented with a login page where you can log in with the default username **root** and default password **vmware**.

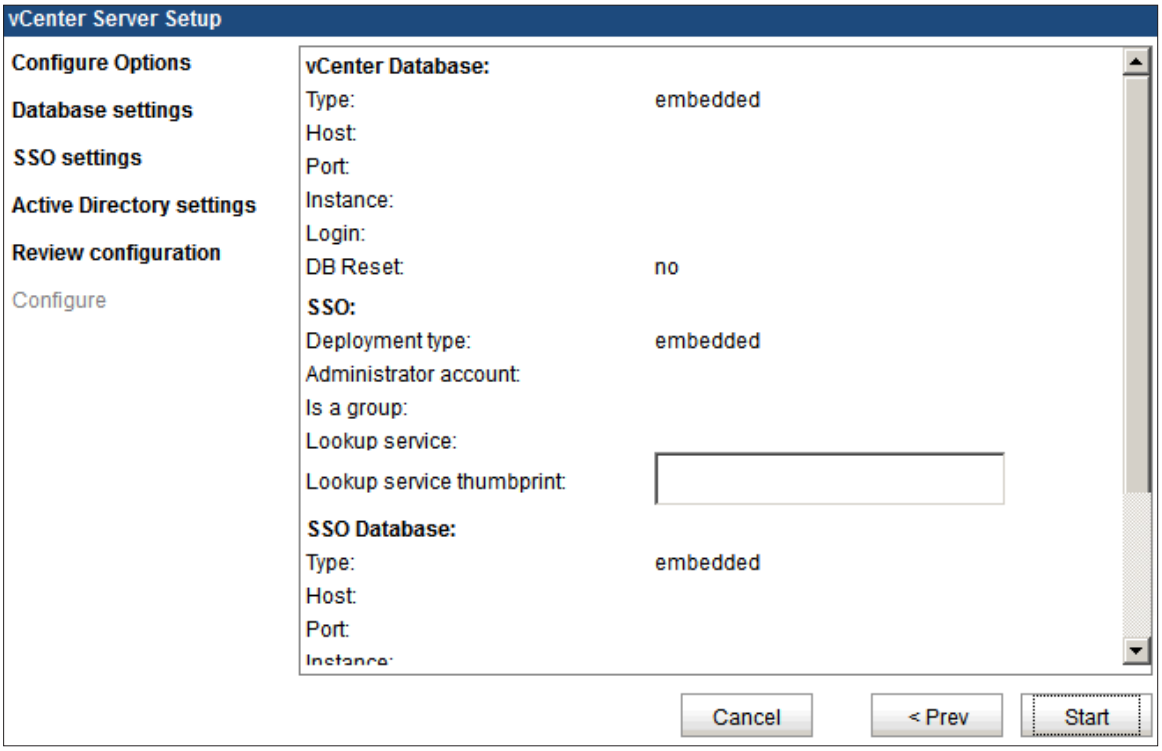


At the initial login, you are presented with a EULA to accept. Select the check box to accept the EULA and click **Next** to continue.

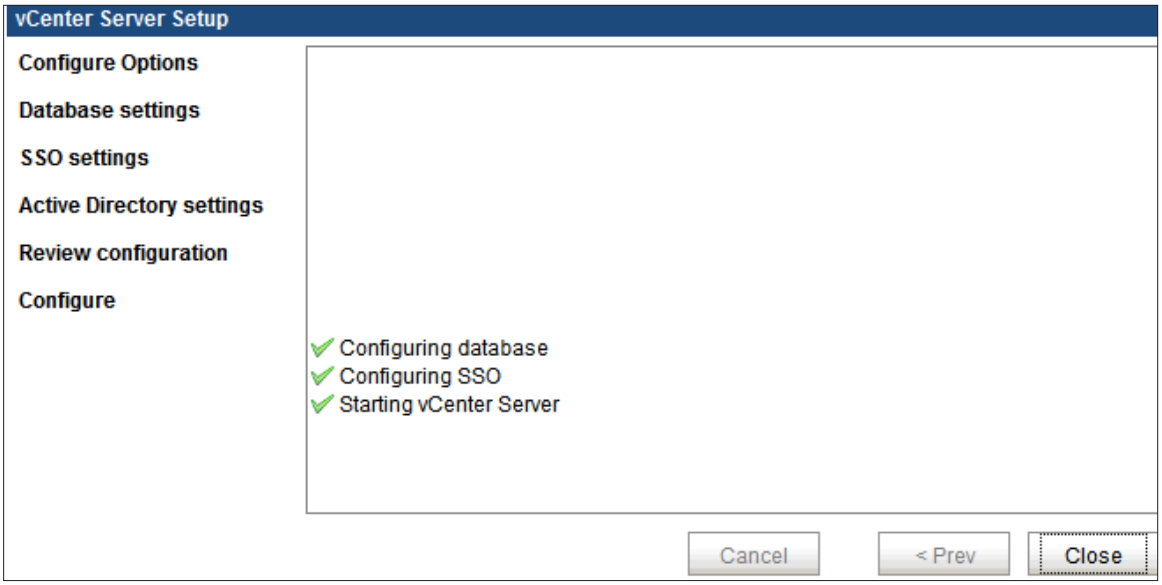


The next step in the configuration of the vCenter Server Appliance enables you to specify different configuration options. If you are using static IP addresses for the vCenter Server Appliance, you must cancel the setup wizard at this time to configure the host name settings before continuing. After that is complete, you can restart this wizard from the home page. If you're not using static IPs, it is not necessary to cancel the wizard.

Click **Next** to move to the next step using the setup wizard.



In this guide, we selected the default options. As a result, we do not have any other inputs to provide. Click **Start** to begin the initial configuration process.



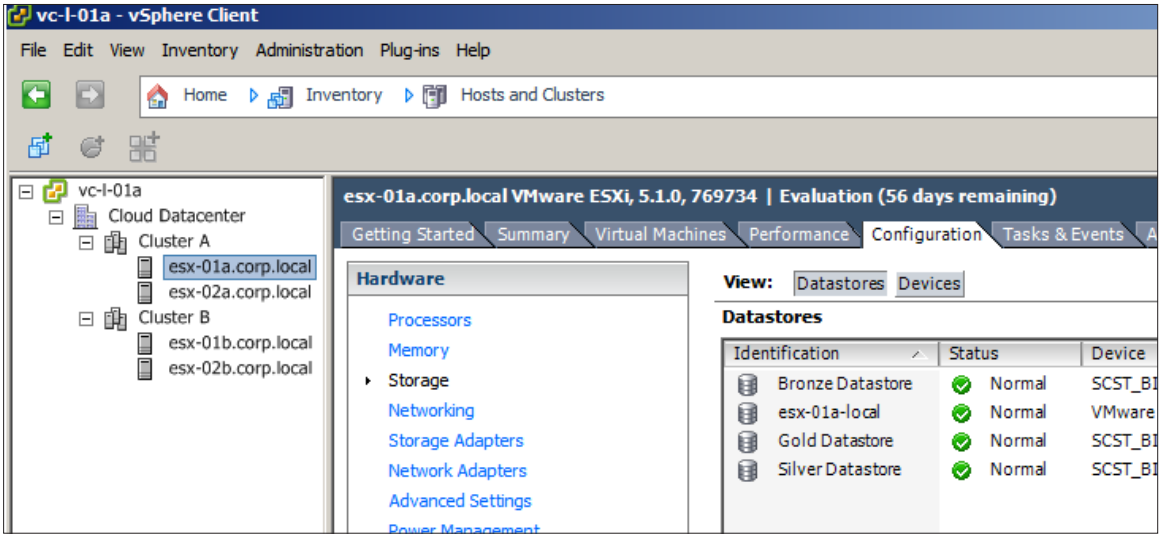
After you have started the vCenter Server instance, click **Close** to exit the setup wizard.

At this point, you should be able to use the vSphere Client to connect to this vCenter Server instance.

Performing Additional vCenter Server Appliance Configuration

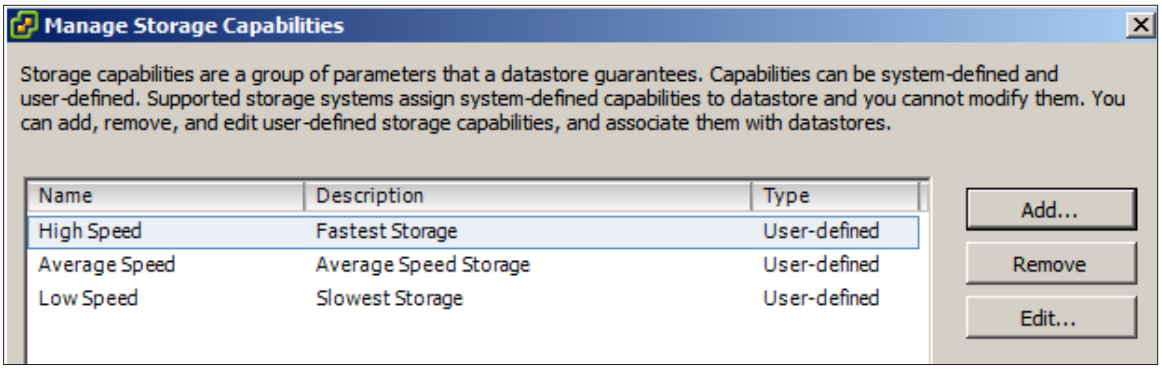
To take full advantage of the procedures presented within this guide, you must perform additional configuration of the vCenter Server Appliance. This entails the configuration of the clusters, hosts, networking and storage that is used.

It is assumed that you are already familiar with these topics, so they are not covered in detail. However, to assist you in the configuration as it is presented in this guide, some guidelines are given here.



First, configure two clusters and add two hosts to each cluster. When you create each cluster, ensure that you configure the vSphere DRS automation level to be **Fully Automatic**.

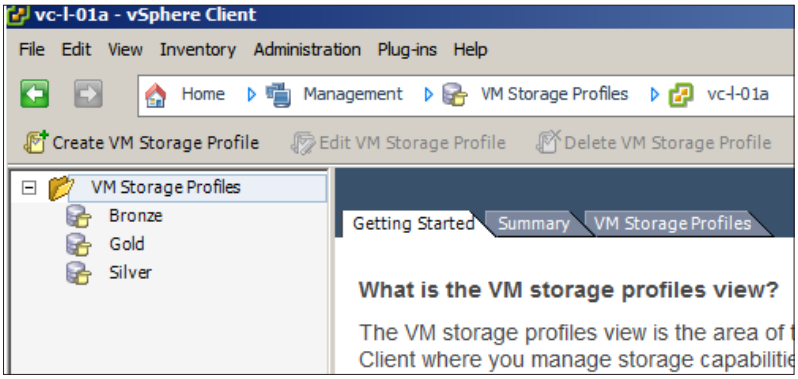
Ensure that all of the hosts have access to three datastores. In this guide, we have named these datastores to represent the storage tier that they will be providing. In the preceding figure, the **Gold, Silver** and **Bronze** datastores are shown.



Configure storage profiles for the storage and ensure that the Storage Profiles feature is enabled. In this guide, three storage capabilities have been defined, to represent the speed of the storage used. For example, this might represent the use of solid-state drives, Fibre Channel (FC) –connected storage and iSCSI-based storage. These capabilities have been assigned to the datastores as shown in the following table:

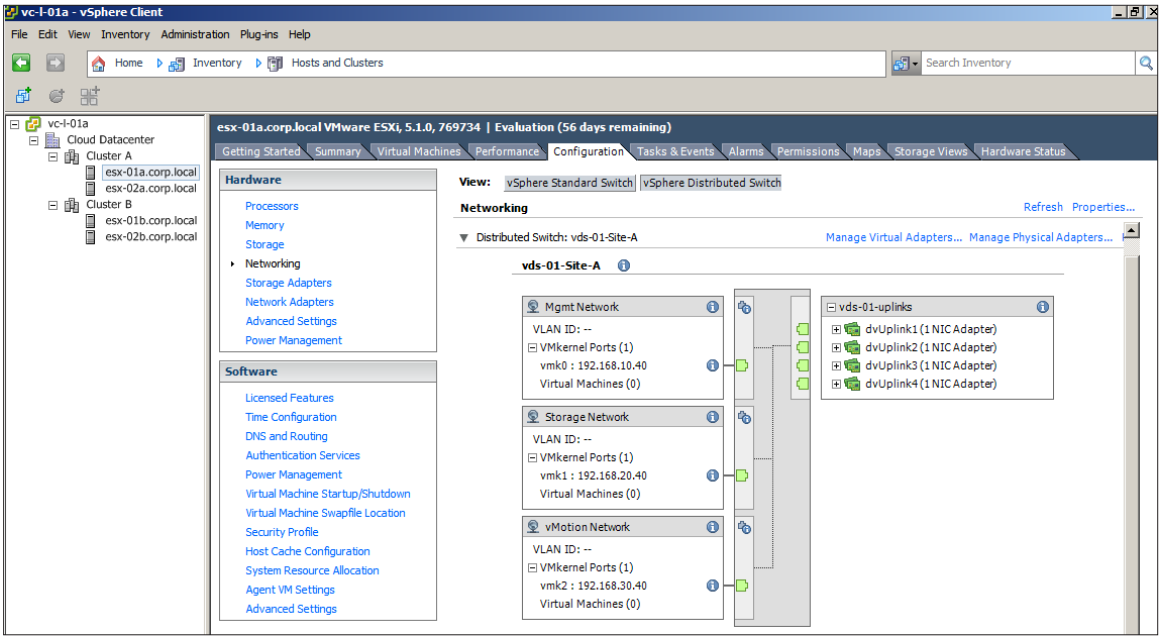
DATASTORE	STORAGE CAPABILITY
Gold Datastore	High speed
Silver Datastore	Average speed
Bronze Datastore	Low speed

Similarly, three storage profiles have been created: **Gold, Silver** and **Bronze**.



Each of these storage profiles has been associated with a storage capability. This is shown in the following table:

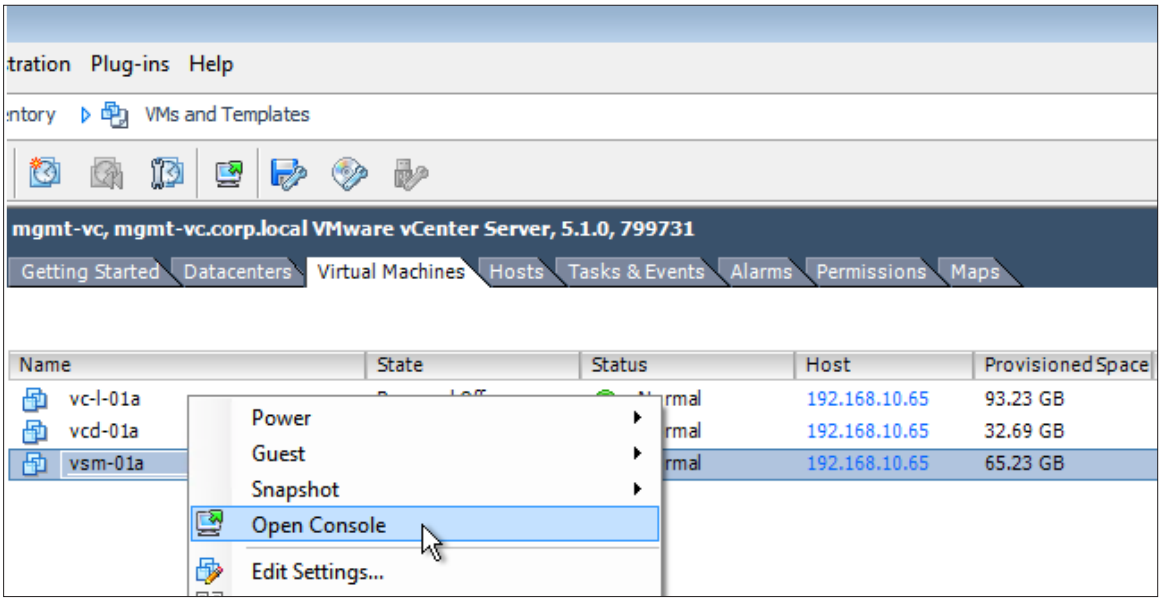
STORAGE PROFILE	STORAGE CAPABILITY
Gold	High speed
Silver	Average speed
Bronze	Low speed



For networking purposes, a VMware vSphere Distributed Switch™ has been created with some standard port groups. It is connected to all the hosts.

Performing vCloud Networking and Security Manager Configuration

We now must perform the initial configuration of the vCloud Networking and Security Manager.



To start, use the vSphere Client connected to the vCenter Server that manages the management cluster. Open the console to the vCloud Networking and Security Manager deployed earlier.

```
/etc/rc.d/init.d/rc: End /etc/rc.d/rc3.d/S98local start

[   90.964558] e1000: mgmt NIC Link is Up 1000 Mbps Full Duplex, Flow Control: N
one

manager login: admin
Password:
manager> enable
Password:
manager# setup

Use CTRL-D to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

IP Address (A.B.C.D): 192.168.10.24
Subnet Mask (A.B.C.D): 255.255.255.0
Default gateway (A.B.C.D): 192.168.10.1
Primary DNS IP (A.B.C.D): 192.168.10.20
Secondary DNS IP (A.B.C.D):
Warning: Secondary DNS not set.
DNS domain search list (space separated): corp.local
Old configuration will be lost
Do you want to save new configuration (y/[n]): y
Please logout and login back again.
manager# _
```

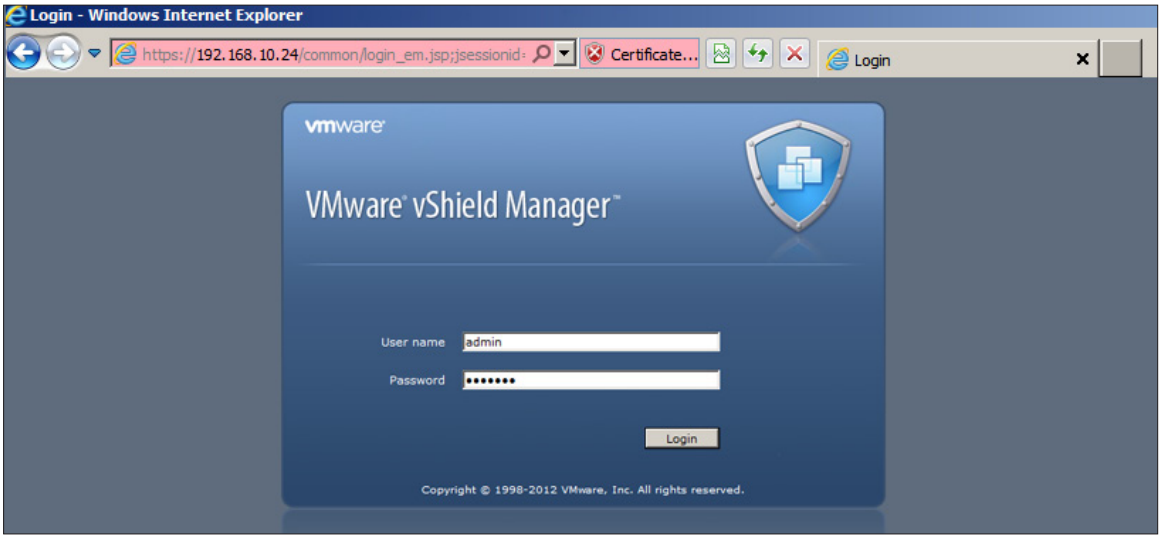
When it is connected to the console, log in with the username **admin** and the password **default**. Type the command "enable" to enter the privileged mode.

Provide the password **default** again. At the prompt, type "setup" to start the initial configuration process.

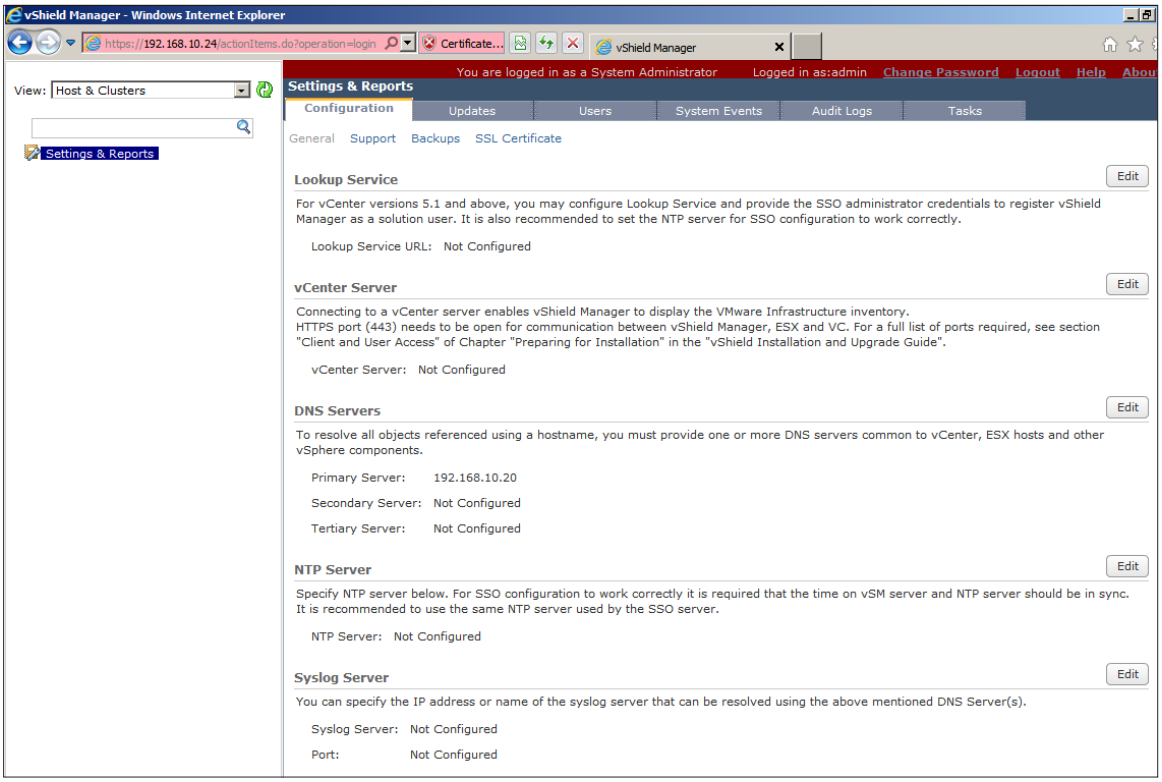
When prompted, enter the appropriate values for the vCloud Networking and Security Manager IP address, netmask and DNS information.

To save the new configuration, verify the information entered and answer "y" when prompted. At the prompt, type the command "exit" to log out. Then close the console window.

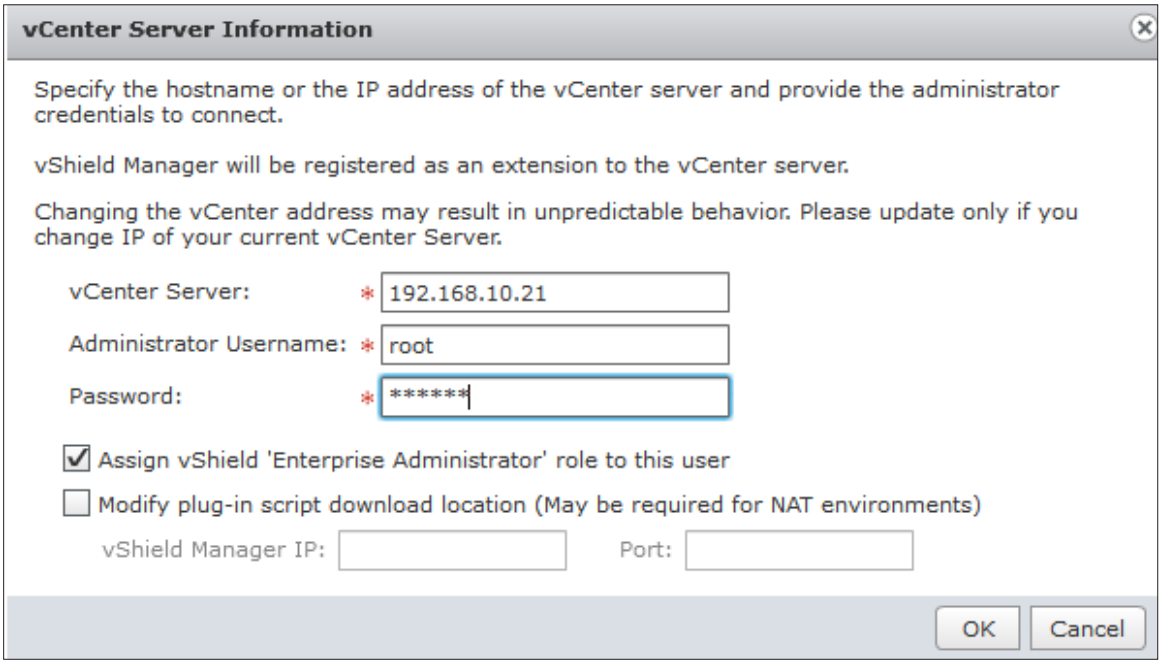
At this point, we can use a Web browser and connect the vCloud Networking and Security Manager user interface using the IP address specified to complete the initial configuration. It might take a couple of minutes for the previous step to complete before you can access the vCloud Networking and Security Manager user interface.



