



Intel® Cloud Builders Guide: Cloud Design and Deployment on TAROX ParX* Server Series

VMware vCloud Director*



Intel® Xeon® Processor 5500 Series

Intel® Xeon® Processor 5600 Series



AUDIENCE AND PURPOSE

This reference architecture guide seeks to simplify the deployment and operation of a cloud. This guide describes a cloud with VMware vCloud Director*, the TAROX Systems & Services GmbH with ParX* R2080i and ParX 1080i powered by the Intel® Xeon® processor, and the details for this particular cloud configuration.

The content is targeted to IT professionals responsible for the design, implementation, validation, and utilization of cloud structures. Details for the hardware configuration, software configuration, and results from specific test cases implemented that demonstrate basic operational capabilities are described in this guide.

This guide should complement product documentation and is provided as a starting point for the actual development of an enterprise or service provider cloud.

Table of Contents

Software Components	3
Executive Summary	3
Introduction	3
VMware* Overview.....	3
Introduction to VMware vCloud* Director	4
Test Bed Overview	6
Physical Architecture.....	6
Logical Architecture	9
Technical Review	9
Installation and Configuration	9
VMware vSphere* Hypervisor.....	9
VMware vCenter* Server	9
VMware vShield Manager*	10
Oracle Database*	10
VMware vCloud Director* Installation and Configuration	10
Connect VMware vCloud Director* with vCenter* and vShield Manager*	10
Use Case Details	12
Overview.....	12
Set Up Provider VDCs	13
Set Up External Networks	15
Set Up Network Pools.....	17
Set up Organizations and Users	18
Set Up Organization VDCs	22
Create Organizational Networks.....	25
Create Catalogs.....	27
Use Infrastructure as a Service	29
Dynamic Scaling	32
Termination of vApp.....	33
Separation of Roles and Responsibilities.....	34
Notification and Alerts	35
Next Steps	35
Scalability of the Application Level	35
Additional Usage Models.....	35
Planning Considerations	35
Hardware.....	35
Network Technology Architecture	36
Storage Architecture.....	36
Security.....	36
Software.....	36
VMware vCenter Server*, VMware vShield Manager* and VMware vCloud Director*	36
Additional Information	36
Glossary	37
Endnotes	38

Software Components

Item	Version
VMware vCloud Director*	1.0
VMware vSphere* ESXi	4.0 Update 2 or 4.1
VMware vCenter Server*	4.0 Update 2 or 4.1
VMware vShield Manager* 4.1	4.1

Table 1 - Cloud Test Bed Software Configuration

Executive Summary

To break the trend of ever-increasing demand for compute resources and the resultant rise in operational costs, a new model for IT services has emerged—cloud computing. Cloud computing is an approach to computing that utilizes the efficient pooling of an on-demand, self-managed virtual infrastructure, consumed as a service. This approach abstracts applications and information from the complexity of underlying infrastructure, so IT can support and enable business value. Cloud computing architectures are built on the foundation of virtualization, and as the customer-proven leader in virtualization, VMware* helps to chart the course to cloud computing. VMware works in concert with Intel and other industry leaders to help businesses of all sizes migrate to secure cloud computing in order to establish a new era in IT that finally addresses the compounded problems of IT cost and complexity. VMware's proven technology is a logical starting point to develop cloud reference architectures.

In these challenging economic times, when IT is asked to do more with less, businesses need to use their existing investments in applications, hardware, and know-how. VMware facilitates a pragmatic approach to enable the benefits of cloud computing as they turn today's data center into secure private clouds inside the enterprise firewall. In parallel, VMware and Intel work with host and service providers to enable compatible public cloud infrastructures. In the drive towards federation and common management services between clouds, the VMware vSphere* environment presents a path toward a seamless, dynamic operating environment. This approach will ultimately enable enterprises to bridge internal

resources with available external resources, which helps to achieve the full flexibility and benefits of cloud computing. The result is a hybrid cloud.