When connected to the vCloud Networking and Security Manager interface, log in with the username "admin" and the default password "default."



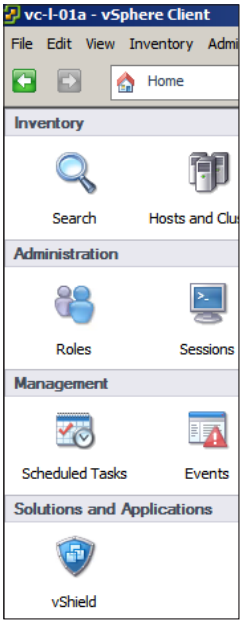
At a minimum, we must associate this vCloud Networking and Security Manager instance with the vCenter Server that we deployed for use by vCloud Director. Ideally, you would configure all of the options presented on the configuration screen. To configure any of the parameters, simply click the edit button next to it. Click the edit button next to **vCenter Server**.



You will be prompted to enter information needed to connect to the vCenter Server instance. This includes the host name or IP address and the login credentials. Enter the appropriate information as needed. The default login credentials for the vCenter Server Appliance are "root" and "vmware."

Select the **Assign vShield 'Enterprise Administrator' role to this user** check box. Click **OK** to continue.

At this point, you will be prompted to confirm the authenticity of the vCenter Server that you are connecting to. Click **Yes** to continue.



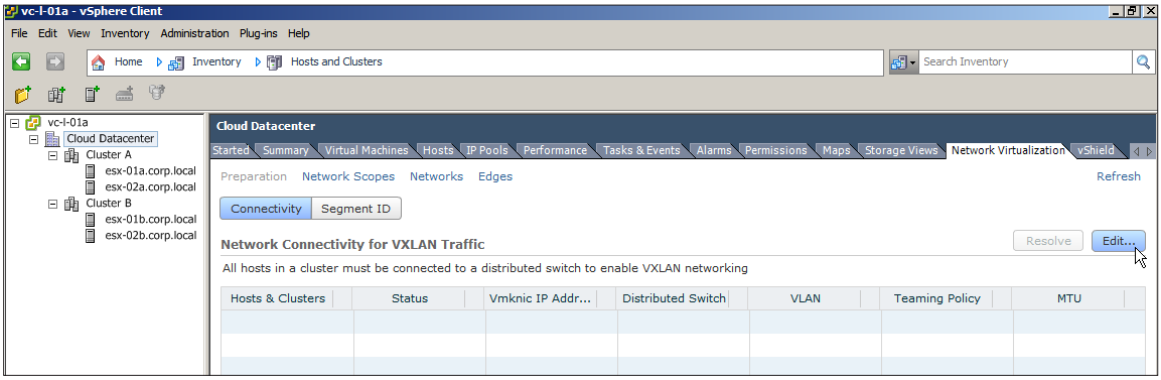
You can confirm that the vCloud Networking and Security Manager association to the vCenter Server instance was successful by using the vSphere Client and validating that the option for vShield is displayed under **Solutions and Applications**.

VXLAN Preparation

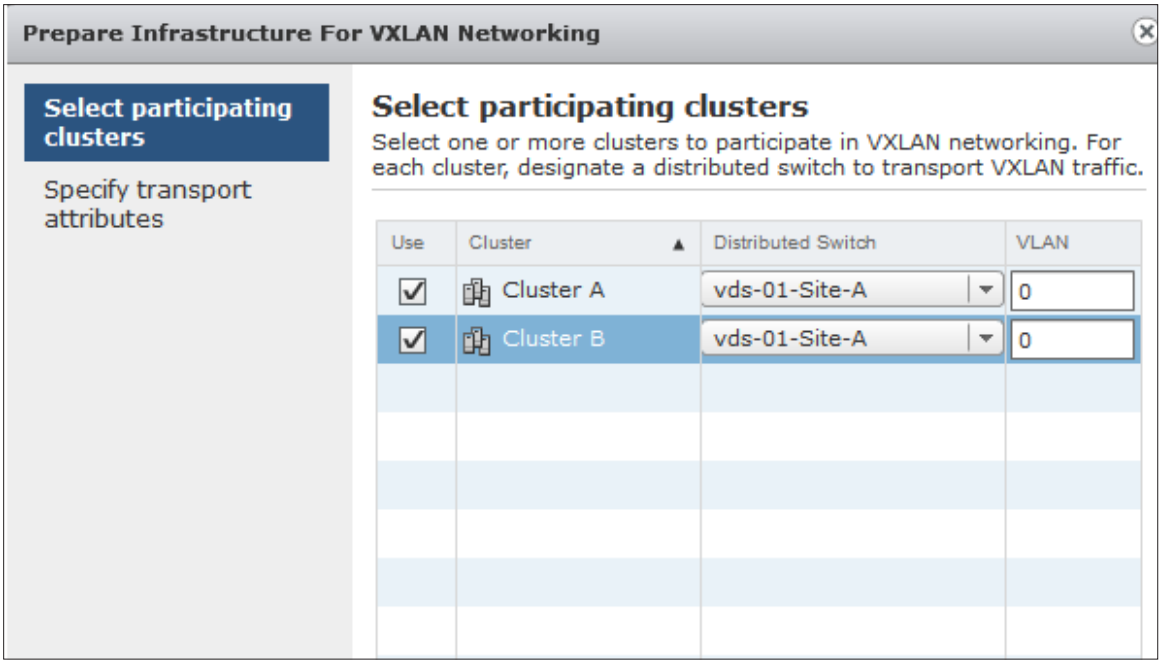
VXLAN provides capabilities to dynamically create thousands of networks on top of an existing network infrastructure as well as create a stretched layer 2 domain across clusters that might reside in different networks.

To use VXLAN with vCloud Director, the VXLAN fabric first must be prepared. Before continuing, ensure that your network is capable of supporting multicast packets and that there is a DNS server accessible.

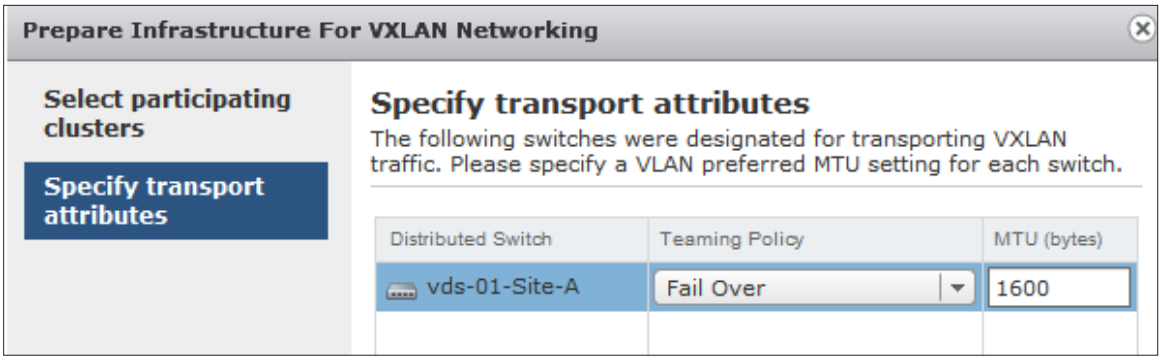
Connect to the vCenter Server instance you deployed earlier to be used by vCloud Director with the vSphere Client.



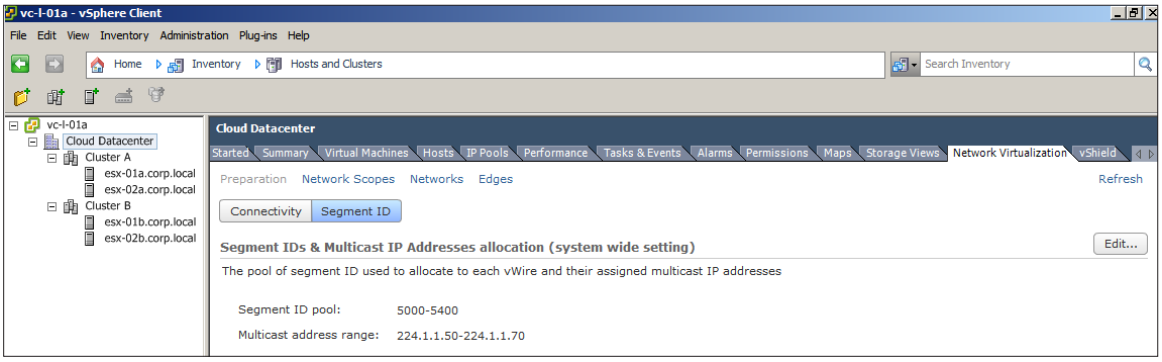
Select the datacenter object in the left-hand pane. You will notice a new tab in the right-hand pane labeled **Network Virtualization**. Select this tab and click the **Preparation** link. There are two steps in the preparation of the VXLAN fabric: defining the connectivity and defining the segment IDs. These two options are displayed after you have clicked the **Preparation** link. Select the **Connectivity** tab and click the **Edit** button.



This brings up a window that enables you to select the clusters that will use the VXLAN fabric. Select both of the clusters and the Distributed Switch that you created earlier when you prepared the vCenter Server. If you must specify a VLAN ID, do this as well. Click **Next** to continue.

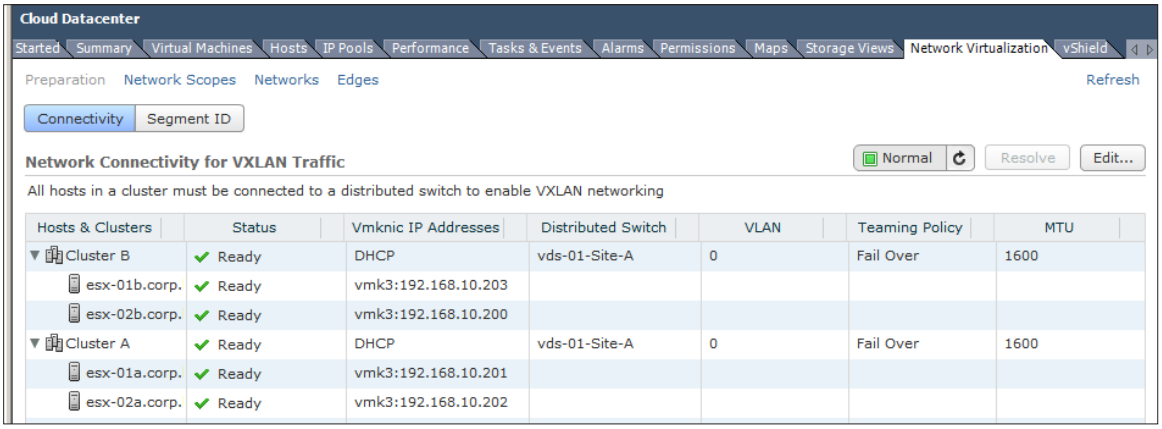


The next screen enables you to select the **MTU** size and the **Teaming Policy** to be used for the **Distributed Switch** selected. The teaming policy is highly dependent on the type of network used in your evaluation environment. In this guide, the teaming policy is set to **Fail Over**. Ensure that you select an option compatible with your environment. Leave the MTU setting at **1600** and click **Finish** to continue.



Next, select the **Segment ID** tab and click **Edit.** This will display a pop-up window where you can enter the range of segment IDs to use for the segment ID pool and the multicast address range.

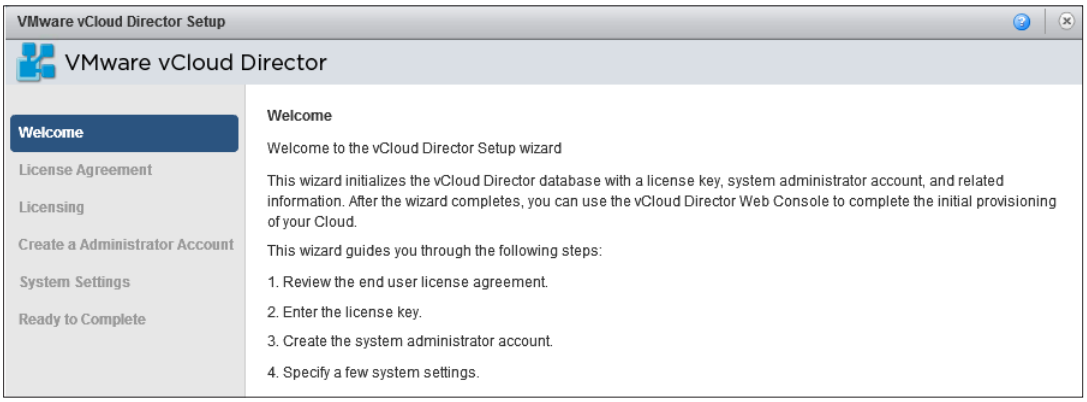
The values that you use will depend on the network configuration of the environment you are working in. After you ensure that the values are acceptable for your environment, click **OK** to apply the changes.



Select the **Connectivity** tab again and verify that the status is labeled as **Ready**. You will notice that the vmknics have acquired an IP address from the DHCP server.

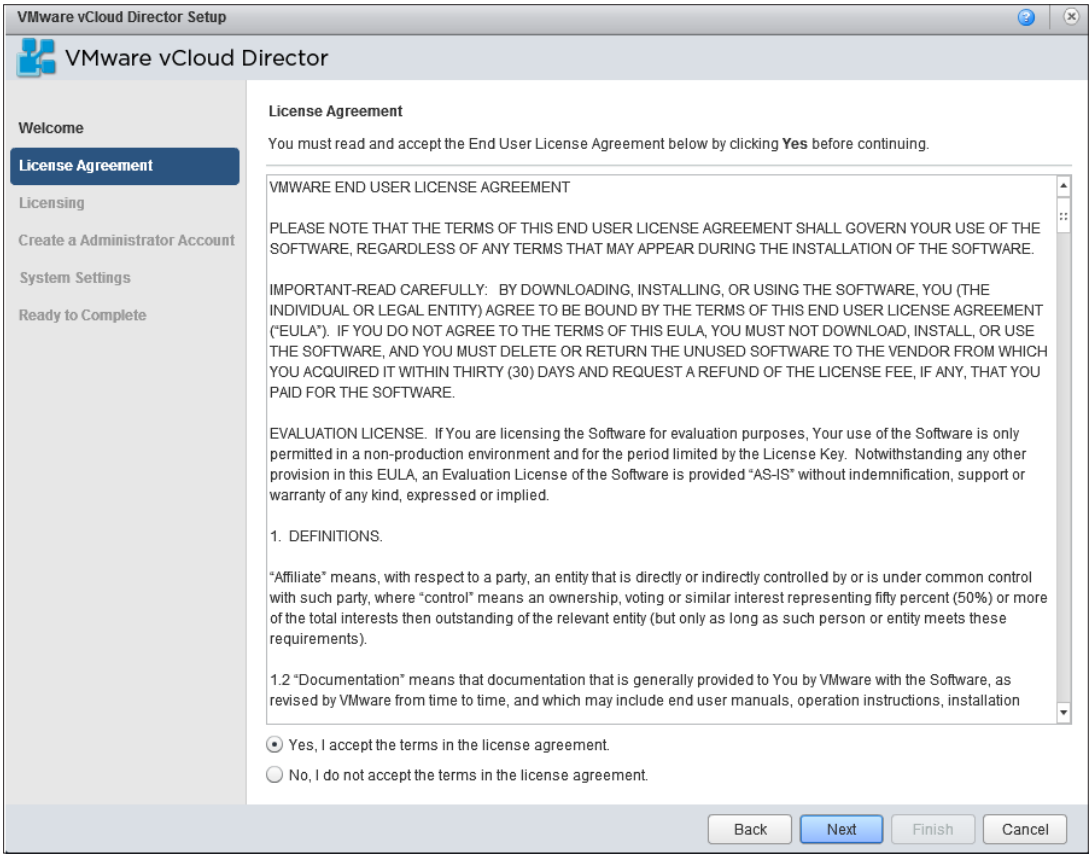
vCloud Director Initial Setup

Before you can start using vCloud Director, you must complete the initial installation that is presented the first time you log in to the vCloud Director interface. The default username for the vCloud Director Appliance is "root" and the default password is "vmware."

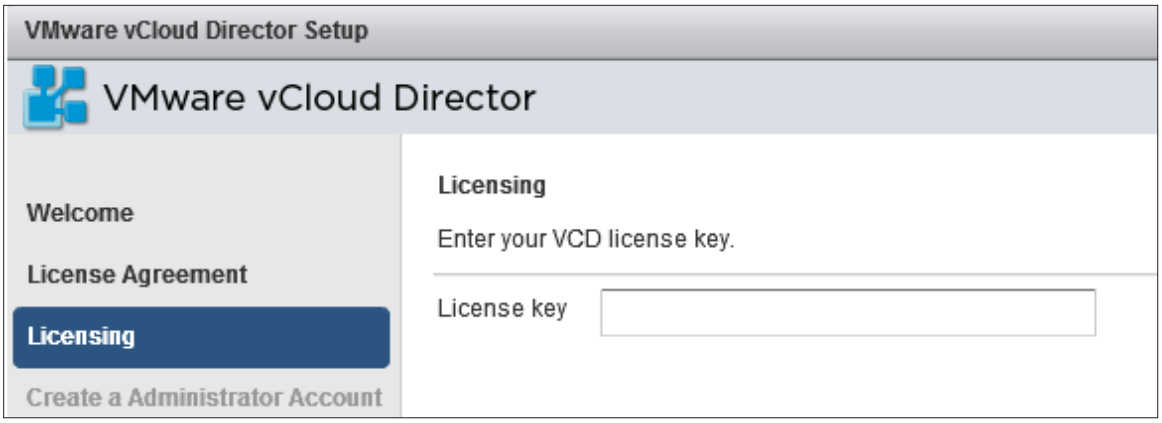


Connect the vCloud Director by using the URL https://<address>/cloud, where <address> is equal to the lowest IP address that you specified when deploying the vCloud Director Appliance.

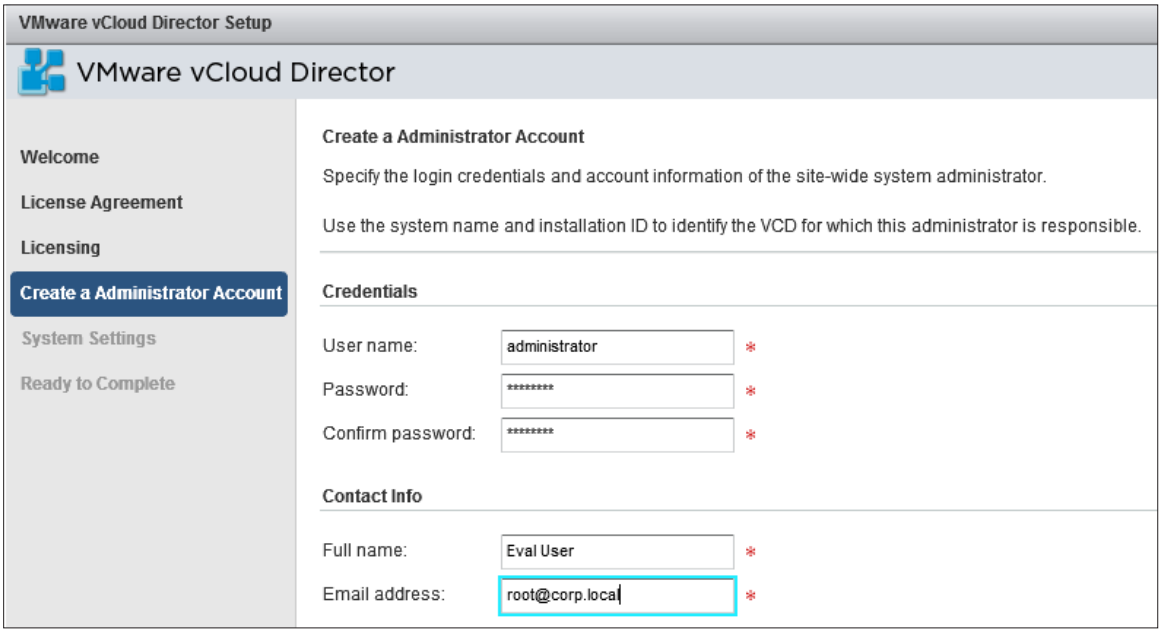
This will display the initial setup wizard for vCloud Director. Click **Next** to continue past the **Welcome** page.



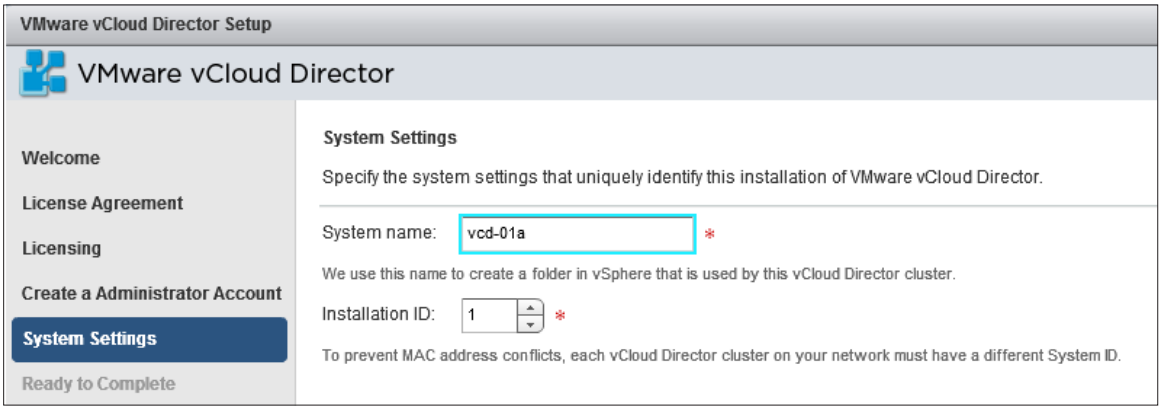
On the next page, click **Radio** to accept the EULA. Click **Next** to continue.



Now you will be asked to provide your vCloud Director license key. Enter a valid license key and click **Next** to continue.

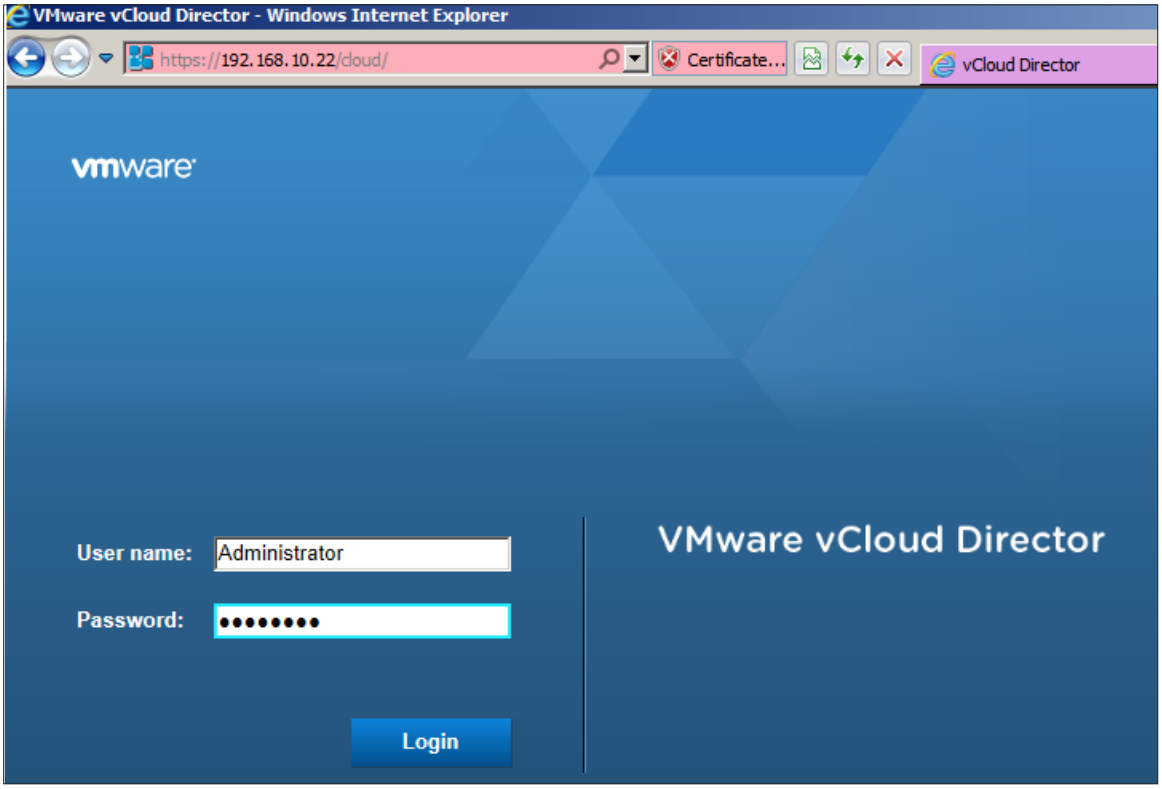


The next page enables you to define the user account to be used for the cloud administrator. Specify a username and password and complete the remaining identification fields. Click **Next** to continue.



The wizard then enables you to specify the name and installation ID for this vCloud Director instance. This guide calls the vCloud Director instance **vcd-01a**. The Installation ID can be left at the 1 default, because there are no other vCloud Director instances deployed. If there were, each instance would require a unique **installation ID**. Click **Next** to continue.

On the next screen, review the information you provided. Click **Finish** to exit the wizard.

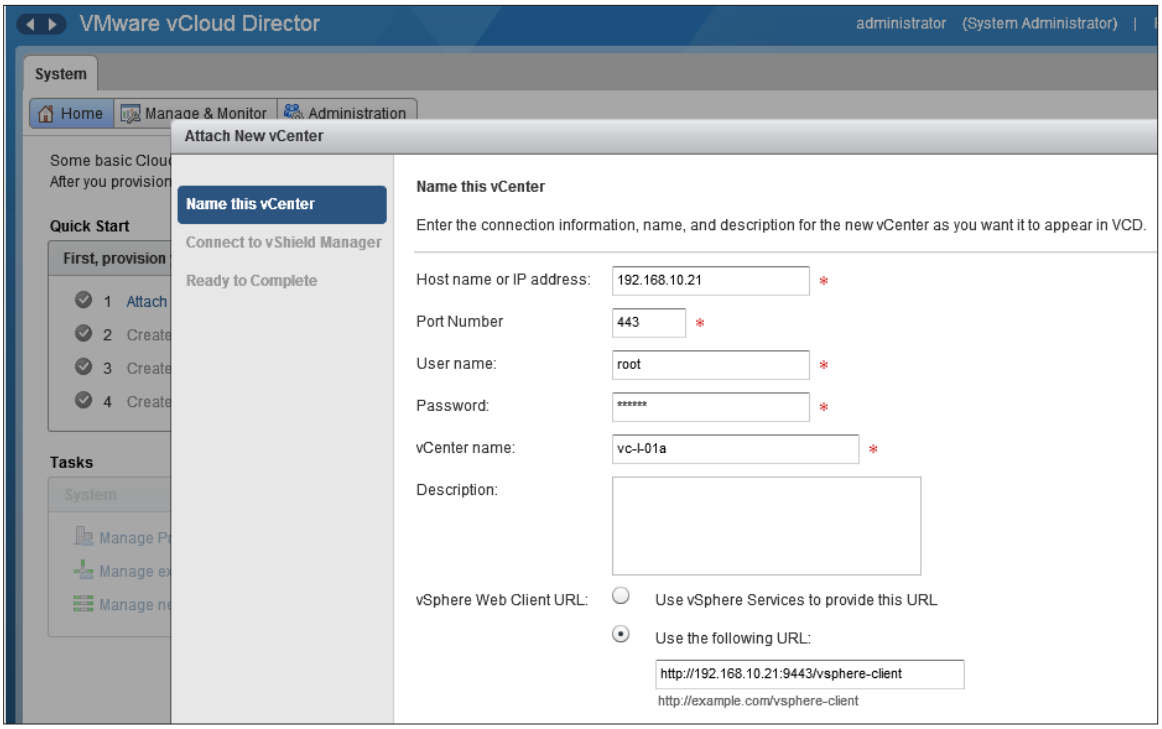


Log in to the vCloud Director user interface using the same URL you used previously and specifying the login credentials for the cloud administrator account defined earlier.

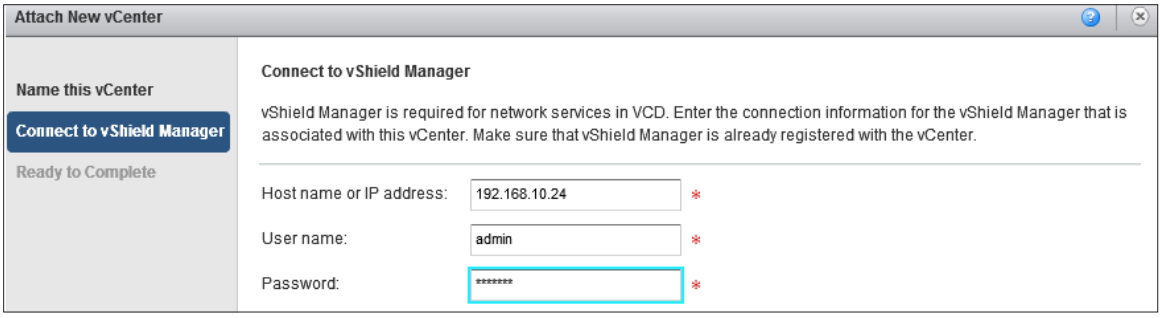
Attaching to Virtual Center

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 end users.

After logging in to vCloud Director as the cloud administrator, select the **Attach a vCenter** option under **Quick Start**.



This will bring up a wizard that enables you to specify the information required to associate the vCenter Server instance you created earlier with this vCloud Director instance. Enter the appropriate information as shown in the preceding screenshot. Click **Next** to continue.



Enter the necessary information to connect to the vCloud Networking and Security Manager. Click **Next** to continue.

You then will be provided with a summary of the information that you entered. Review the information and click **Finish** to complete the wizard.

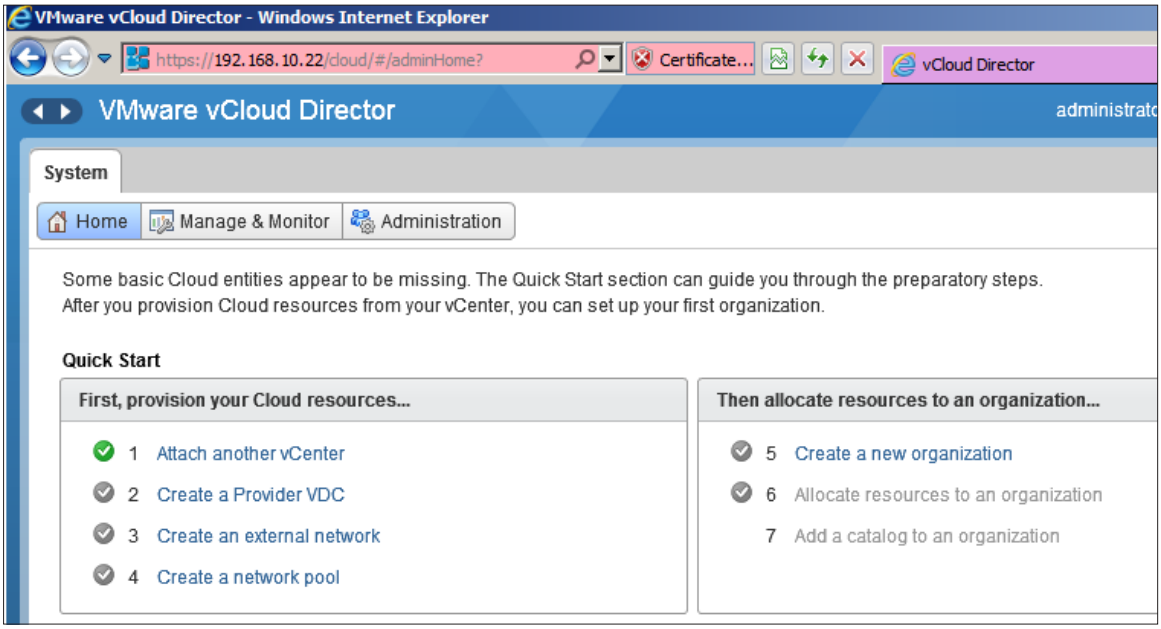
Defining the Provider Virtual Datacenter

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

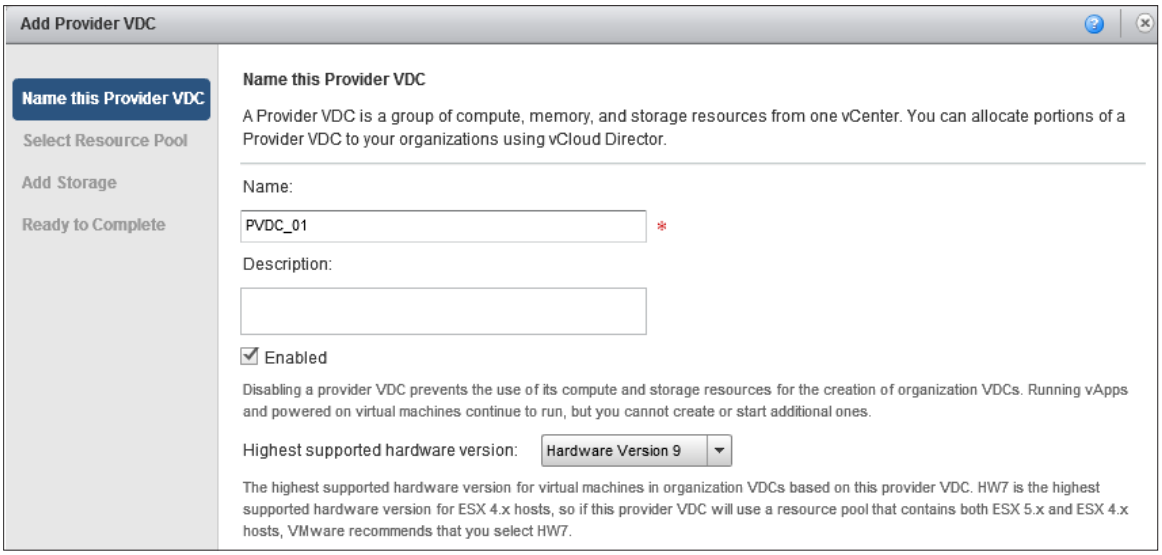
Creating a Provider VDC

After a vCenter Server has been attached to vCloud Director, the resources that it provides can be added to a provider VDC. A provider VDC provides the capability for multiple vCenter Servers to be connected to vCloud Director and 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 later will get divided up among the various organizations within your vCloud Director environment. You can consider the resources that make up a provider VDC as, 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.

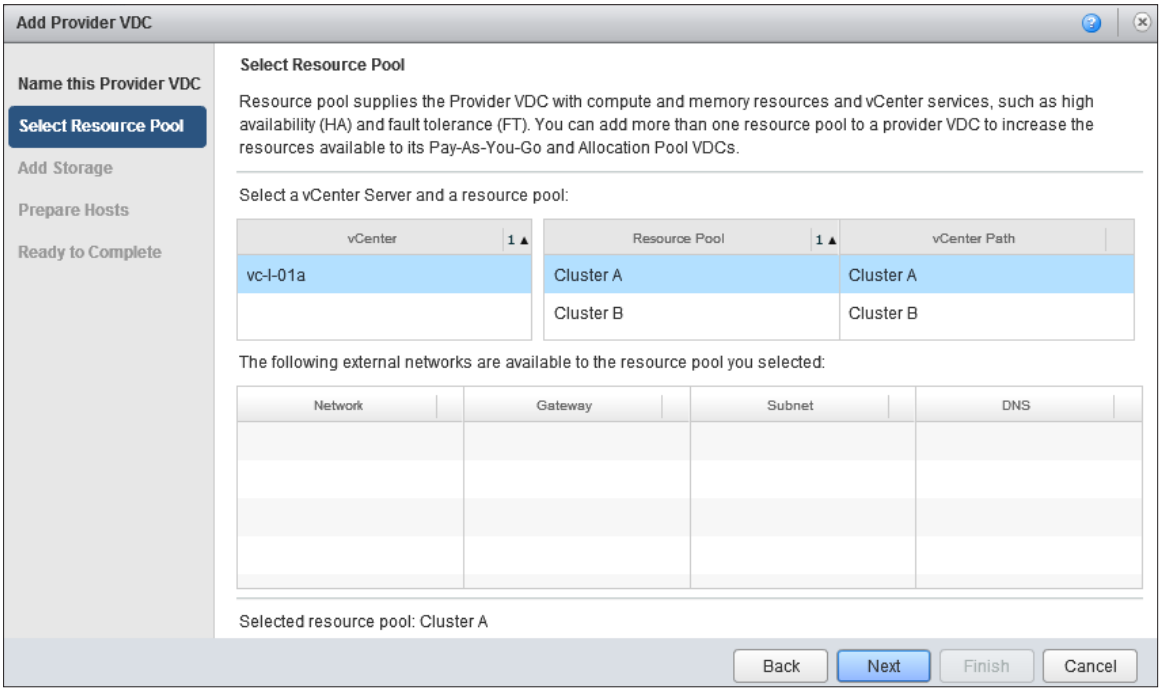


This brings up a wizard that will walk you through the process of creating a provider VDC. The first part of this process is to give a name to the provider VDC to be created. In this guide, we will create multiple provider VDCs. To facilitate ease in recognition, name the first provider **VDC PVDC_01.**

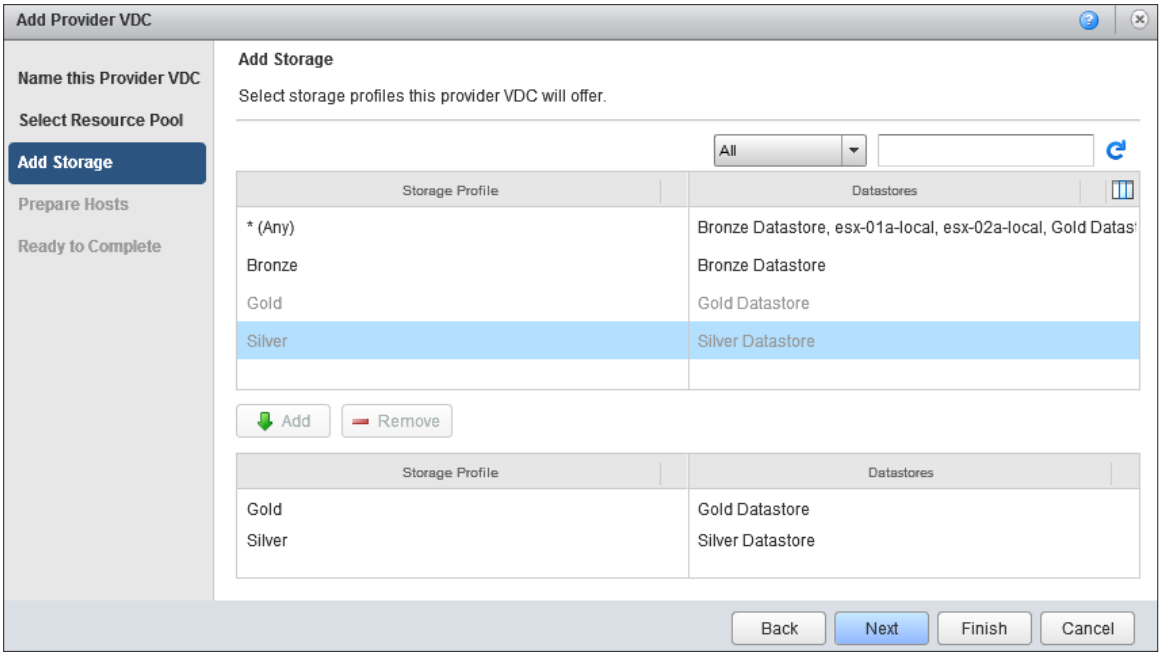
Because we will be using this provider VDC immediately, Select the **Enabled** check box.

To enable maximum flexibility, ensure that the **Highest supported hardware version** is set to **Hardware Version 9**.

Click **Next** to continue.



The wizard then prompts you to select the resource pool that will be used. First, select the vCenter Server that you associated with the vCloud Director instance. Then the resource pools available for selection will appear in the adjacent table. For this provider VDC, select **Cluster A** and click **Next** to continue.

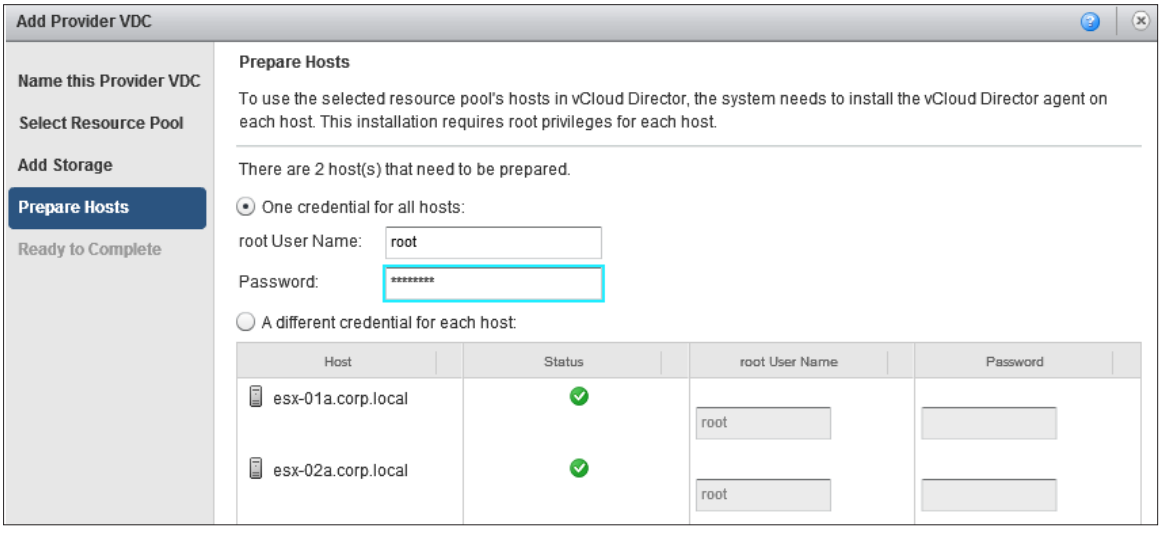


The next step in the wizard enables you to select the storage that this provider VDC will supply. In vCloud Director 5.1, all storage is represented as a storage profile. This information is refreshed from the vCenter Server instance every 5 minutes by default. If you do not see the storage profiles that you defined, quit the wizard and perform the steps again after 5 minutes.

If you do not have the ability to use storage profiles or did not configure them, you will notice a storage profile labeled **Any**, which represents all of the available storage.

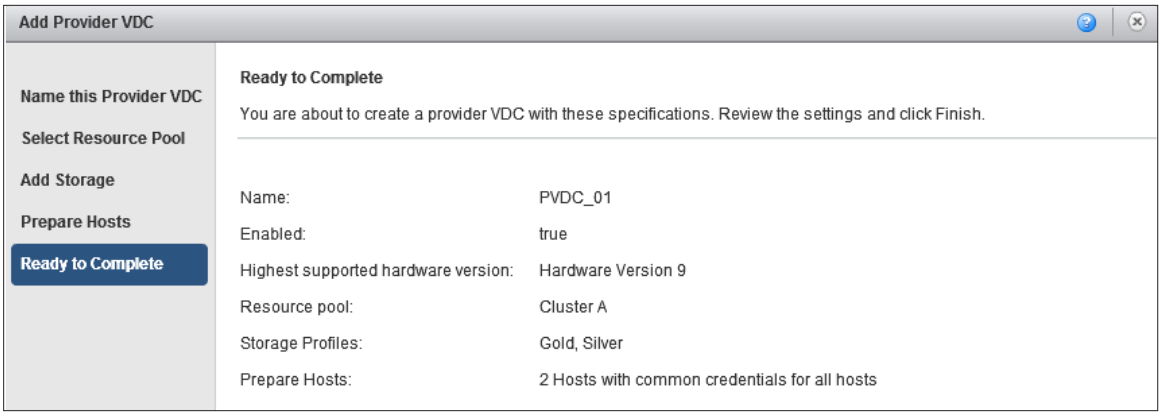
Select the **Gold** storage profile and click **Add** to add the storage profile. Repeat for the **Silver** storage profile. This will enable this provider VDC to supply multiple tiers of storage.

Click **Next** to continue.



Next, you must specify the root login credentials for the vSphere hosts that are part of the cluster that you selected earlier. This enables vCloud Director to install an agent on each of the hosts.

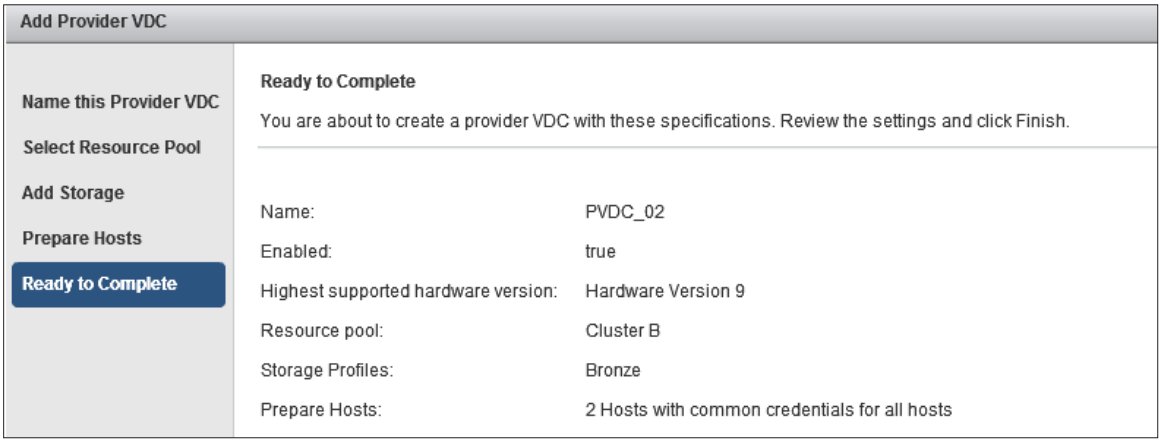
Specify the correct information needed and click **Next** to continue.



You then can review the information provided in summary form. Ensure that the information is correct. Click **Finish** to complete the wizard.

Create an Additional Provider Virtual Datacenter

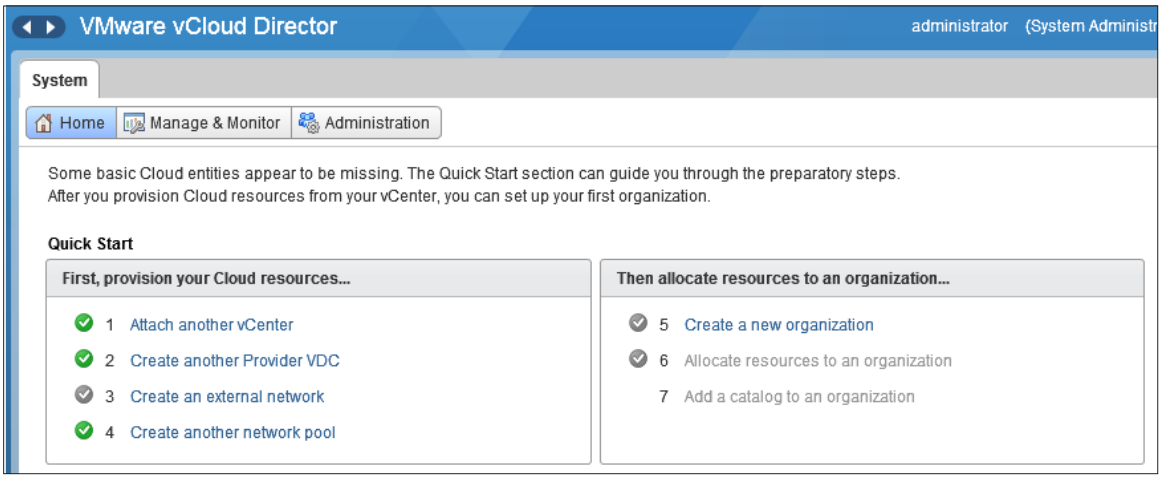
For the purposes of this guide, repeat the previous steps to create another provider VDC called **PVDC_02**. Use the second cluster and assign the **Bronze** storage profile to this provider VDC.



The summary page for provider **VDC PVDC_02** looks like the preceding example.