At the core of cloud computing is the ability of the underlying compute, network, and storage infrastructure to act as an efficient, shared resource pool that is dynamically scalable within one data center or across multiple data centers. With this foundation, critical higher-level capabilities, such as secure multi-tenancy, guaranteed quality of service, federation, and data center automation are made possible. Intel, along with leaders in software, works to address these new core innovations in Infrastructure as a Service (IaaS) and has initiated a program to rapidly enable enterprises and service providers to clarify best practices around design (including reference architectures), deployment, and management. For enterprise IT and cloud service providers who need to use their existing data center infrastructure to supply cloud services to their customers, this Intel® Cloud Builders guide provides a comprehensive solution overview that covers technical planning and deployment considerations.

Introduction

VMware* Overview

For decades, IT has been characterized as complex and inefficient because it fails to meet the needs of businesses in an effective and timely manner. Desperate to increase agility without higher costs, organizations seek a new approach to reduce IT complexity, and cloud computing has quickly evolved as that approach. VMware's customer-proven virtualization solutions uniquely accelerate an

organization's transition to the cloud, which enables IT to efficiently pool on-demand, self-managed virtual infrastructure, at the same time it preserves existing investments. Through VMware* solutions, built on the industry's most deployed virtualization platform — VMware vSphere* — IT can maximize efficiency without compromising service delivery, and increase agility while maintaining control.

As the global leader in cloud infrastructure, VMware also offers solutions that promote freedom of choice. The same VMware architecture deployed by enterprises is deployed by thousands of service providers, which enables a compatible bridge between a private cloud hosted internally in a data center and public clouds hosted remotely. Together with Intel and a broad set of industry partners, VMware advances open standards and solves next-generation hurdles, so that all organizations can rapidly achieve the benefits of cloud computing.

VMware views cloud computing as an approach to computing that uses the efficient pooling of on-demand, self-managed virtual infrastructure, which is consumed as a service. There are six core characteristics of cloud computing that VMware solutions deliver:

1. **Pooling:** Use of virtualization to change the model from machine-based to highly elastic resource pools that are shared across applications and users to enable on-demand resource allocation in the most efficient manner.
2. **Zero-Touch Infrastructure:** Policy-driven management automates routine operational tasks, which

- minimizes operational expense and overhead.
3. **Self-Service:** Provisioning and deployment are dramatically simplified through the self-service model within the parameters of defined business and governance policies, while management of systems and infrastructure is dramatically reduced through policy-driven automation.
4. **Control:** Built on a robust platform that is architected for high availability with the ability to optimize resource allocations and ensure service levels. Built-in disaster recovery mechanisms ensure business continuity. Offers a security model that encompasses dynamic infrastructure and boundaries to protect the cloud. Application-aware infrastructure that self-optimizes application performance.
5. **Openness and Interoperability:** Application mobility between clouds within a common management model, based on open standards, extended to a large ecosystem of public cloud

- providers.
6. **Utilization of Existing Assets:** The ability to bring existing applications and all of IT into the cloud computing model in an evolutionary manner starts internally with a private cloud.

Introduction to VMware vCloud* Director

VMware vCloud Director* is a software solution that enables enterprises to build secure, multi-tenant, private clouds as they pool infrastructure resources into virtual data centers (VDCs) and expose them to users through Web-based portals and programmatic interfaces as fully-automated, catalog based services. Internal IT organizations can build secure and cost-effective private clouds with VMware vSphere* and VMware vCloud Director, and thus act as true service providers for the businesses they support. As such, they can drive innovation and agility, and at the same time increase IT efficiency and enhance security. This solution provides a

pragmatic path to cloud computing because it gives customers the power to use existing investments and the flexibility to extend capacity between clouds.

- **Deliver Infrastructure as a Service:** VMware vCloud Director* enables IT organizations to deliver resources to internal users as VDCs. IT organizations can logically pool compute, storage, and network capacity into virtual data centers, to manage resources more efficiently, with complete abstraction between consumption and delivery of IT services. Instead of providing users or organizations with siloed physical infrastructures, IT teams can deliver isolated VDCs that draw resources from a common physical infrastructure. By pooling these physical resources on the back end, hardware utilization and consolidation increases. Similarly, underlying infrastructure can be pooled into tiers and offered to users at distinct service levels and prices.