Network Pools

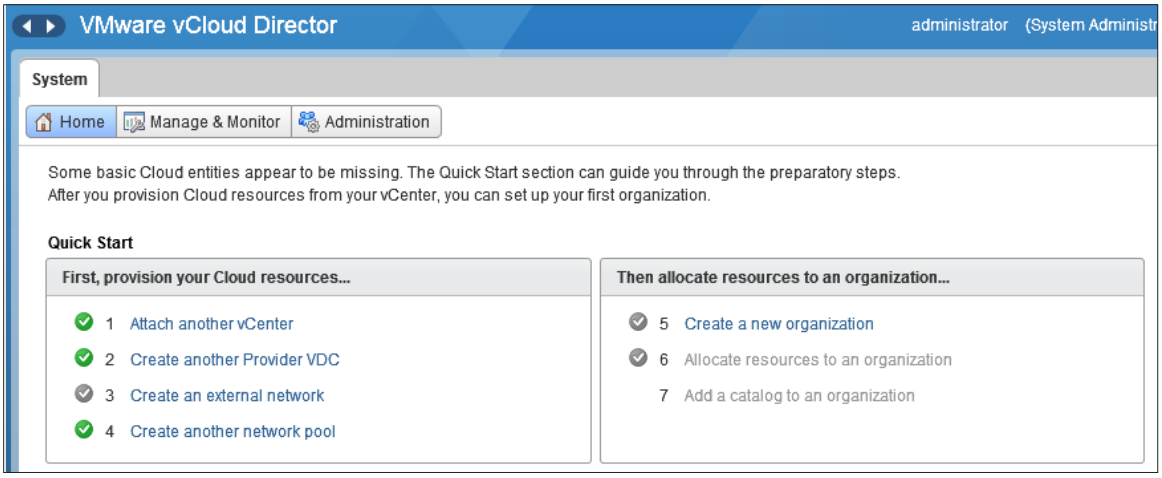
Network pools provide a collection of undifferentiated networks that then are consumed by organizations to provide connectivity within the cloud environment. vSphere network resources such as VXLAN, VLAN IDs and port groups back a network pool.



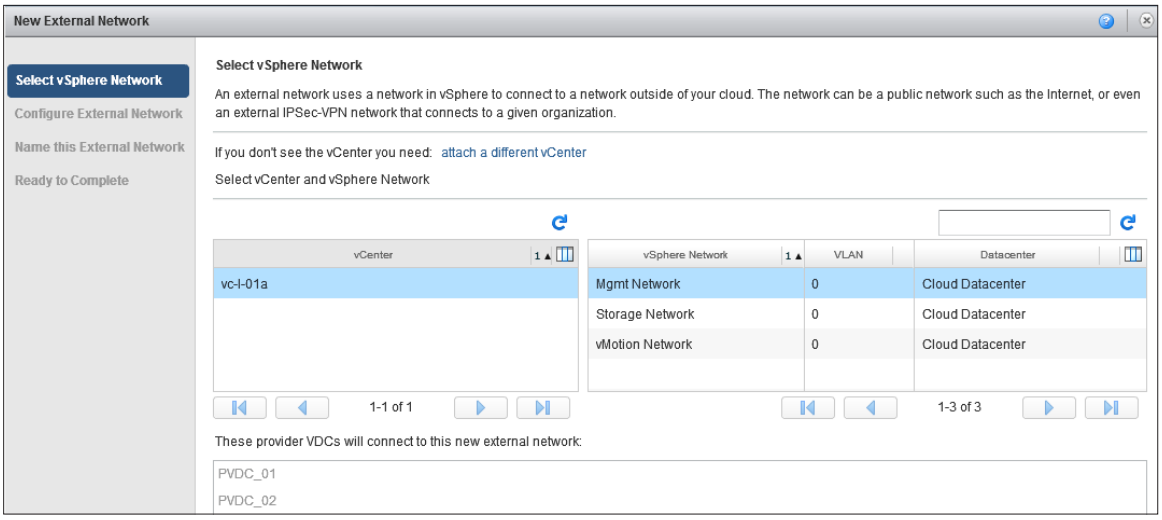
After the creation of the provider VDCs in the previous step, a green check mark appears next to step 4 of the **Quick Start** section. It is present because vCloud Director automatically creates a network pool using the VXLAN fabric you prepared earlier.

Defining an External Network

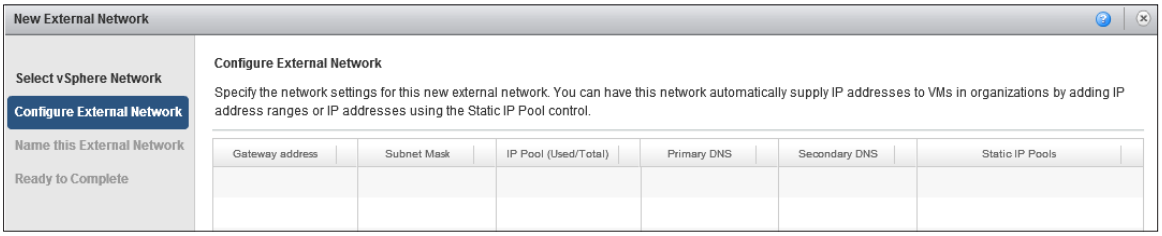
An external network is one that enables virtual machines in your cloud to connect outside of your cloud environment. You can use it to provide access to a corporation's intranet or the Internet or to establish an IPsec VPN connection to an external network or another organization.



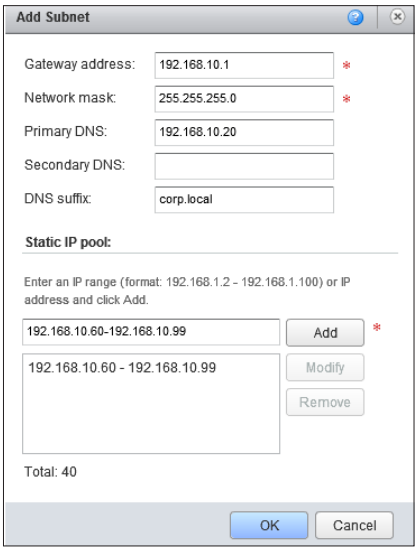
To create an external network, select **Create an external network** under **Quick Start** on the **Home** screen.



This brings up a wizard. On the first page, select the vSphere network to be used for the external network. Select **Mgmt Network** and click **Next** to continue.

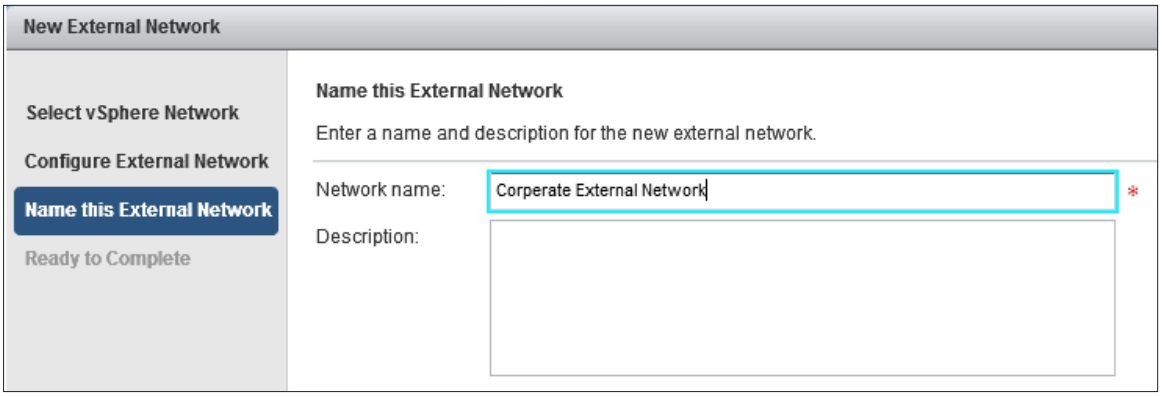


The next step using the wizard enables you to define the network settings used for the external network. Click **Add** to configure the settings.



Specify the information required to match your network configuration. You also must configure a range of IP addresses that can be assigned to objects connecting to this external network.

When finished, click **OK** to close this dialog box and return to the wizard. You can see the information you entered listed in the table. Click **Next** to continue.

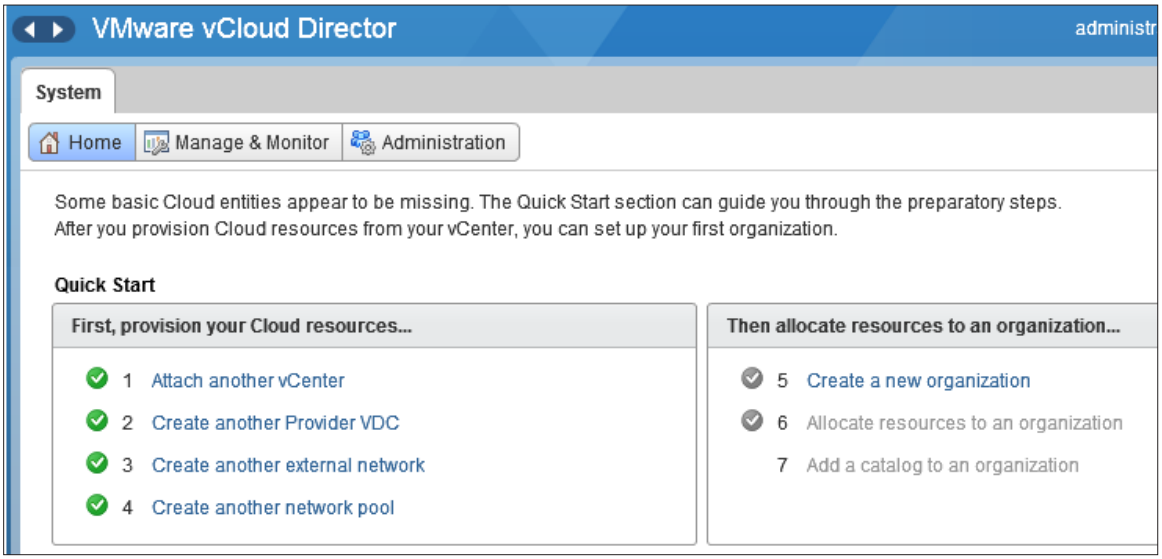


Next, provide a name for this external network. Specify the name **Corporate External Network** and click **Next** to continue.

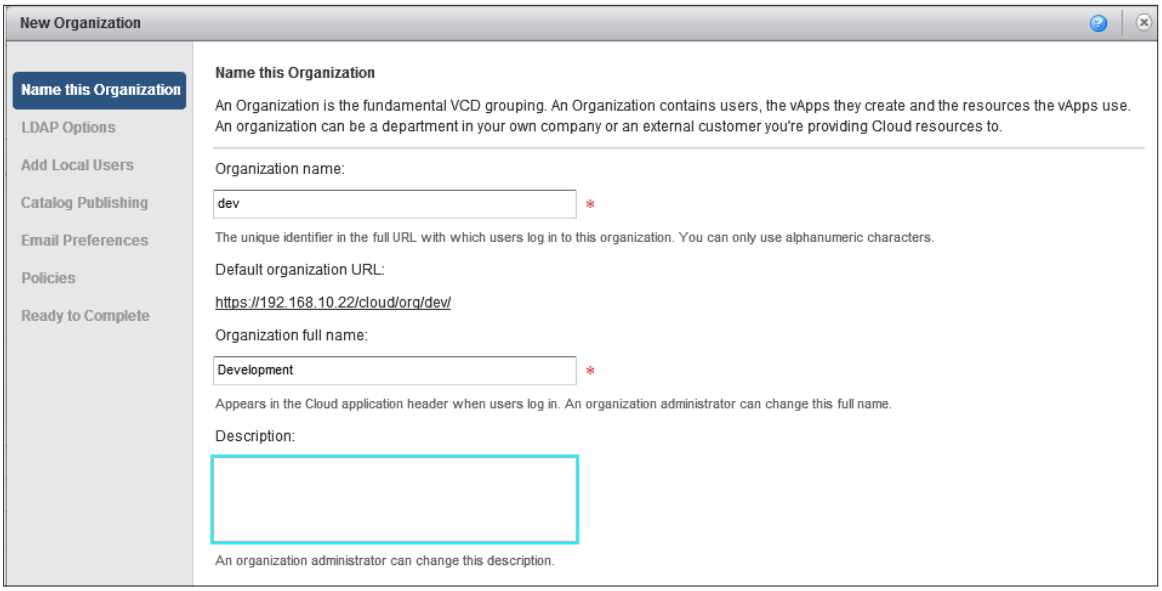
Review the provided summary page and click **Finish** to complete the process of creating an external network.

Create an Organization

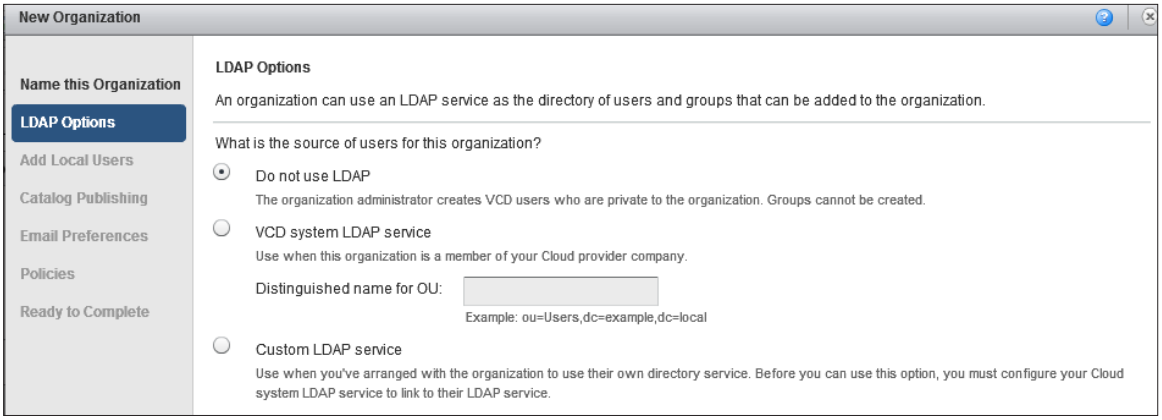
Now it is time to create the organizations to consume the resources previously configured in the provider VDC. Create one organization in this section for a development team. This organization leverages the resources in the provider VDC for the workloads they create.



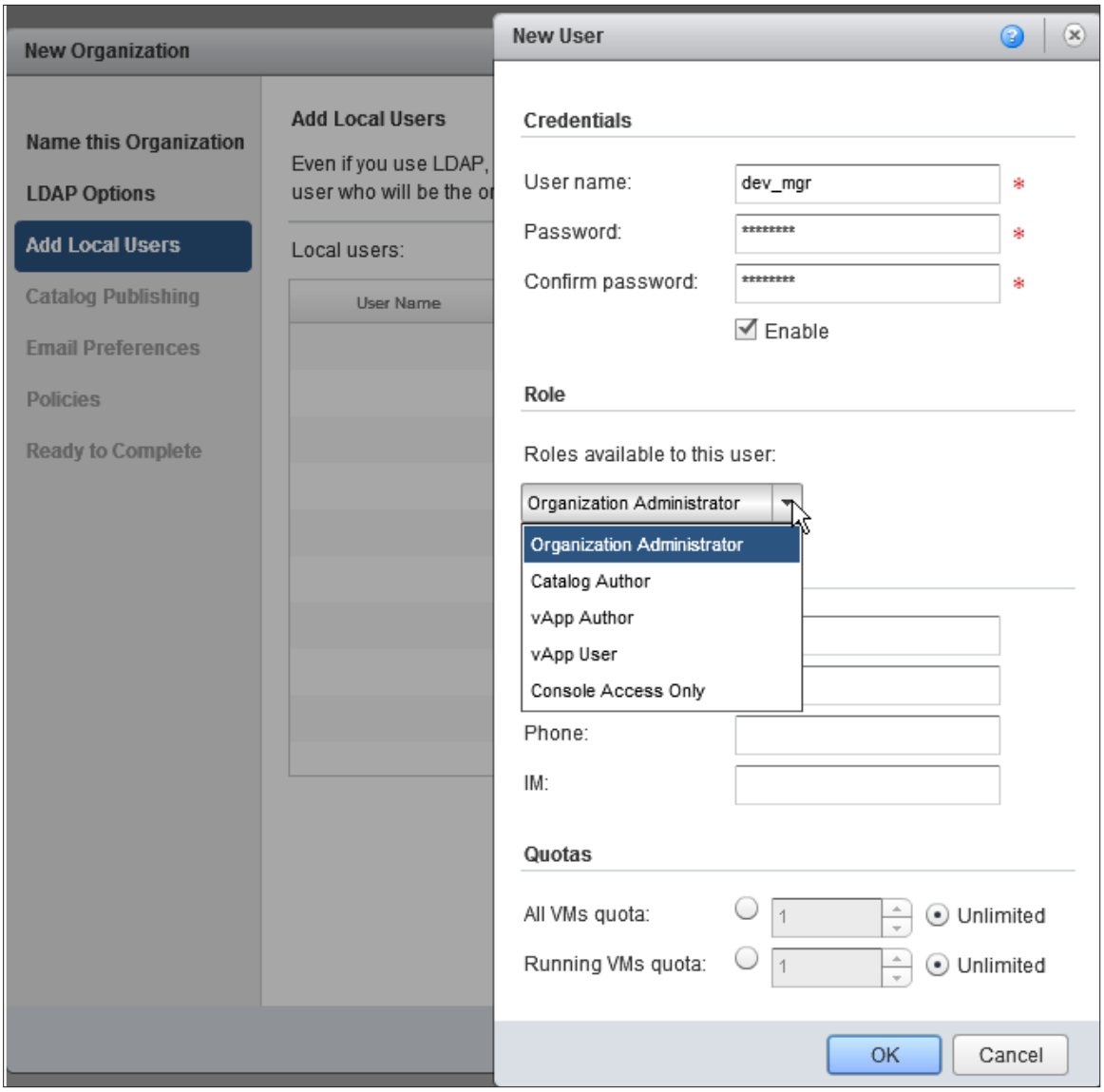
To begin, select **Create a new organization** under **Quick Start** on the **Home** screen.



The first step using the new organization wizard is to name the organization. As you type **dev** for the organization name, the **Default organization URL** is created automatically. This is the URL that users within this organization use to access the vCloud Director portal specific to their organization. Enter the name **Development** for the organization and click **Next** to continue.

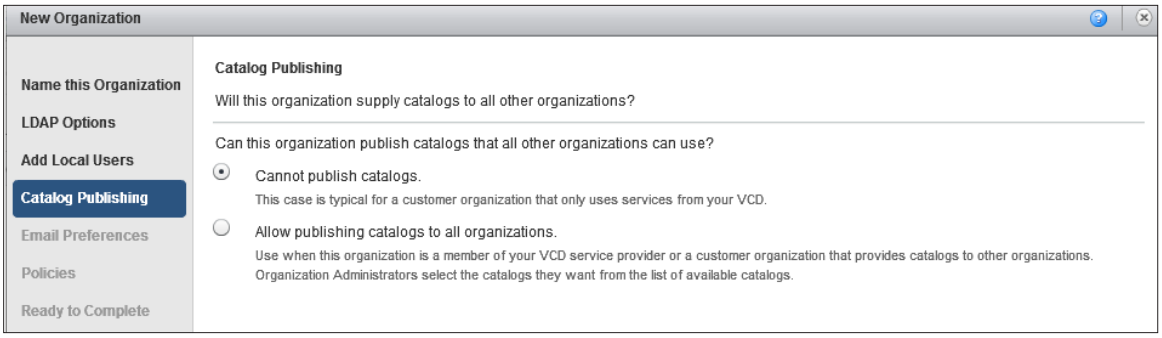


The next step is to define an LDAP service to use for this organization. Although this guide does not use an LDAP service, there are several options available to give administrators flexibility to manage large numbers of users. Click **Next** to continue.



Because we are not configuring LDAP services, we can define users manually by adding local users. Click **Add Local Users** to display a dialog box that enables you to define a local user for this organization. Name the user **dev_mgr** and ensure that this user is associated with the **Organization Administrator** role. This gives the assigned user full access to this organization. Other roles are available by default to provide varying degrees of access for users. A cloud administrator also can create custom roles if necessary.

Click **OK** to close the dialog box. Click **Next** to continue.

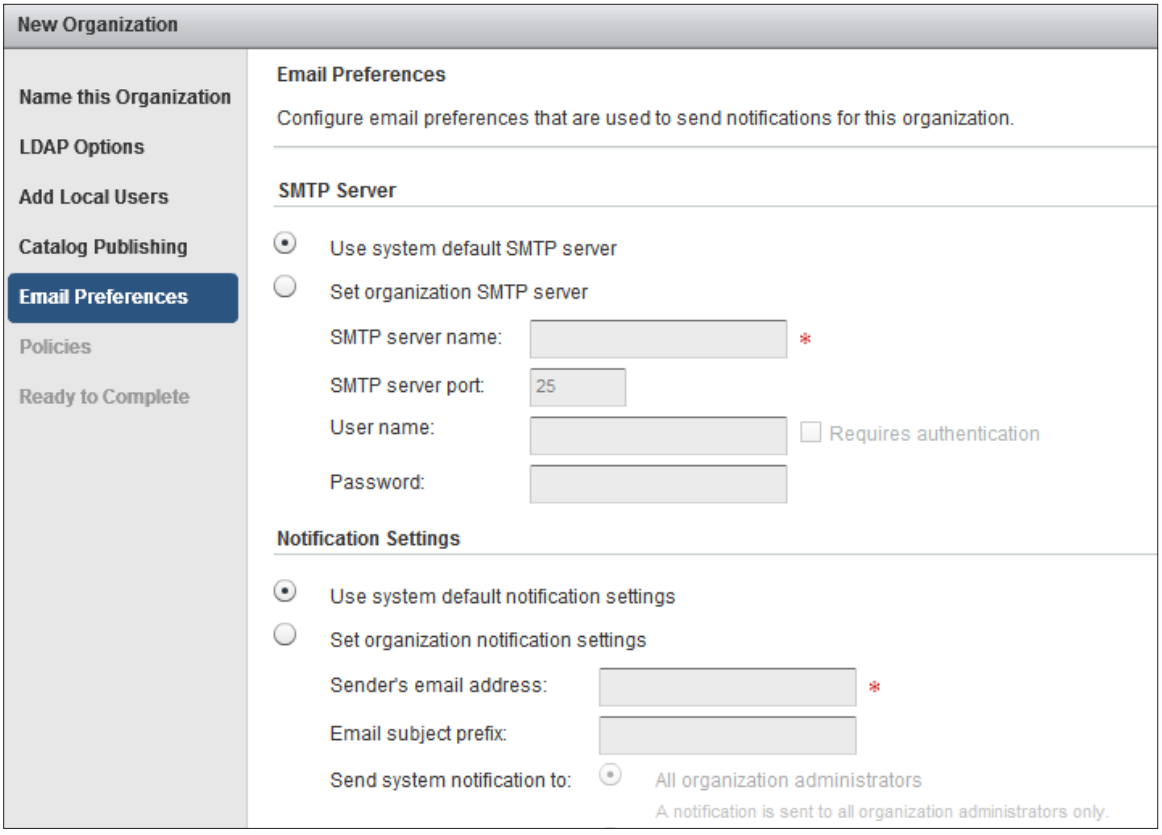


You then can specify whether this organization can share catalogs with other organizations.

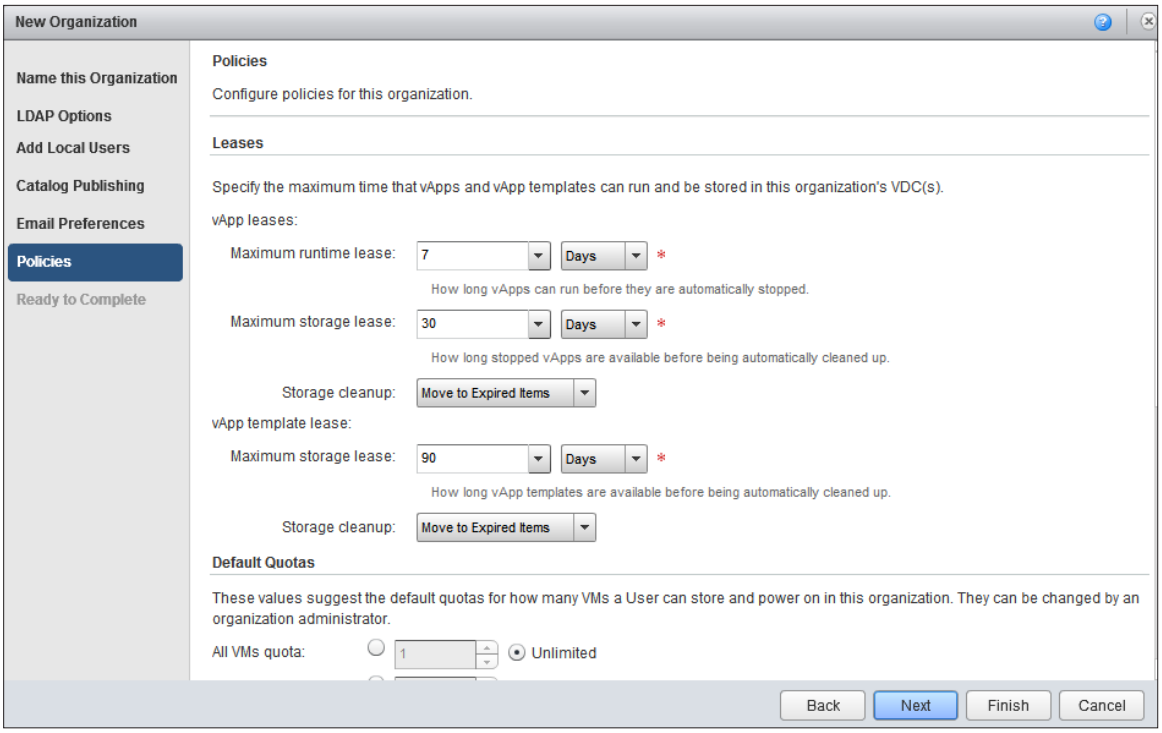
Catalogs are a collection of vApps, vApp templates and media. An organization can create multiple catalogs. For example, an organization might choose to create a catalog of vApps that contain a set of builds for a QA team to test. The same organization might have another catalog containing .iso image files for the OS installation media they use. Different organizations at times might find that they create catalogs containing many of the same items.