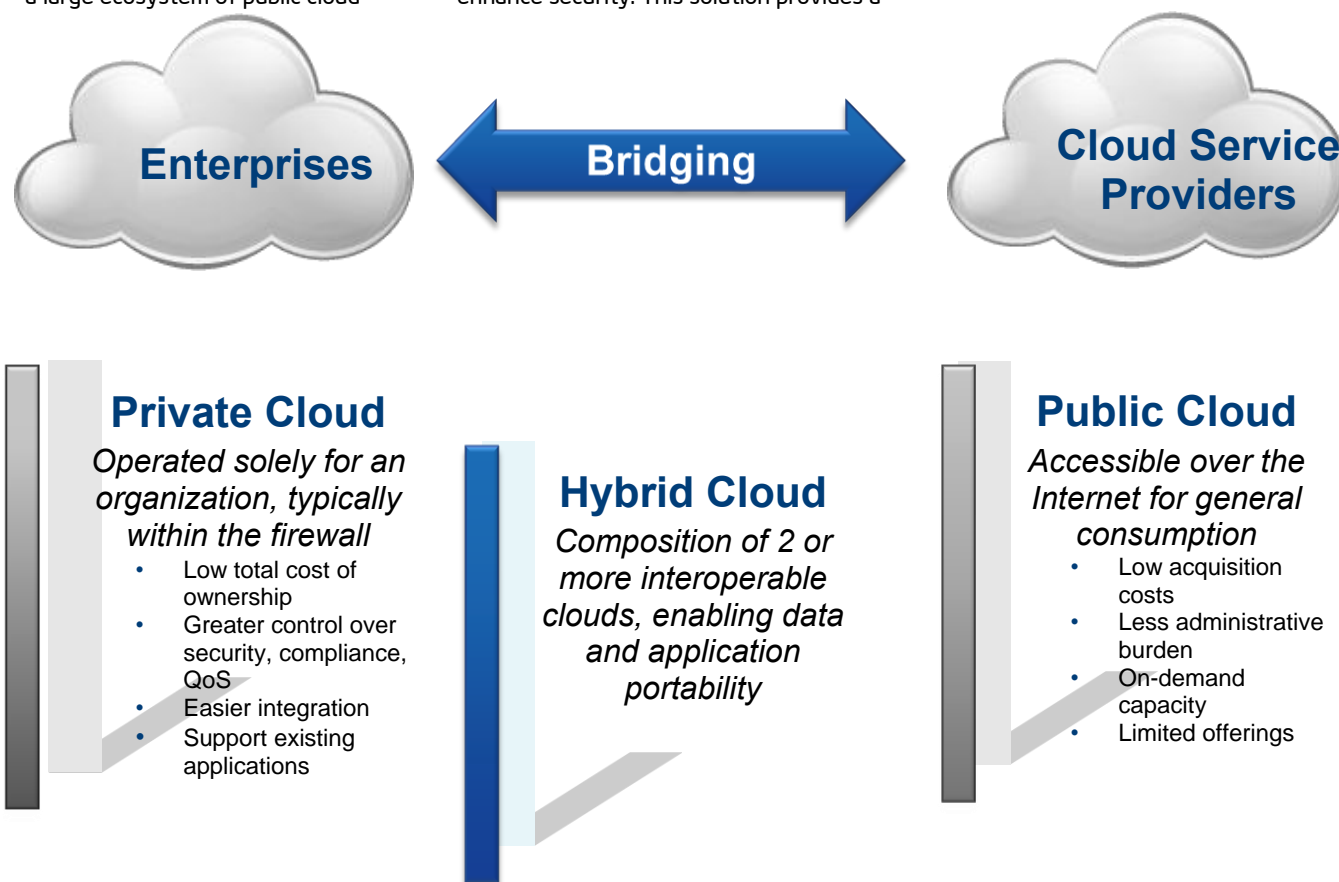


Figure 1 - Choice of Flexible Cloud Deployment Models

- Consume Infrastructure as a Service:** VMware vCloud Director* also changes the way that users consume IT services. There is no need to file service desk tickets and wait in queues; instead, application and line-of-business owners can utilize self-service portals to access their own VDC. VMware vCloud Director enables users to consume these resources as a catalog based service through a web portal and programmatic interfaces. IT teams can define multiple consumption models that use the same infrastructure, which range from capacity-as-you-go to reserved pools. These can be delivered at an appropriate cost model with VMware vCenter* Chargeback, which helps drive accountability and enables granular usage monitoring. Ultimately, IT organizations maintain control with permissions, quotas, and leases governed by role-based access controls that utilize existing LDAP directory services.