For this reason, 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.

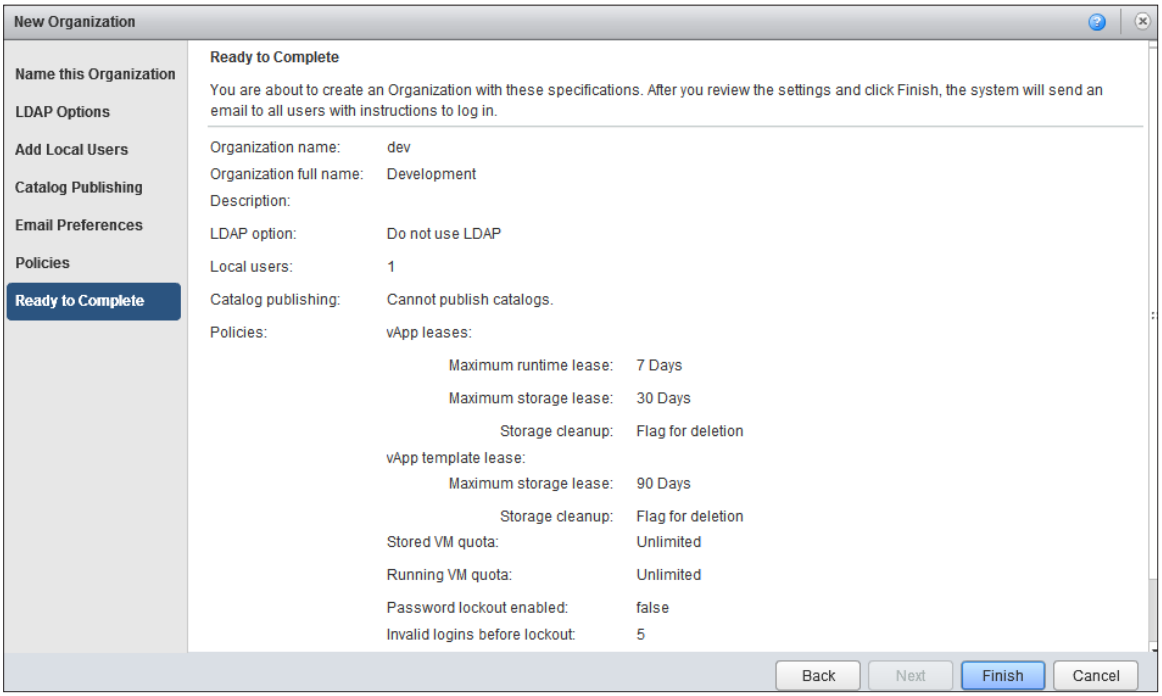
On this screen, you can enable an organization to share its catalogs with other organizations or specify that it cannot. Leave the default setting **Cannot publish catalogs** selected to specify that the organization cannot share a catalog with other organizations. Click **Next** to continue.



The wizard then enables you to configure email settings for this organization. Click **Next** to continue.



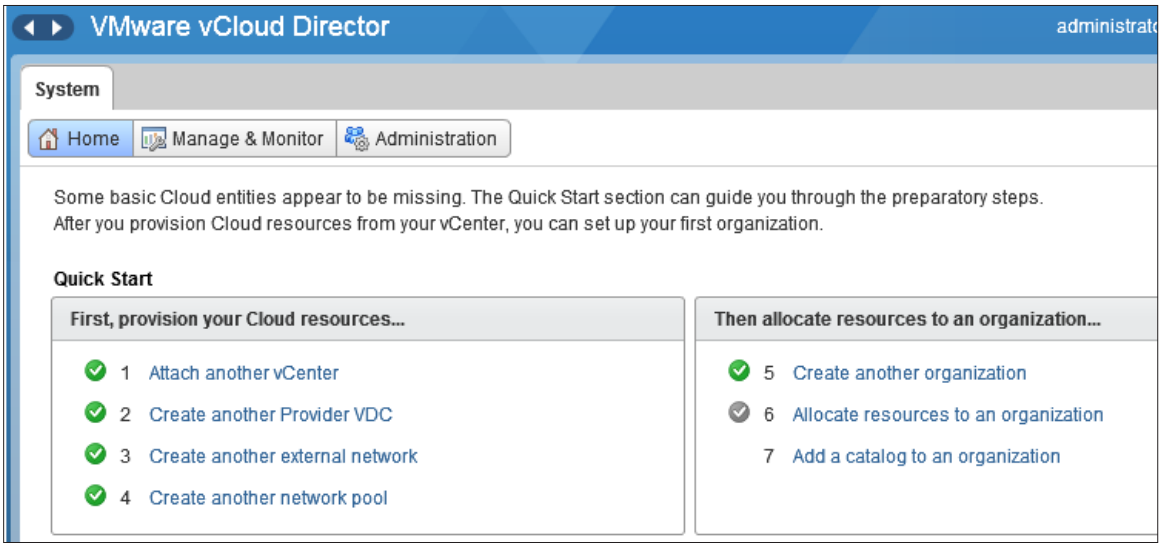
The next step using the wizard enables you to configure a series of policies for the organization. You can define quotas for how many resources the organization can have, specify lease times for the resources, and set password policies and limits for various activities. Leave the default settings for these and click **Next** to continue.



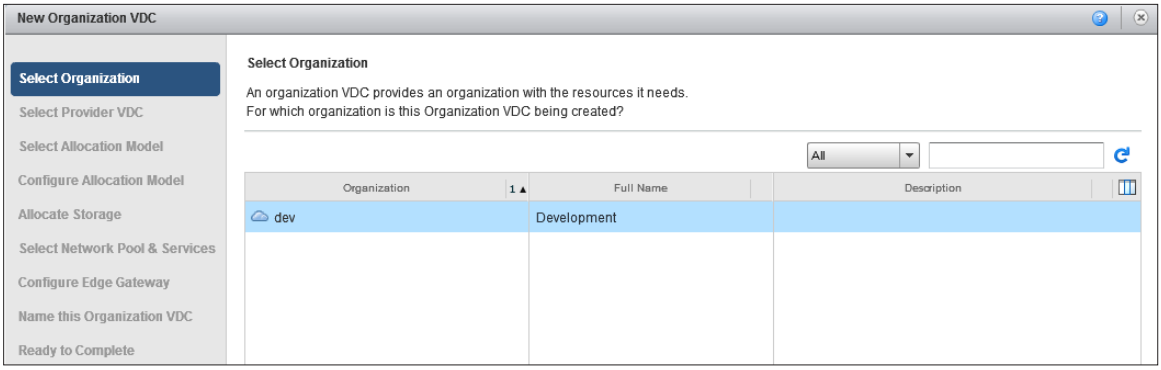
You then are presented with a summary page that enables you to review the information provided. When you are satisfied with the information, click **Finish** to create the organization.

Allocate Organization Resources

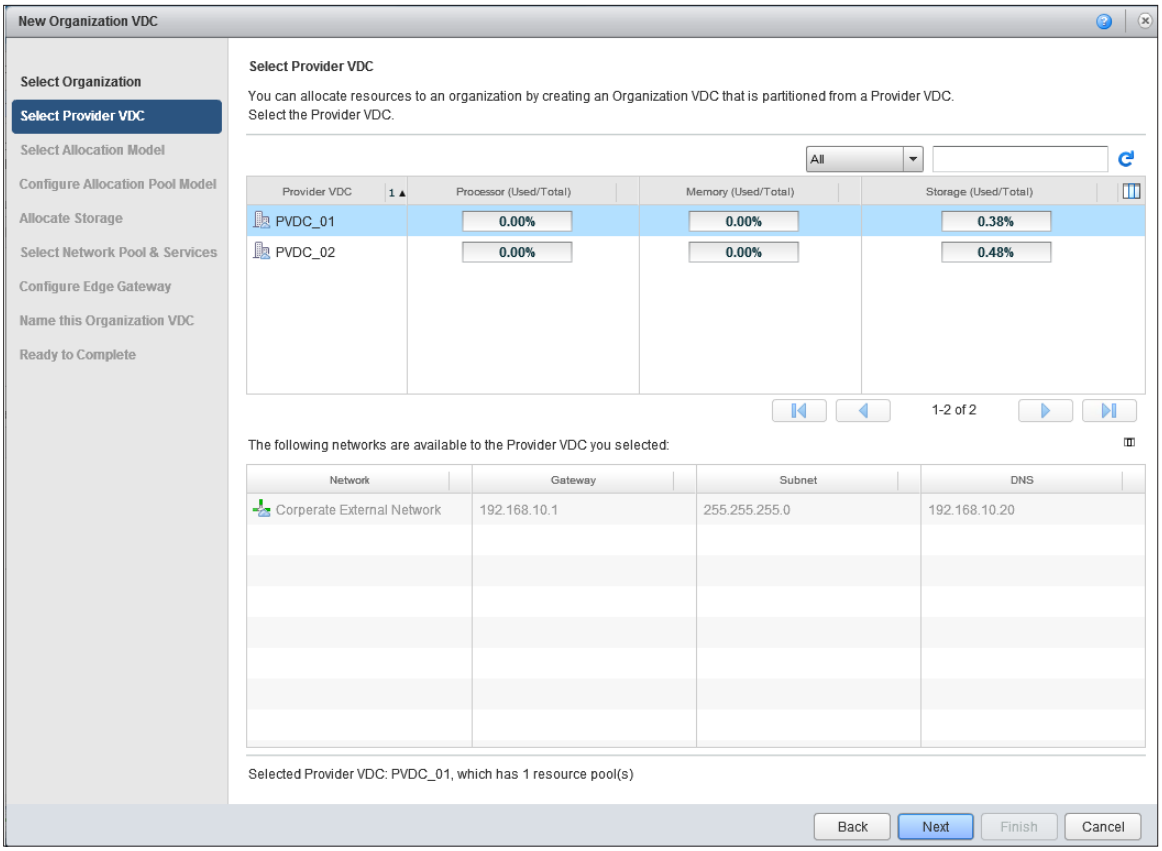
Allocating resources to an organization involves making resources from the provider VDC available to an organization VDC that is associated with the organization.



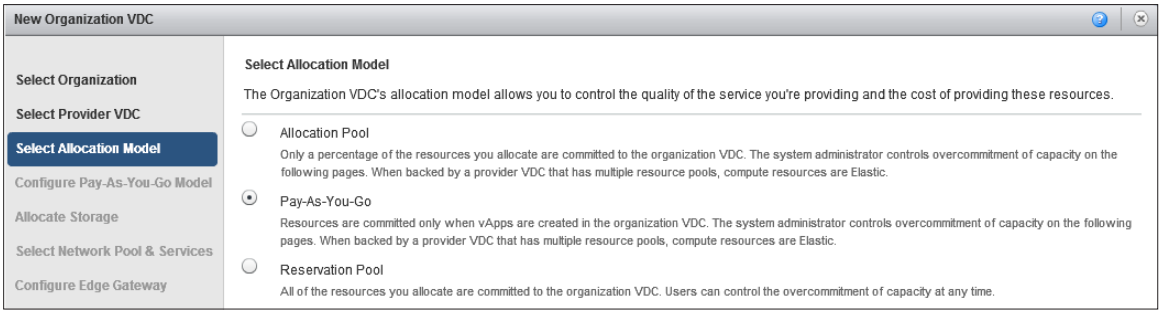
To create an organization VDC, select **Allocate resources to an organization** under **Quick Start** on the **Home** screen.



Associate this organization VDC with the **dev** organization that you created earlier. Click **Next** to continue.



Next, select the provider VDC that the organization VDC will draw its resources from. Select **PVDC_01** and click **Next** to continue.

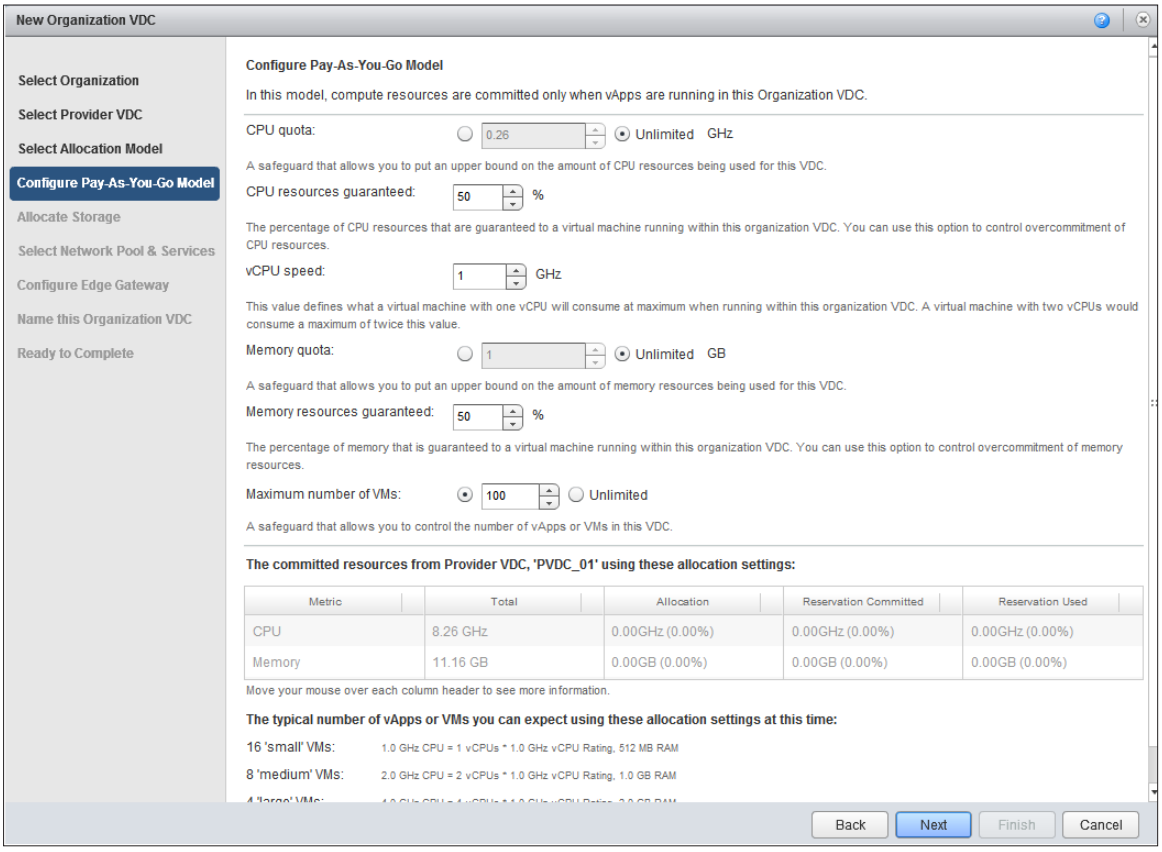


Now select an allocation model to use for this organization VDC. The following three methods are available to control the quality of service and the costs associated with the resources that you will be allocating:

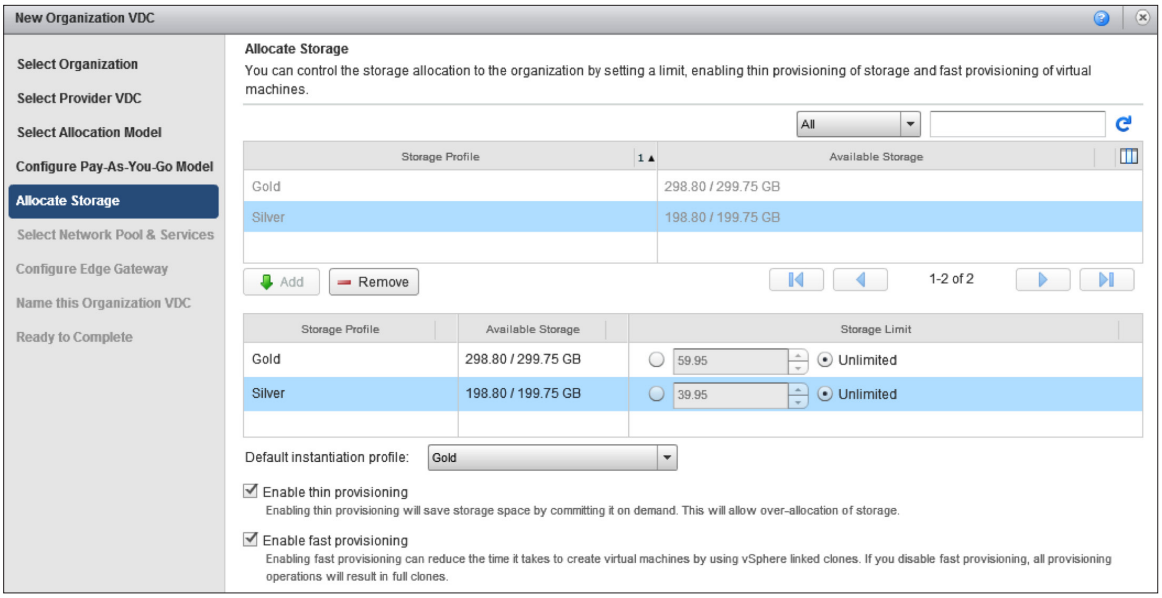
- **Allocation Pool**
  Only a percentage of the resources you allocate is committed to the organization VDC. You can specify the percentage. This enables you (the provider) to overcommit resources across multiple VDCs to different organizations.

- **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. This 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 committed to the organization VDC immediately. In this case, control of overcommitment passes to the users in the organization. They can control overcommitment by specifying reservation, limit and priority settings for individual virtual machines.

In this guide, we use the pay-as-you-go model of resource allocation. Select **Pay-As-You-Go** and click **Next** to continue.



The next step using the wizard gives you the ability to configure the allocation model you selected to match the needs of your environment. With the pay-as-you-go model, you can specify percentages of CPU and memory resources that are guaranteed to the organization. Change **CPU resources guaranteed** and **Memory resources guaranteed** to **50%** to increase the resources guaranteed within this organization. Click **Next** to continue.

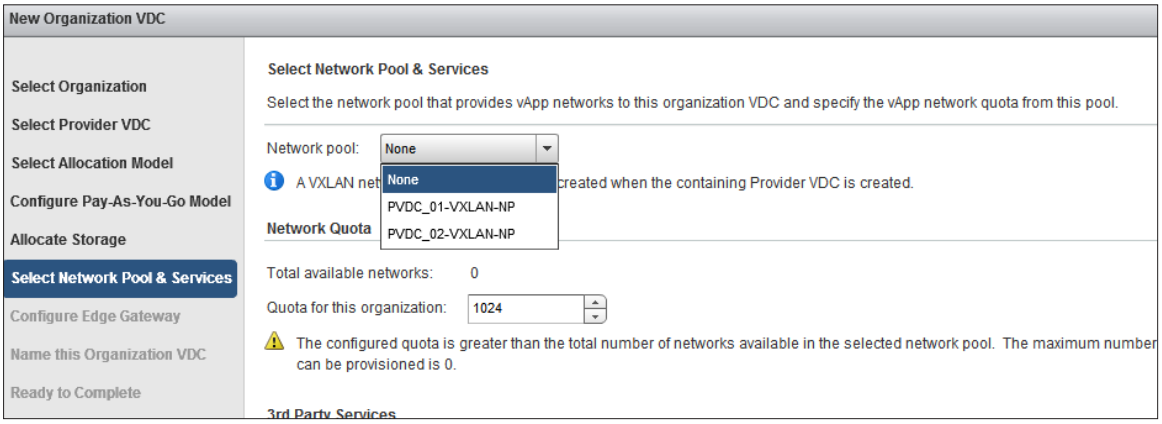


After configuring the selected allocation model, you must allocate storage to the organization VDC. In this example, we select the **PVDC_01** provider VDC that we created earlier. This provider VDC contains only two tiers of storage as defined by the **Gold** and **Silver** storage profiles. To provide these same tiers of storage to the organization, select them and click **Add**.

It is not necessary to allocate all the tiers of storage present within a provider VDC to an organization VDC. This enables you to have a single provider VDC that can supply different tiers of storage to several organizations.

A default instantiation profile can also be defined for the organization. When a new vApp is created within an organization, the virtual machines that are contained within that vApp will be placed on the storage profile by default. If necessary, the user can override this.

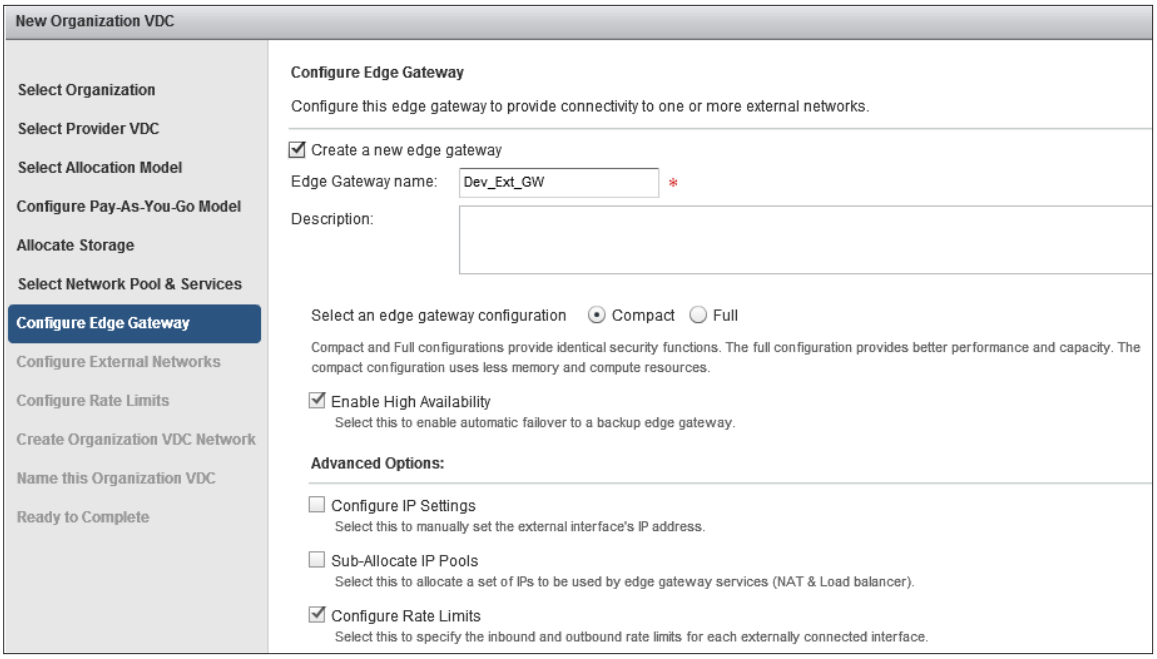
Check the **Enable thin provisioning** and **Enable fast provisioning** boxes. Click **Next** to continue.



The next step enables you to select the network pool and services available to this organization VDC. As mentioned, vCloud Director automatically created a network pool previously when you created the provider VDCs. Select the network pool **PVDC_01-VXLAN-NP** to select the network pool created for the PVDC_01 provider VDC.

With the settings provided in this guide, there are 100,000 networks that can be defined. If you choose to set a quota, you can also do that here.

Click **Next** to continue.



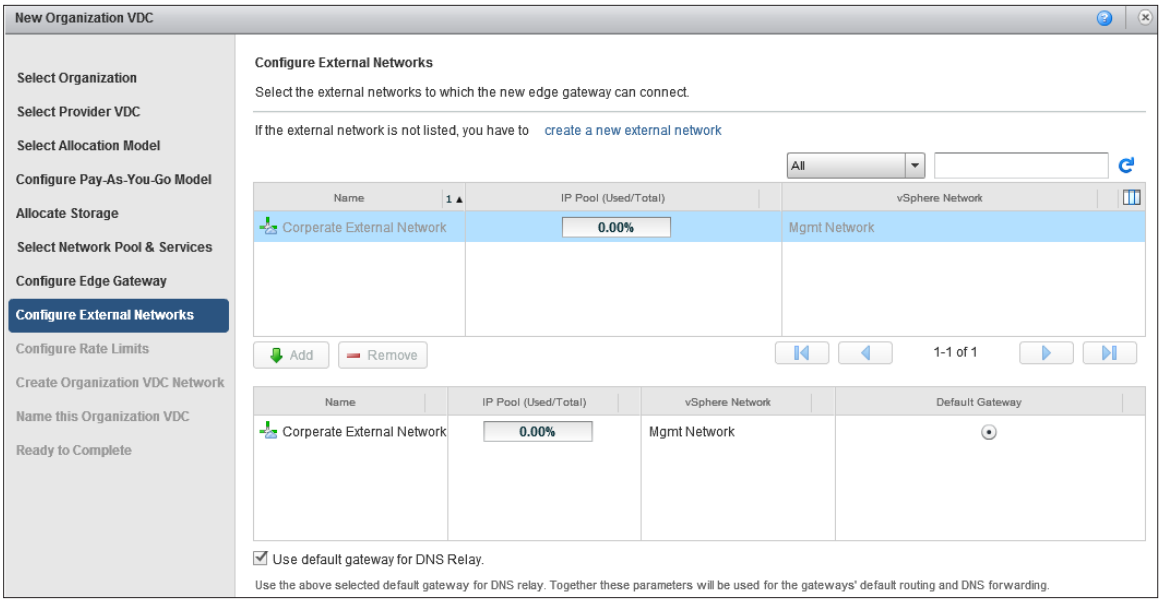
The next step offers the option to create an **Edge Gateway** for this organization. Select the **Create a new edge gateway** check box. The configuration options for the edge gateway are then displayed. Provide a name for the edge gateway and select a configuration model for it.

There are two configuration models: full and compact. There is no difference in functionality between the two. The difference is in the performance they provide. Select the compact model for now. If you find you need better performance, you can easily upgrade to the full model later.

Select the **Enable High Availability** check box for the edge gateway. This creates a secondary edge gateway that will instantly provide services in the event that the primary edge gateway device fails.

There are also some advanced options that you can use to manually set the external IP address of the edge gateway, to suballocate IP pools, and to configure rate limits on the inbound and outbound interfaces of the edge gateway.

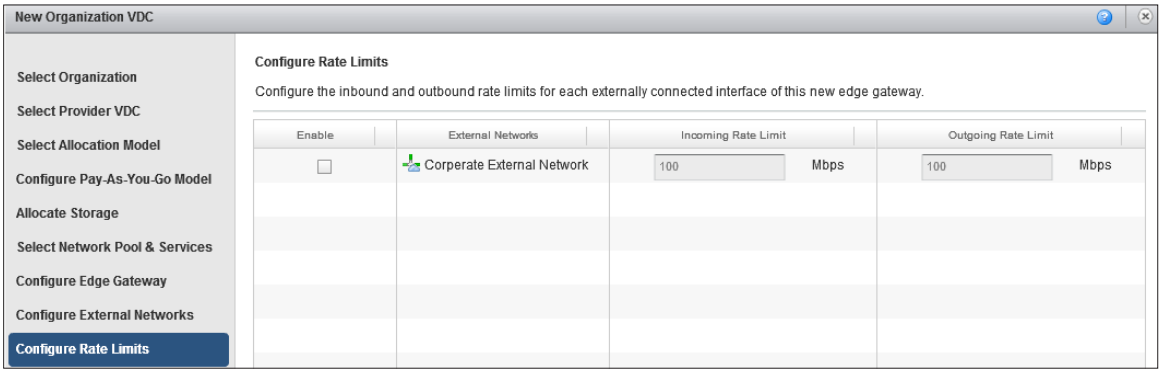
Select the **Configure Rate Limits** check box. Click **Next** to continue.



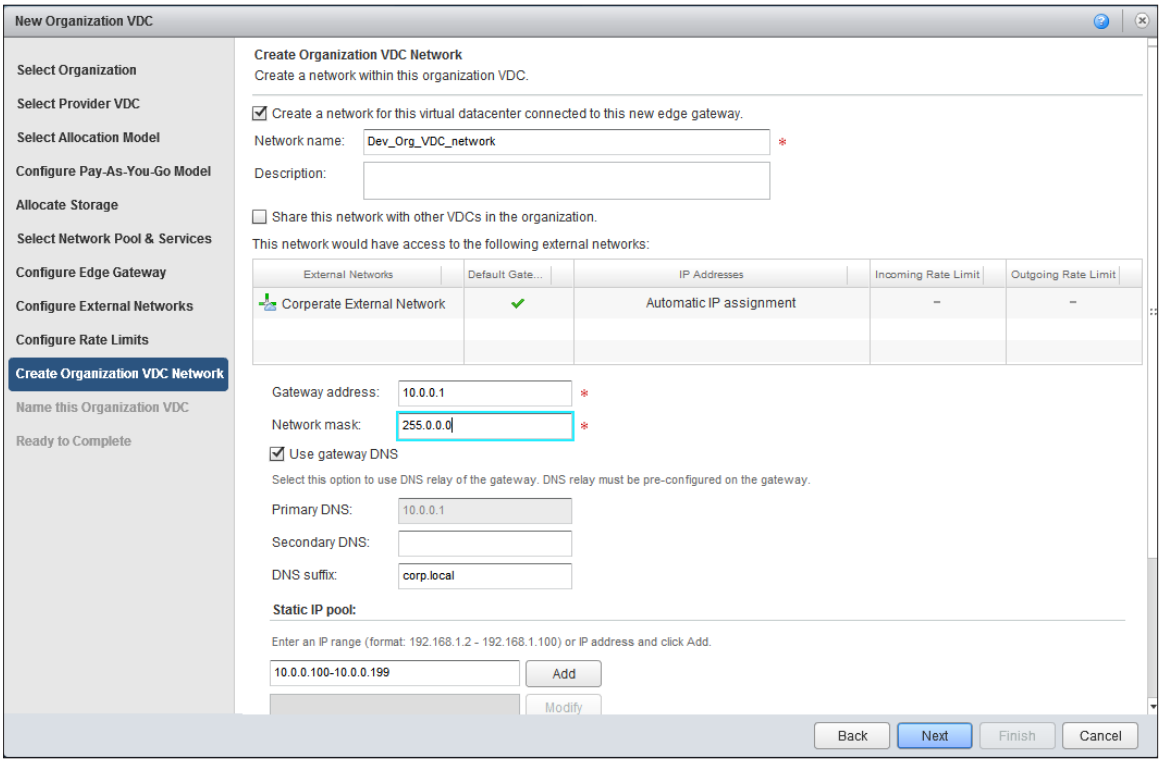
To add the external network that you configured earlier to the organization VDC, select it and click **Add**.

vCloud Director 5.1 has the ability to use the edge gateway as a DNS Relay. This creates a level of abstraction between the organization and the external networks. Selecting this option enables virtual machines created within the organization to be pointed to the edge gateway to resolve DNS queries. Any changes to the external DNS configuration will not require a reconfiguration of the DNS settings of the virtual machines.

Select the **Use default gateway for DNS Relay** check box to enable the DNS Relay feature. Click **Next** to continue.

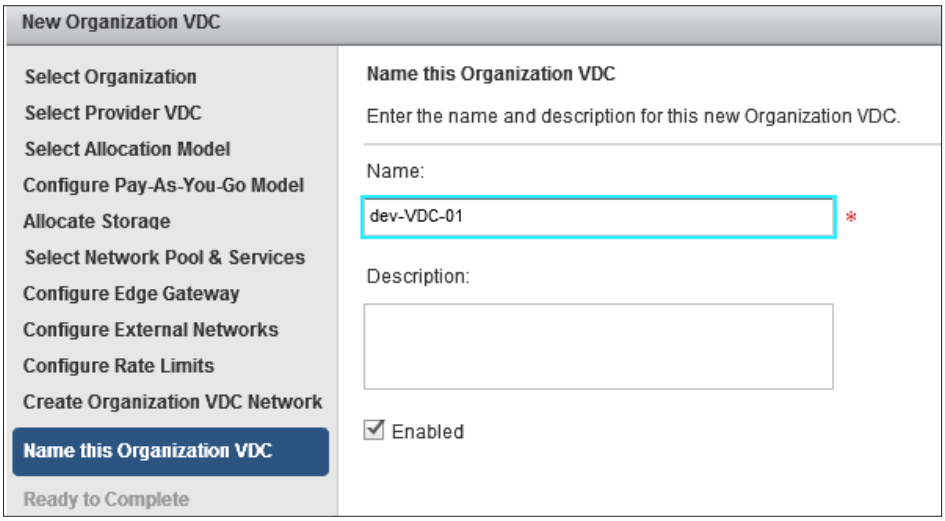


We previously selected the ability to configure limits on the inbound and outbound traffic. The wizard now enables us to configure those limits. Select the check box to enable the rate limits and specify the appropriate values. Click **Next** to continue.



The wizard enables you to create an organization VDC network. Users within the organization can connect to this network to enable communication for their vApps. Select the **Create Organization VDC Network** option. In the text boxes provided, enter the name for the network, the gateway address and the netmask to be used. Define the DNS suffix, if required, and a static network pool to use for this network.

Click **Next** to continue.

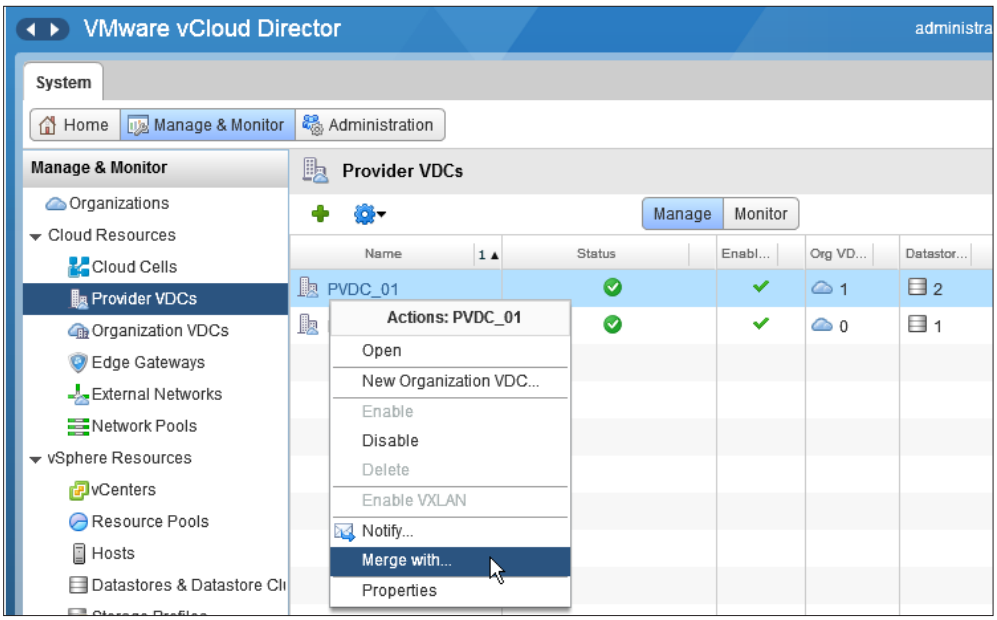


Next, provide a name for the organization VDC and select the **Enabled** check box. Click **Next** to continue to the summary page.

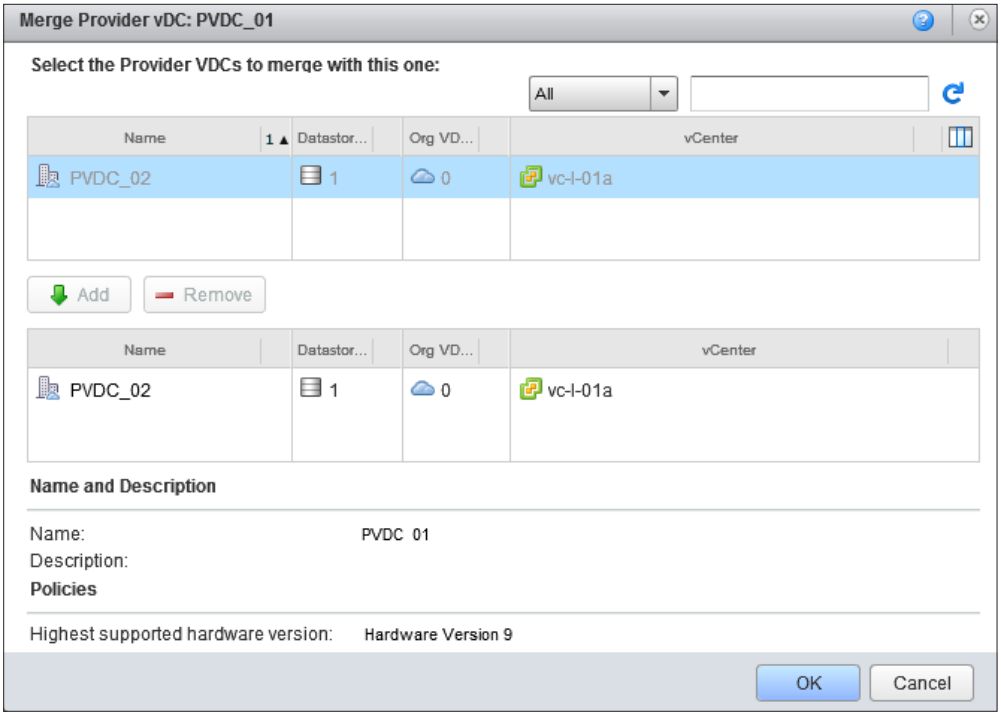
Review the information provided. Click **Finish** to complete the process of creating the organization VDC.

Merging Provider VDCs

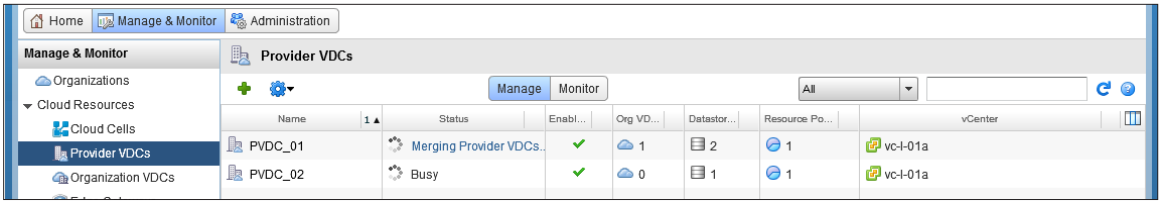
vCloud Director 5.1 has the ability to merge provider VDCs. This is helpful if you created multiple provider VDCs and want to consolidate resources. To demonstrate this capability, we now will merge the two provider VDCs that we created earlier into a single one.



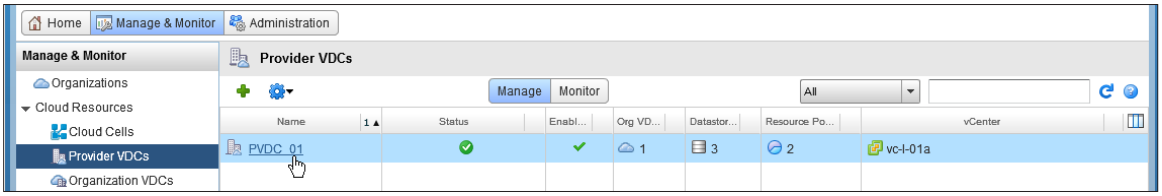
Click the **Manage & Monitor** tab. Then select **Provider VDCs** in the left-hand pane. Right-click **PVDC_01** and select the **Merge with...** option.



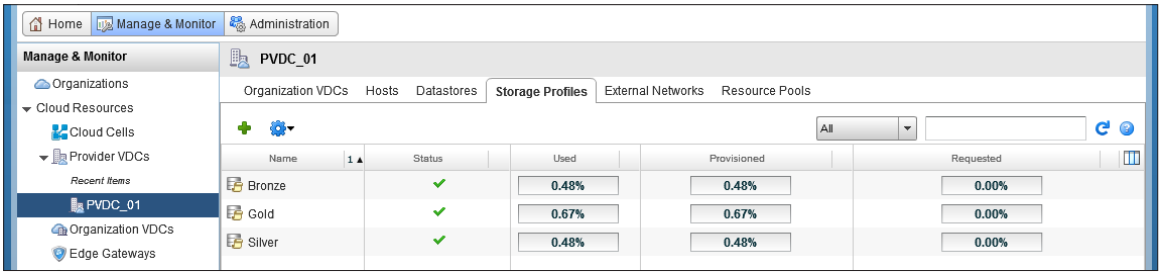
This brings up a screen where you can select the provider VDC that you want to merge with. Select **PVDC_02** and click **Add**. Click **OK** to start the merge.



You will see the status of the merge operation progress.



After it completes, you will have one provider VDC listed. **PVDC_01** now contains all three datastores. Click the name of the provider VDC for more details.



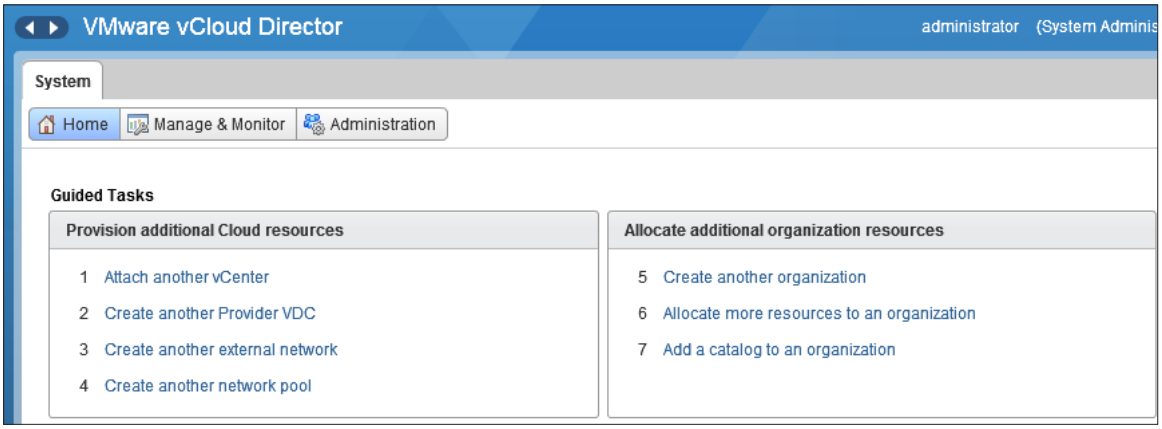
Click the **Storage Profiles** tab. You will see that the provider VDC now contains all three previously defined storage profiles. Click the **Resource Pools** tab. You will see that both clusters also have been added to the provider VDC.

Developing Service Offerings

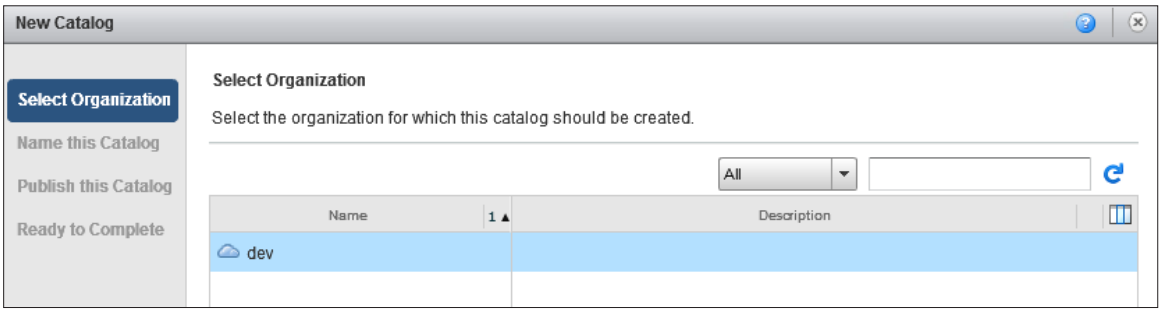
After the organizations have been created, you can also create catalogs for the content that can be readily consumed by members of the organizations. In this section, you will configure a vApp and learn how to make a vApp template as well as how to perform other tasks to help populate your private cloud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

Creating a Catalog

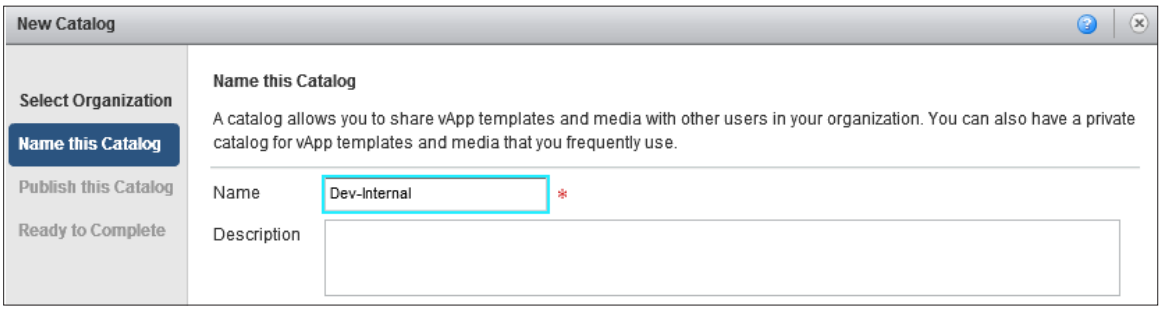
A catalog is a collection of vApps, vApp templates and media that an organization uses. In this guide, we will create a catalog for the development organization.



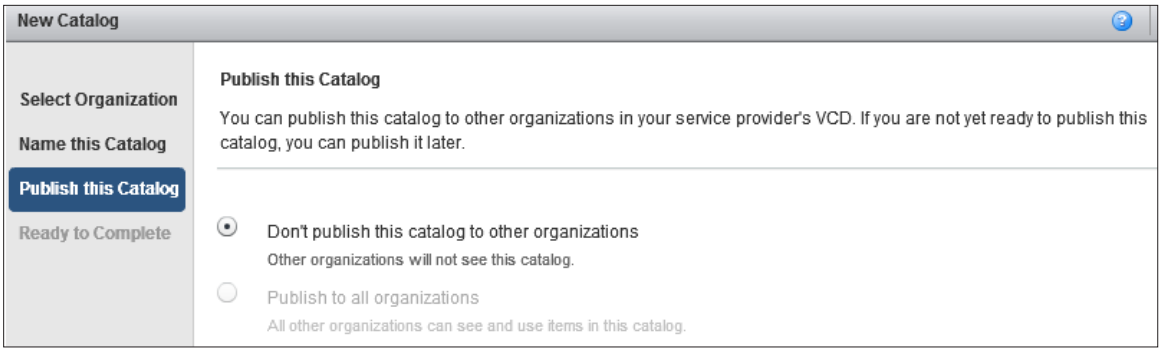
To create a catalog, select the **Add a catalog to an organization** option under **Guided Tasks** on the **Home** screen.



Select the **dev** organization. Click **Next** to continue.



Provide a name and a description for the catalog. Click **Next** to continue.

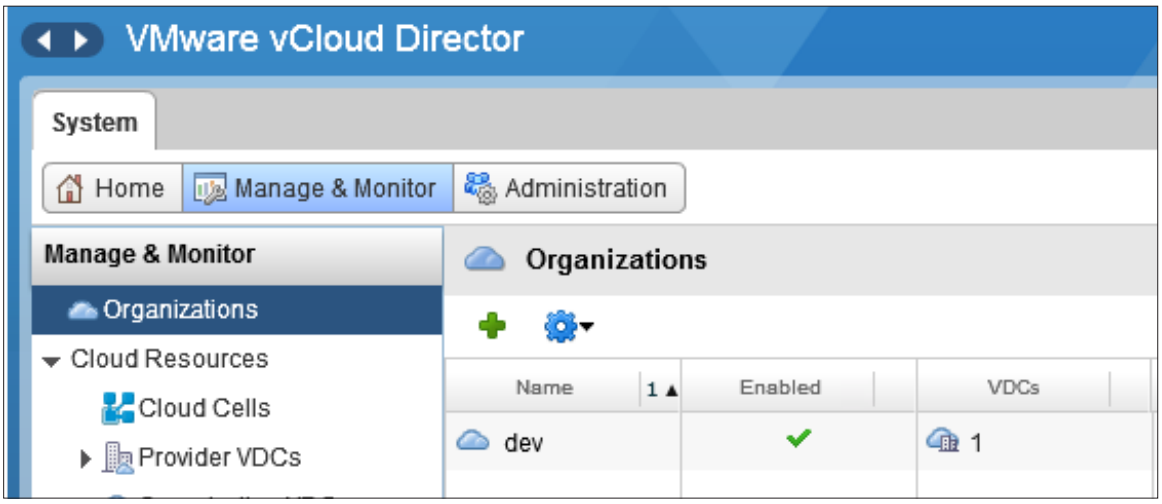


Because we are creating the catalog as the cloud administrator, we have the option to share the catalog with other organizations. Leave the default selected to restrict this catalog to only the dev organization. Click **Next** to continue.