In this new model, IT organizations become cloud service providers for the business,

and they achieve the benefits of cloud computing without sacrifice to security or control. Users experience unprecedented responsiveness and agility, and IT management can reduce costs through increased consolidation, task automation, and simplified administration. This is all achieved cost-effectively by use of existing investments in people and technology. Because it provides elastic standard storage and networking interfaces, such as Layer 2 connectivity and the ability to broadcast between virtual machines, VMware vCloud Director* integrates with existing VMware vSphere* deployments, and supports existing and future applications. VMware vCloud Director utilizes open standards to preserve deployment flexibility and pave the way to the hybrid cloud. Customers can extend their data center capacity, through partnerships with a broad ecosystem of service providers who offer cloud services based on VMware vCloud Director, to include secure and compatible public clouds and manage them as easily as their own private cloud. For enterprise IT who want

to build private clouds, the combination of Intel® Xeon® processor servers, VMware vSphere, and VMware vCloud Director provides a leading cloud infrastructure to:

- Create VDCs:** VDCs are logical constructs that include compute, storage, and network capacity to enable complete abstraction between the consumption of infrastructure services and the underlying resources.
- Support Multi-tenant Environments:** Administrators can group users into organizations that can represent any policy group, such as a business unit, division, or subsidiary company. Each has isolated virtual resources, independent LDAP authentication, specific policy controls, and unique catalogs. These features enable secure multi-tenancy and safe sharing of infrastructure.