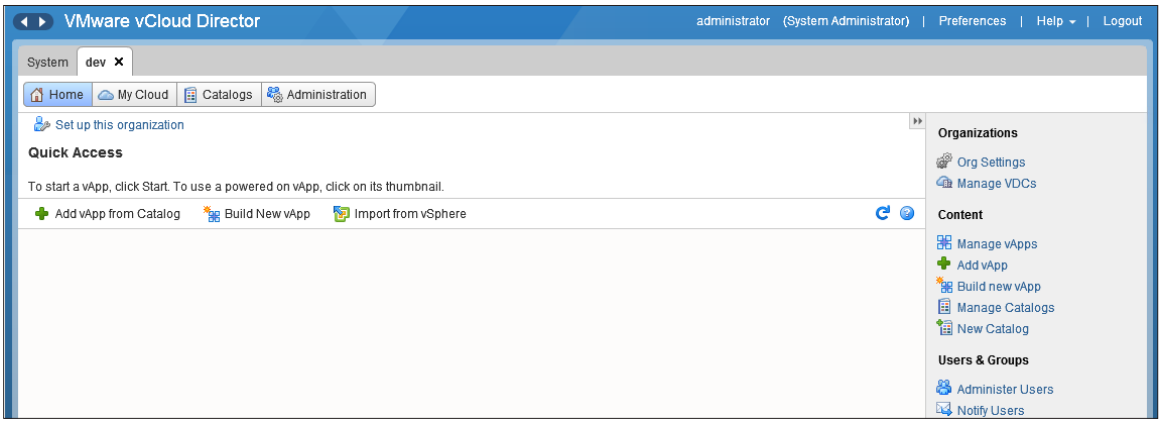
Review the summary information and click **Finish** to complete the process of creating the catalog.

Importing Media

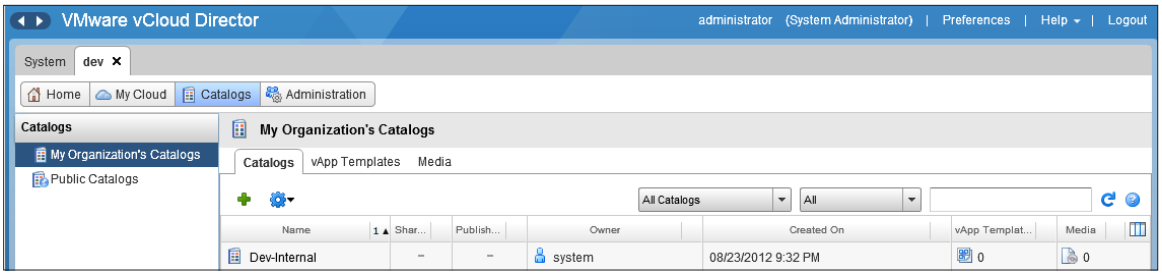
After a catalog has been created, we can add items to it so users can consume them. To start, add a media file.



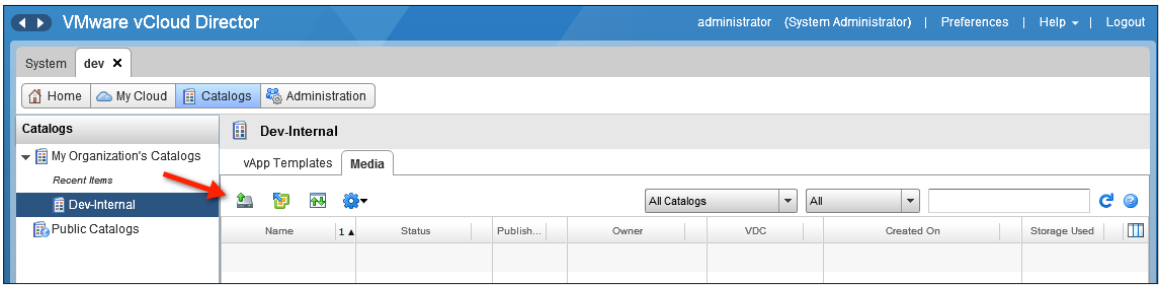
Click the **Manage & Monitor** tab. Select **Organizations** in the left-hand pane. Click the **dev** organization to access it.



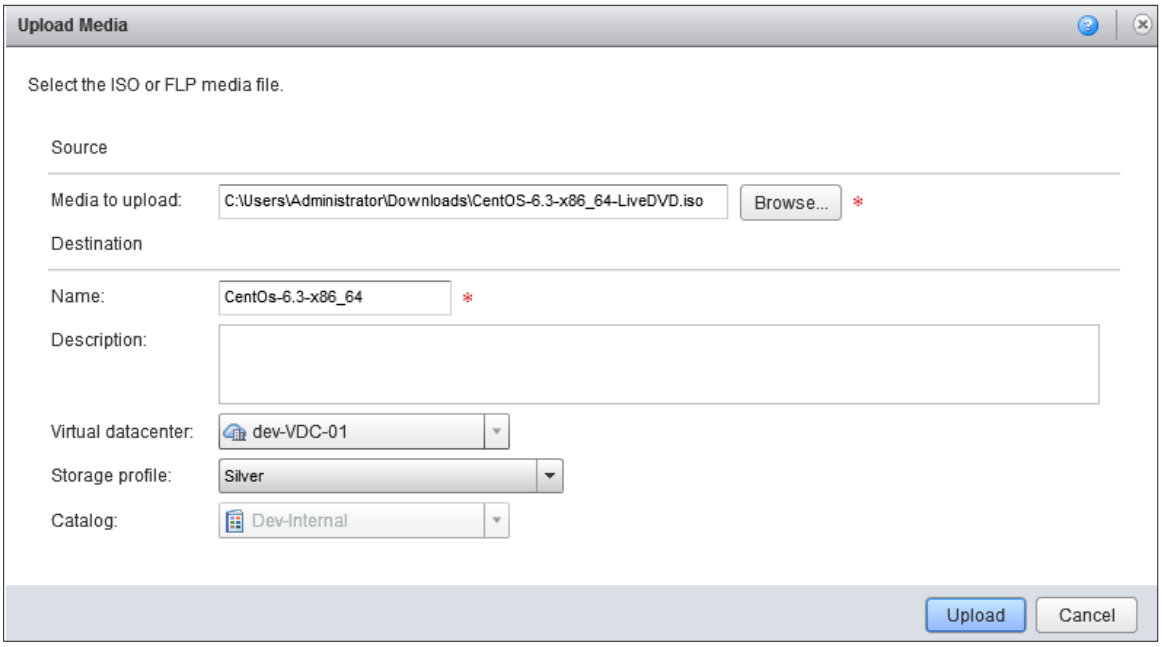
This opens a new tab that shows the **dev** organization as it would look to a user accessing the organization URL.



Click the **Catalogs** tab to access the catalogs available to this organization. You will see the catalog you created listed in the table. Click **Dev-Internal** to display the contents of that catalog.



Click **Upload** to upload a media file. This process requires that Java be installed for the Web browser you are using. If it is detected that Java must be installed, you will be redirected to java.com to download the appropriate package.

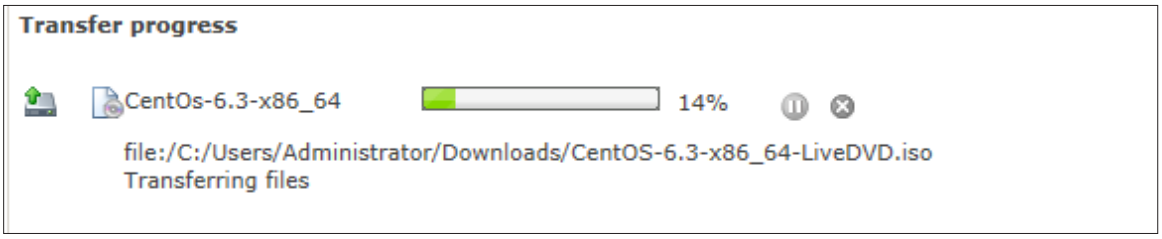


A window is displayed that enables you to specify the media to be uploaded. In this guide, we are uploading an .iso image of CentOS that we will use later when creating a vApp.

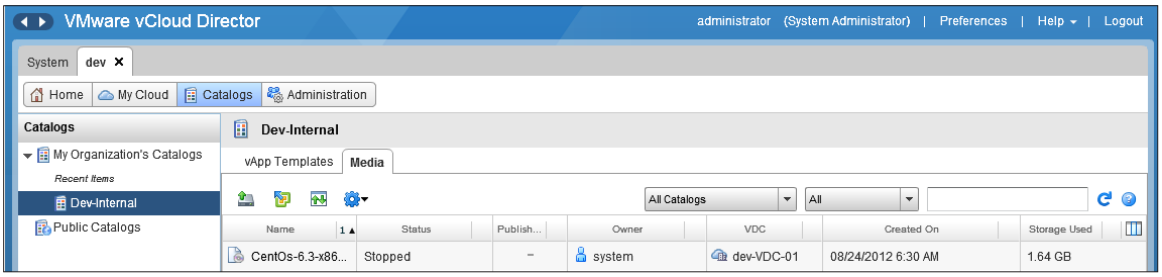
Select the location of the media file and provide a name that will be listed in the catalog for this media.

Because there is only one organization VDC for this organization, you cannot change the one where the media is to be stored. In environments that contain multiple organization VDCs, you can specify location.

You can select a storage profile that will be used to store the media. This enables you to locate your media on a lower tier of storage and reserve the higher tiers for the workloads that will be running in your cloud. Select the **Silver** storage profile and click **Upload** to continue.



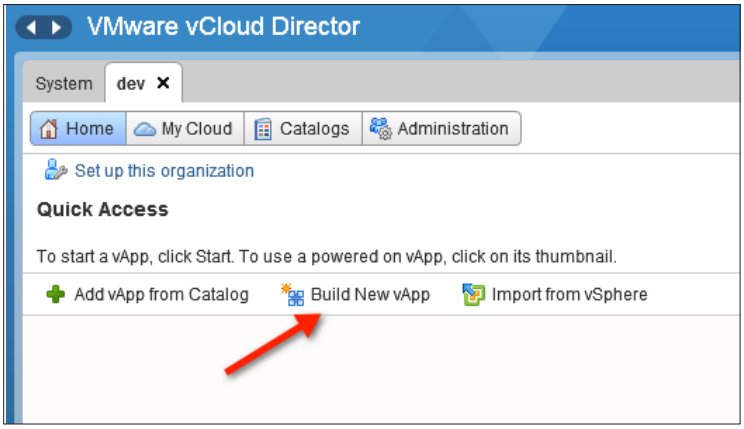
A pop-up window will appear that will display the progress of your upload. Wait until it completes successfully.



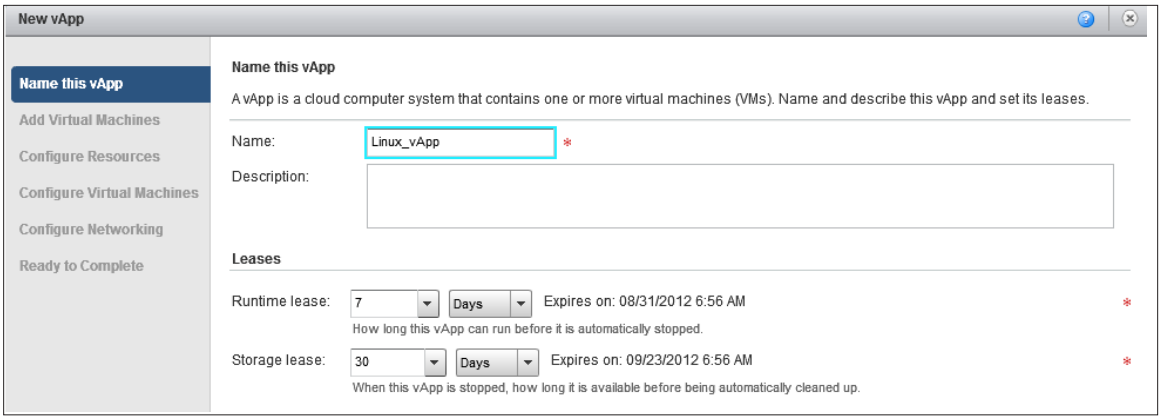
When the import function is complete, you will see the .iso image listed in the catalog.

Building a vApp

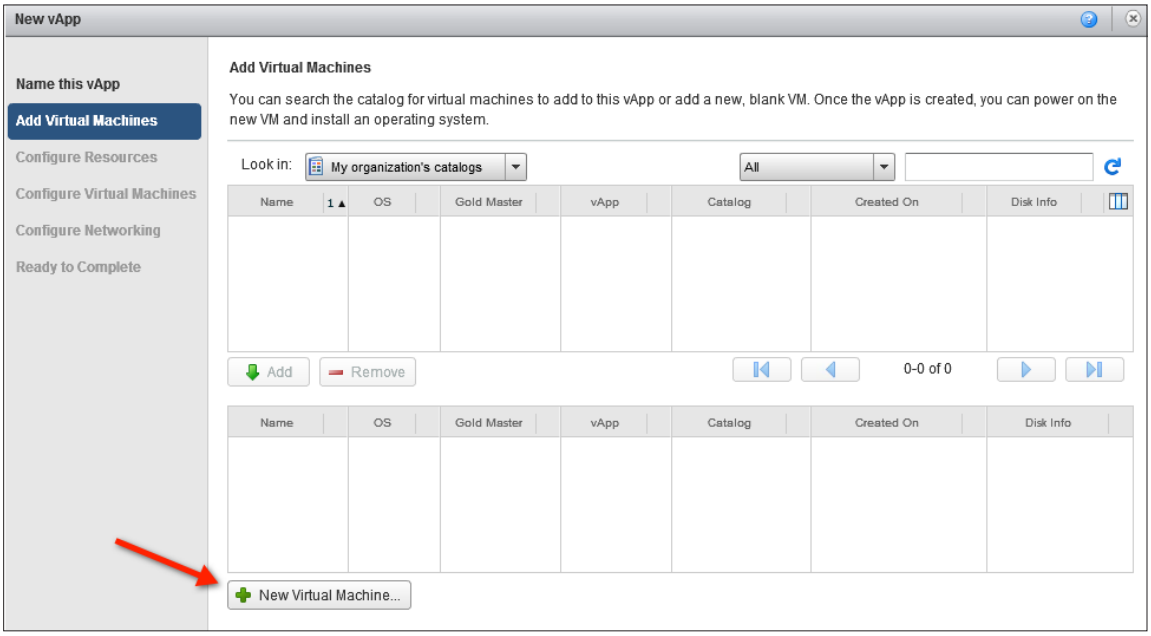
Now we are ready to build our first vApp. A vApp is a collection of one or more virtual machines that run within an organization.



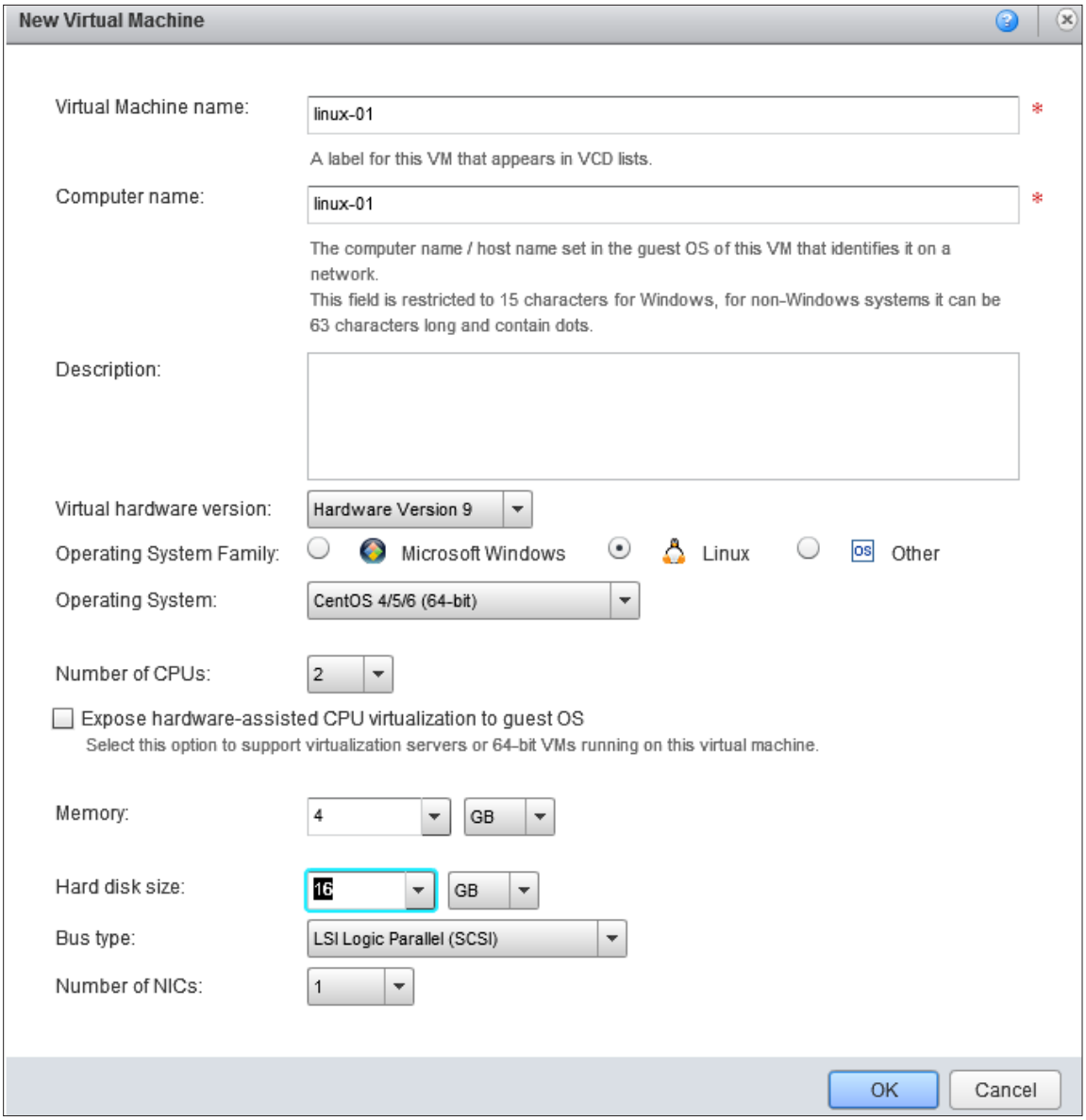
On the **Home** page of the **dev** organization, click the **Build New vApp** option.



Specify the name of the vApp. You can also modify the lease times for this vApp, but you cannot exceed the lease time specified earlier for the organization. Click **Next** to continue.

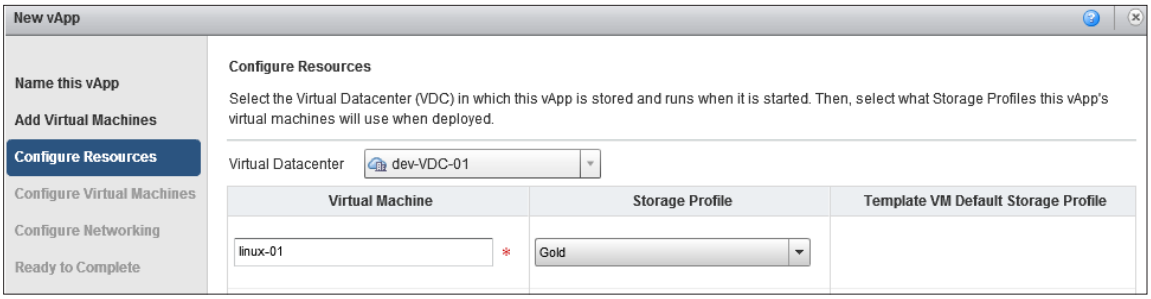


On the next page, we can select a virtual machine template from a catalog to include within this vApp. Because we just created the catalog, it has no templates in it yet. Click **New Virtual Machine**.



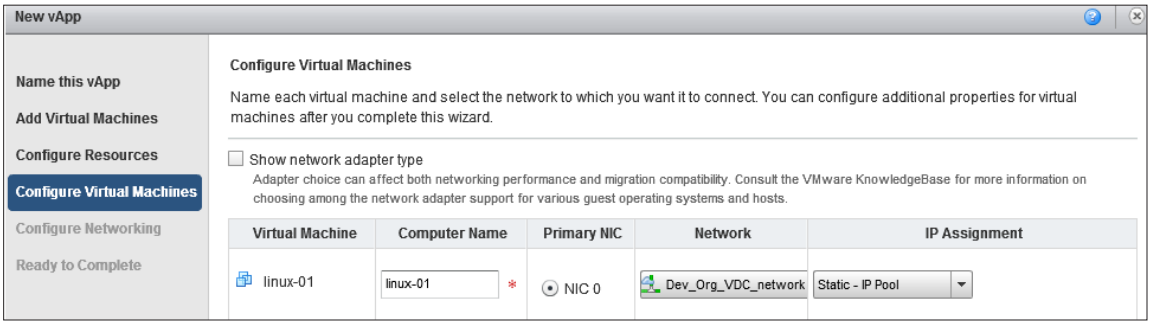
On this page, you can specify the attributes to be used for this virtual machine. Define the name of the virtual machine and specify the other options as needed. Because we already have uploaded a LiveCD CentOS .iso image into our catalog, we will use this. This requires setting the **Operating System Family** to **Linux** and the **Operating System** to a value for **CentOS**.

Click **OK** to close this window. Click **Next** to continue.

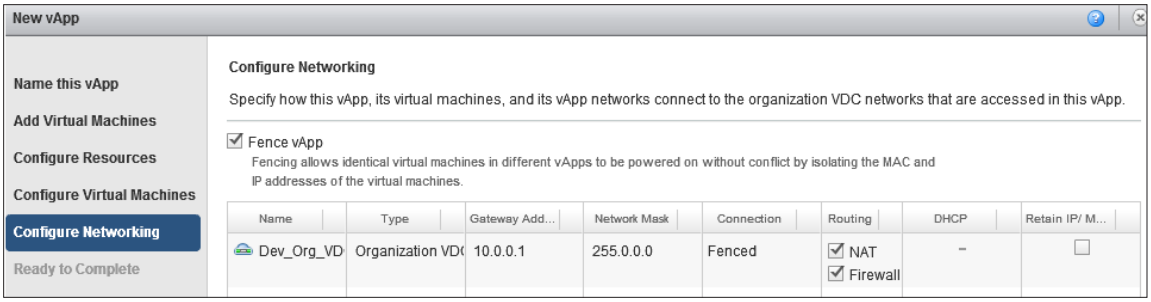


Specify the virtual machine name and the storage profile that it will use.

Click **Next** to continue.



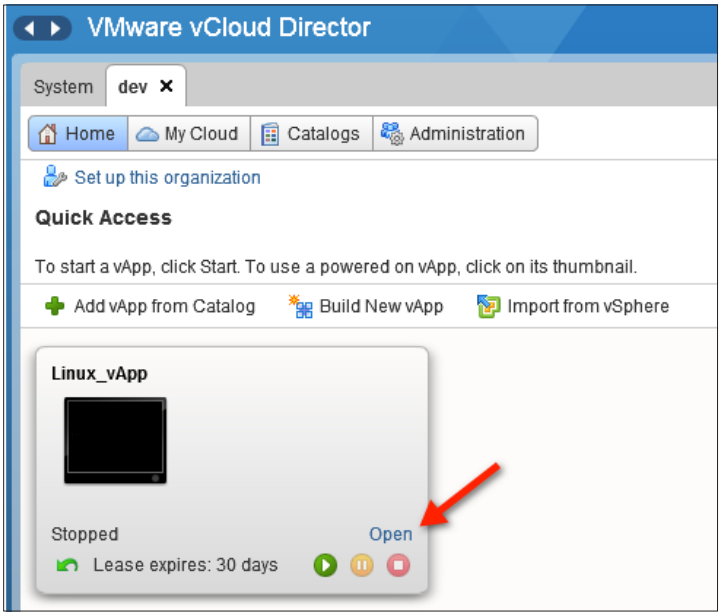
On the next page, you can define the network rail to attach the NIC of the virtual machine to. Select the organization VDC network that you created earlier. You can also define how the virtual machine will obtain an IP address. Set this to **Static – IP Pool,** which you defined for the organization VDC network created earlier. Click **Next** to continue.



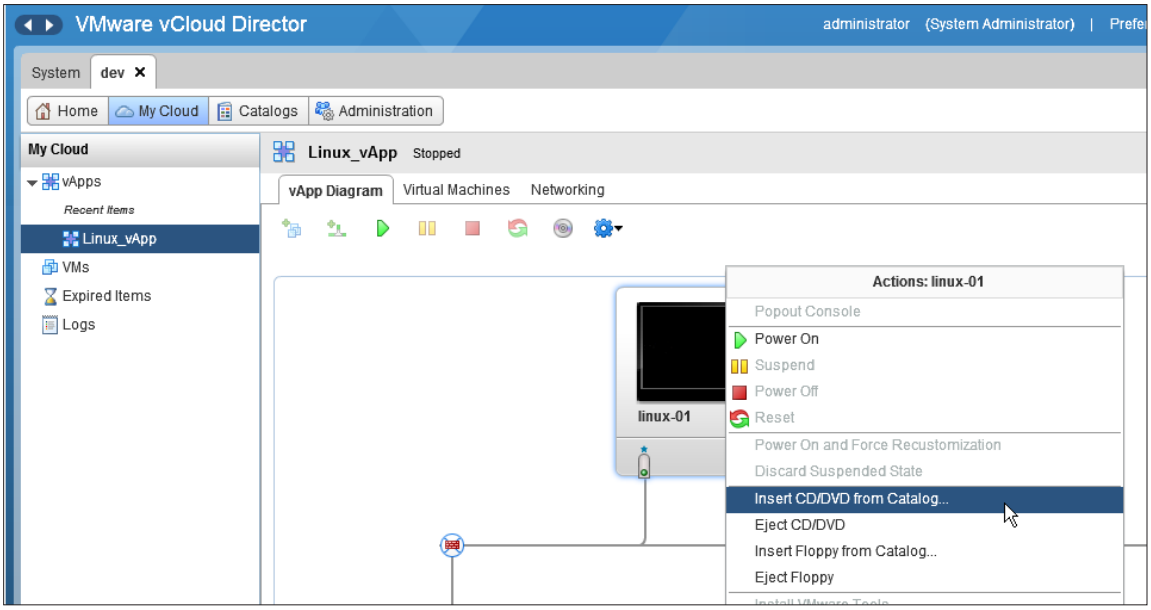
The wizard then enables you to configure the network settings for the vApp. Select the **Fence vApp** option. This enables multiple virtual machines in various vApps to be powered on without conflict by isolating the IP and MAC addresses of the virtual machines.

After selecting this option, you will notice that the routing column enables you to effect services such as Network Address Translation (NAT) and firewall.

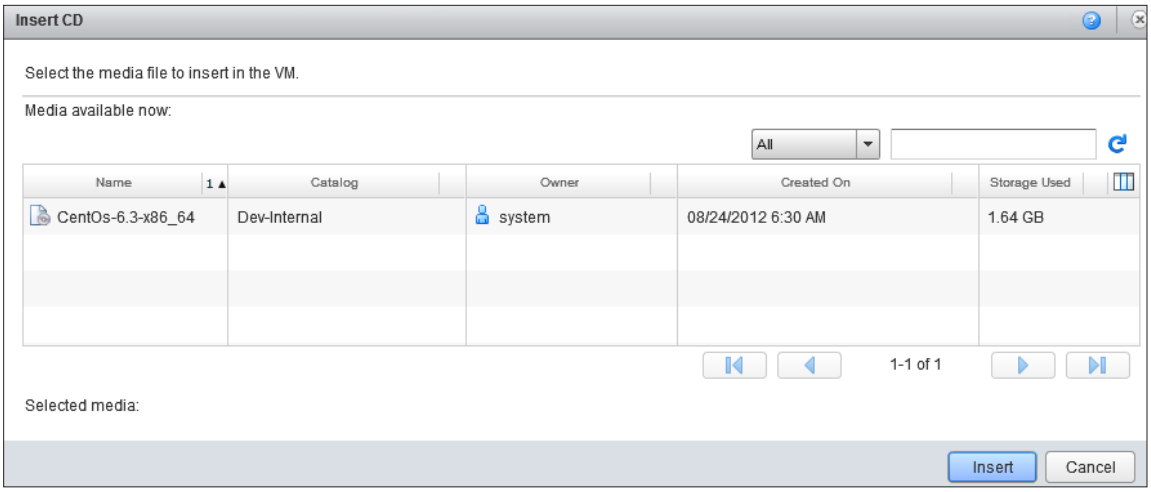
Click **Next** to continue to the summary page. Verify the information and click **Finish** to complete the wizard and create the vApp.



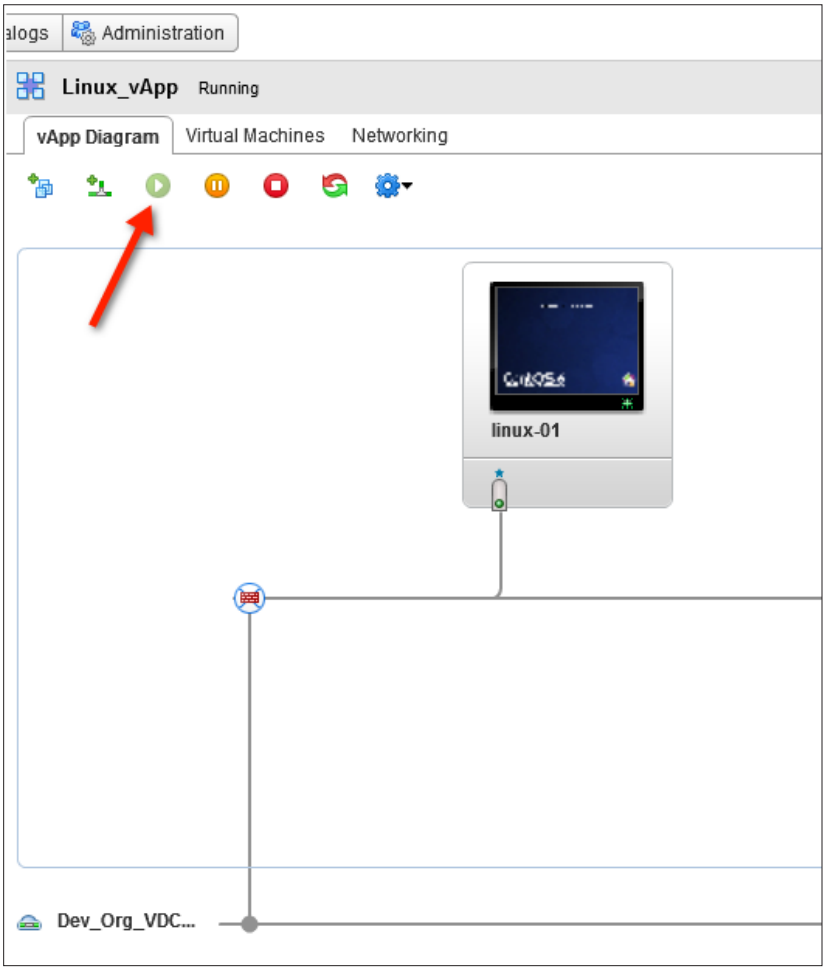
After the vApp has been created, you will see that the status is **Stopped**. Click the **Open** link to drill into the vApp.



On this screen, you will see a graphical representation of the vApp network configuration. Right-click the virtual machine. An action menu is displayed. Select the **Insert CD/DVD from Catalog...** option. This enables us to use the .iso image we previously uploaded to the catalog as if it were in the CD drive.



Select the media for the CentOS LiveCD that you uploaded earlier. Click **Insert**.



Click the **green >** icon to start the vApp and power on the virtual machine. You will notice that the thumbnail for the virtual machine will refresh as the virtual machine begins its boot process.

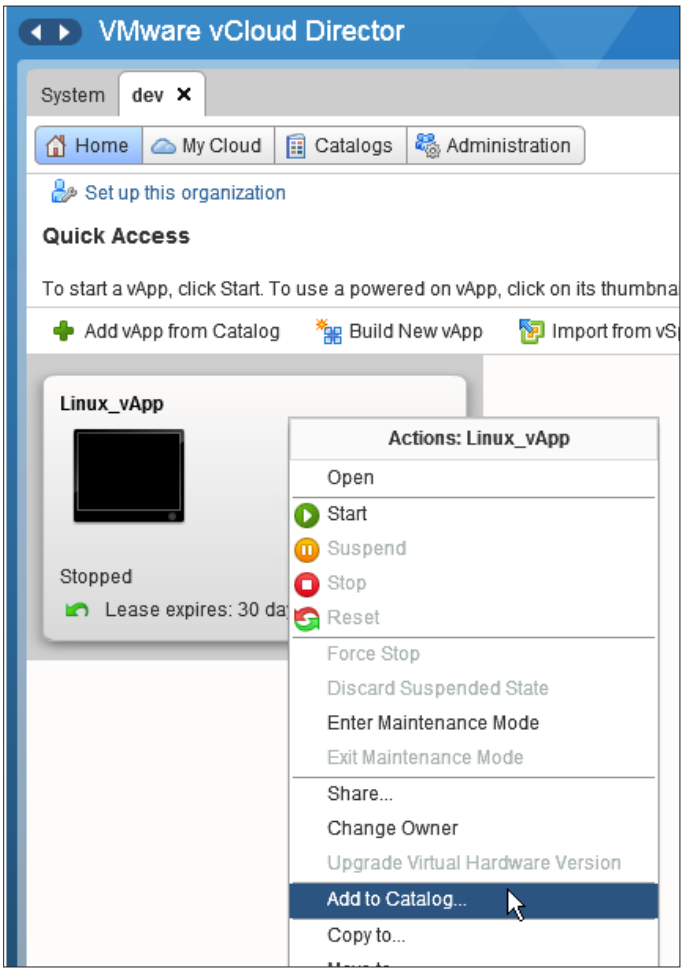
You can access the console for the virtual machine by clicking the thumbnail. If this is your first access attempt, you will be prompted to install the VMRC browser plug-in.

Creating a vApp Template

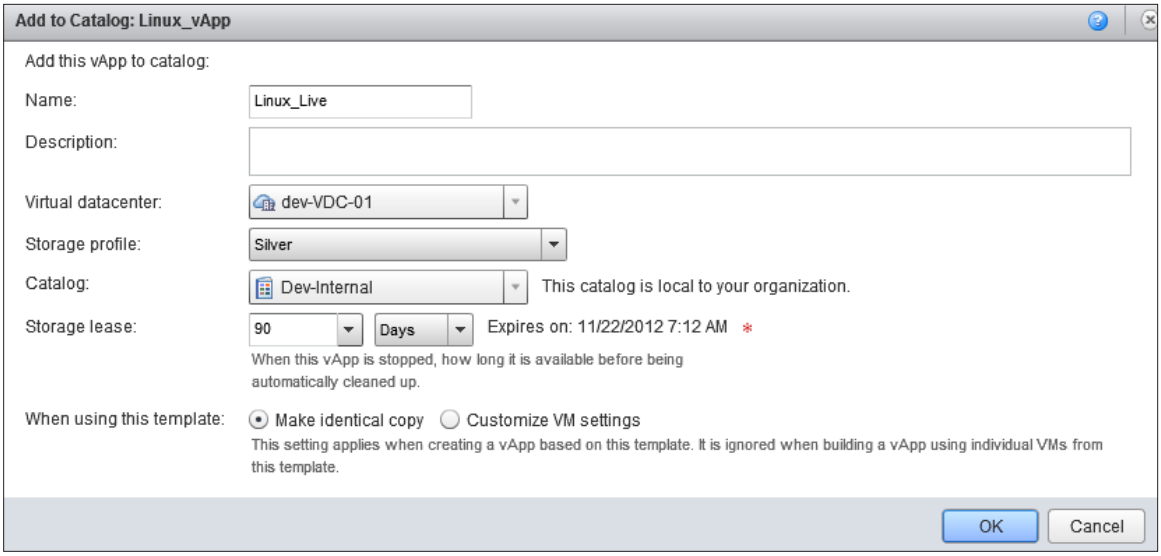
A vApp template enables users in an organization to quickly deploy vApps that have already been configured. By creating a collection of vApp templates, users can avoid the time required to set up and configure an environment for use. It also can enable you as the administrator to define standardized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

The use of fast provisioning (if enabled) with a vApp template greatly accelerates provisioning of new vApps. It might also cause you to see an object called a "shadow" virtual machine, because 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 organization **Home** screen, stop the vApp by clicking the **red stop** icon.



When it has stopped, right-click the vApp to bring up the **Actions** menu. Select the **Add to Catalog...** option.



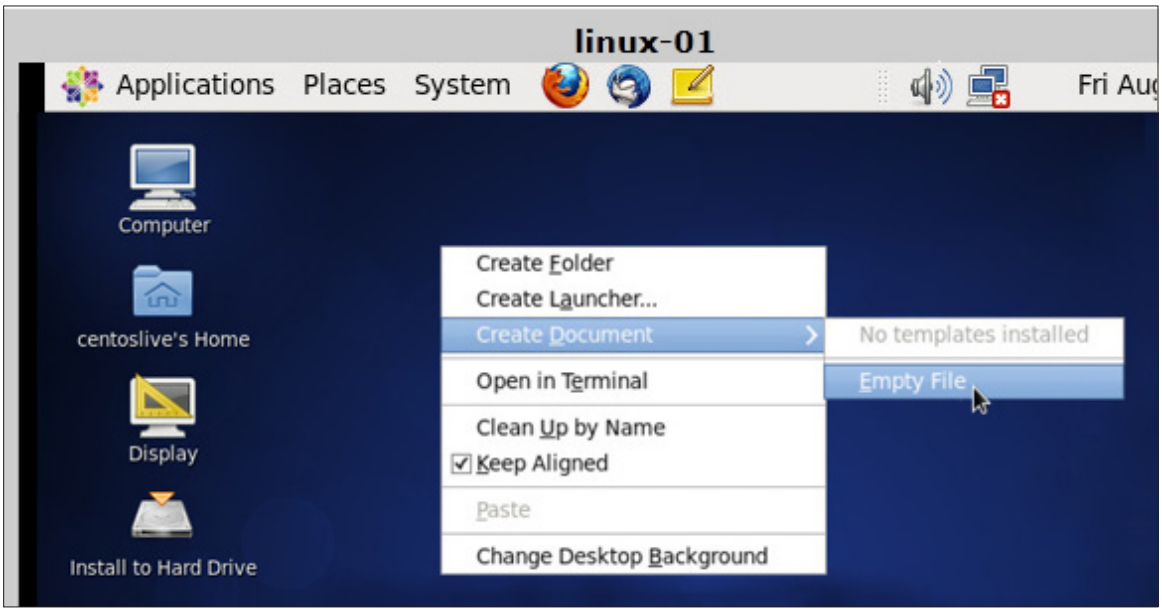
You then can specify the various options for the vApp template. Provide a name and define the storage lease as needed. You also can make an exact copy of the virtual machines or customize them when the template is used. Customization of Microsoft Windows–based machines will require the installation of additional binaries within the vCloud Director instance. Select the **Make identical copy** option and click **OK** to continue.

The vApp template now will be in the organization catalog. It can be used to deploy new vApps by selecting the **Add vApp from Catalog** option.

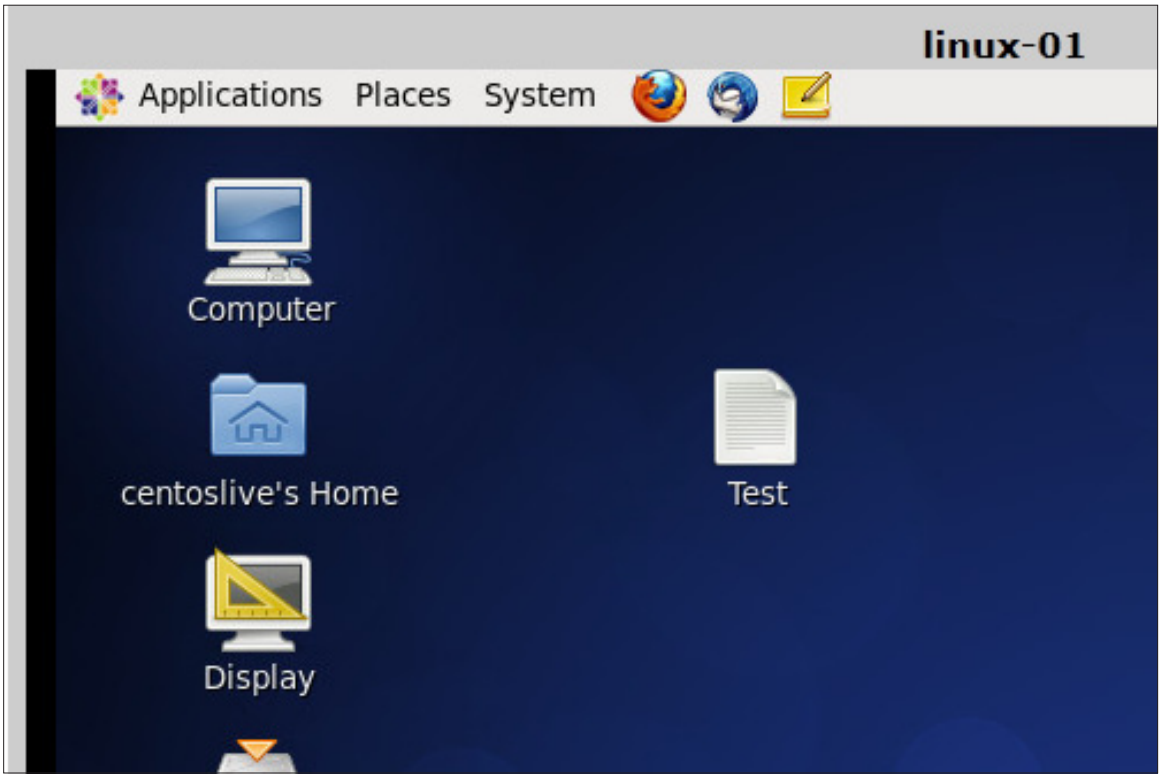
Using Snapshots

Snapshots provide a means to make a point-in-time copy of a virtual machine or a vApp and all the virtual machines it contains. This enables you to perform tasks such as destructive testing of a virtual machine, with the ability to revert to the point in time when the snapshot was taken.

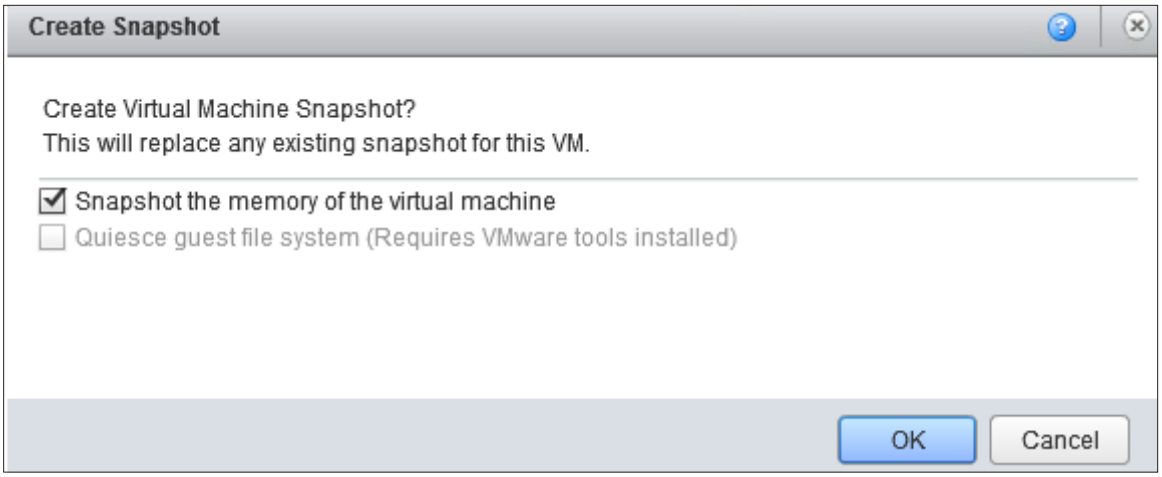
To demonstrate this, we first will create the means to quickly identify the effects of the snapshot. For this, we will use the vApp that you created earlier. If the vApp is powered off, start it and open a console to the virtual machine.



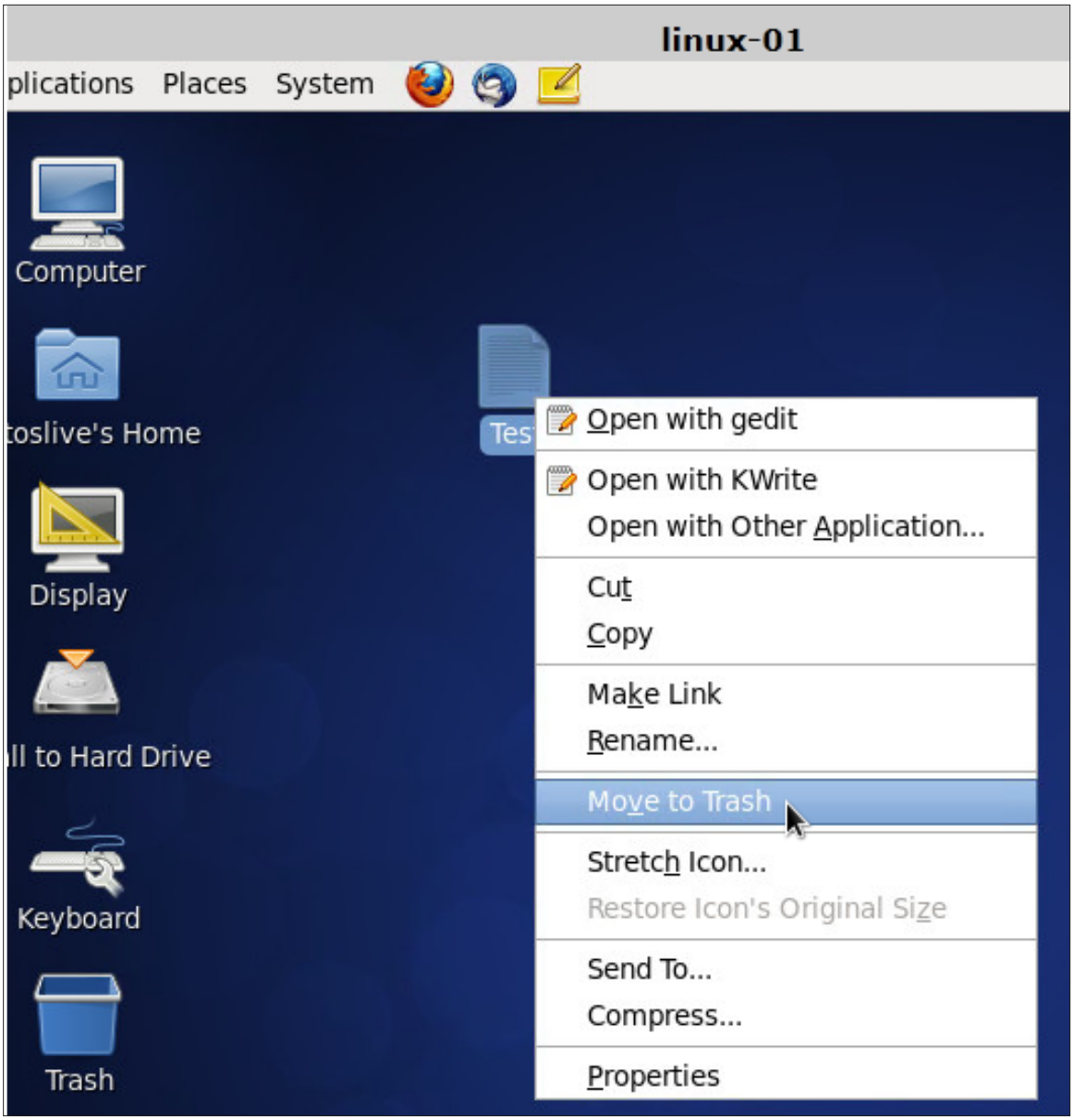
When you have a console to the virtual machine open, right-click the desktop and create a new document.



This file can detect the changes that occur within an environment when using snapshots.



Right-click the thumbnail for the virtual machine and select **Create Snapshot**. This brings up a window that gives you the options to snapshot the memory of the virtual machine and/or to quiesce the guest file system. In this example, you do not have VMware® Tools™ installed, so the **Quiesce guest file system** option is not available. Select the **Snapshot the memory of the virtual machine** check box and click **OK**.



After the snapshot is complete, return to the virtual machine console. Delete the empty file you created earlier by right-clicking it and selecting the **Move to Trash** option.

Return to the vCloud Director user interface and right-click the virtual machine. Select the **Revert to Snapshot** option. Return to the virtual machine console. You will see the empty file again, because you took the snapshot prior to deleting the file.

Conclusion

Next Steps

With VMware vCloud Director, you can do the following:

- 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 vCloud Networking and Security 5.1 security technologies.
- Reduce costs—through increased resource pooling and automation—by efficiently delivering resources to internal organizations as virtual datacenters.
- 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 VMware 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 cloud environment, download and evaluate VMware vCenter Chargeback Manager.

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 comments 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 Evaluation Guide" in the subject line. Thank you for your help in making this guide a valuable resource.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

 Item No: VMW-WP-vCD-5.1-EVAL-GUIDE-USLET-101 Docsource: OIC - 12VM007.10