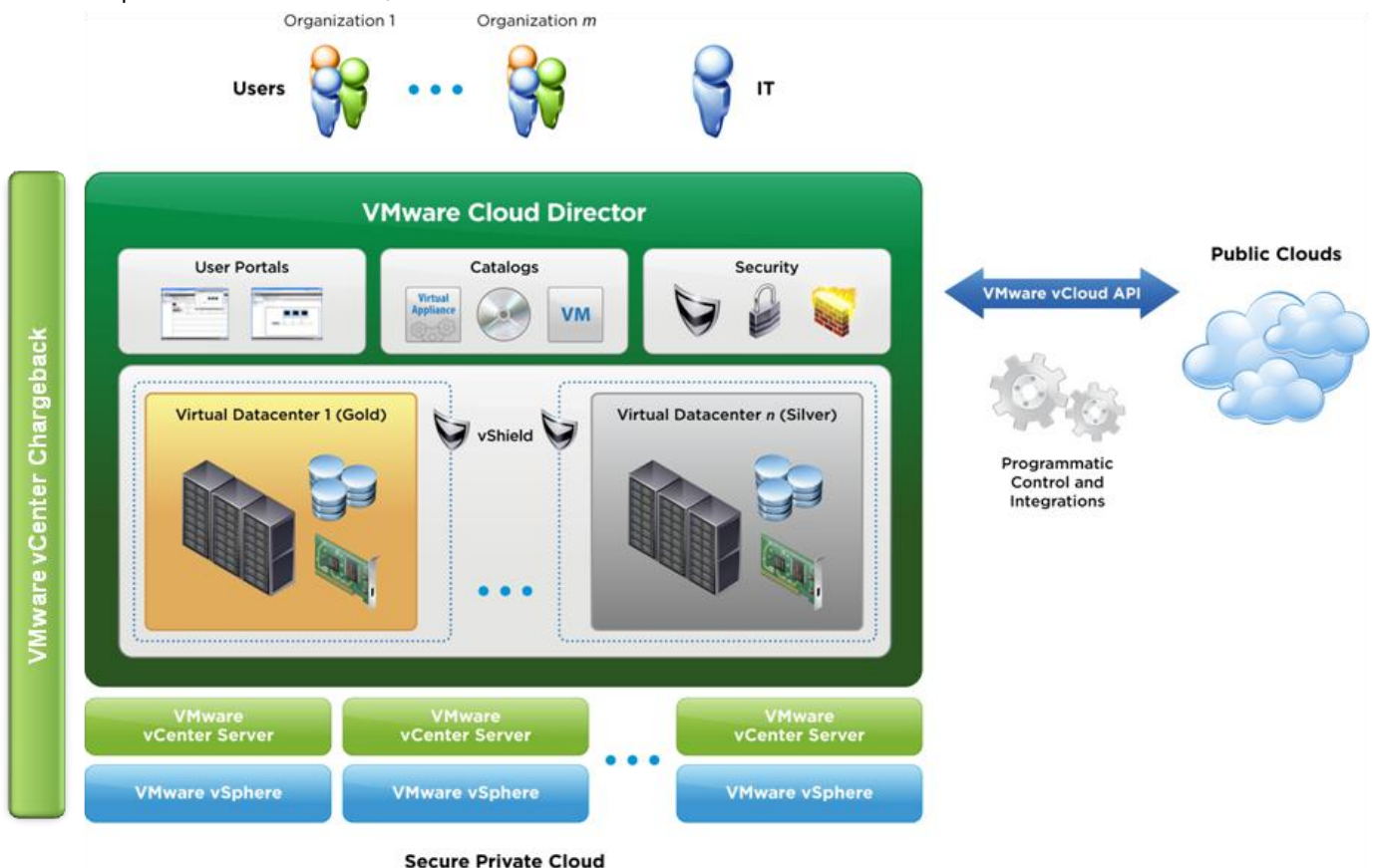


Figure 2 - VMware vCloud* Director Secure Private Clouds Deliver IT Resources

- **Improve Security:** Integrated VMware vShield Edge* security technologies such as perimeter protection, port-level firewalling, network address translation, and dynamic host configuration protocol (DHCP) services offer virtualization-aware security, simplify application deployment, and enforce boundaries required by compliance standards. The upgrade to the full VMware vShield Edge solution adds advanced services such as site-to-site VPN, network isolation, and Web load balancing.
- **Deliver Standardized Infrastructure and Application Services:** Users are empowered to deploy and consume pre-configured infrastructure and application services, such as virtual appliances, virtual machines, operating system images, and other media with the click of a button from central catalogs. This enables IT teams to standardize offerings, which simplifies the ability to troubleshoot, patch, and change management.
- **Automate and Orchestrate:** Administrators can use the APIs in conjunction with the VMware vCenter Orchestrator* plug-in, and integrations with other orchestration and service management software, to automate routine tasks, build information technology infrastructure library (ITIL) workflows, and script complex operations with ease.
- **Lower Management Costs and Quickly Provision Services:** Users get direct access to their catalogs and VDC through user-friendly, self-service Web portals.
- **Based on Open Standards:** The VMware vCloud API is an open, representational state transfer (REST) based API that allows scripted access to consume cloud resources, such as vApp upload/download, catalog management, and other operations. The VMware vCloud API makes basic transfer between clouds possible using the open virtualization format (OVF), which preserves application properties, network configuration, and other settings.

For VMware vCloud service providers who want to build hybrid or private clouds, the combination of Intel® Xeon® processor servers, VMware vSphere*, and VMware vCloud Director* provides the same leading cloud infrastructure which includes:

- **Differentiated Services:** VMware vCloud* service providers can provide three classes of on-demand, self-service virtual data centers (VDCs):
 - **Basic VDC:** Unreserved “pay for use” class. Designed to quick-start pilot projects, and for workloads such as automated software tests that are transient and do not need high performance.
 - **Committed VDC:** Provides committed (reserved) compute resources with the ability to burst above committed levels if additional capacity is available. The enterprise subscribes to a committed VDC to ensure predictable performance and costs. VMware vSphere* provides the resources for on-demand workloads within a multi-tenant infrastructure.
 - **Dedicated VDC:** Provides dedicated compute resources (with the use of specific, dedicated hardware), sometimes known as a “virtual private cloud”. Offers predictable performance because it reserves dedicated resources, which is useful for situations in which security or compliance requirements require physical separation.
- **Provision and Manage:** Create a zero-touch infrastructure to optimize operational efficiency with built-in automation to make smarter and better use of virtual and cloud infrastructure. At the same time, assure compliance and performance in the face of increased service level expectations and accelerated change-deliver self-service with control.
- **Secure:** A single framework provides comprehensive cloud-enabled security to protect hosts, network, applications, data, and endpoints, and also reduces complexity for enhanced performance.

- **Based on Open Standards:** As described above, the VMware vCloud* API makes basic transfers between clouds possible with OVF, which preserves application properties, network configuration, and other settings.

Test Bed Overview

Physical Architecture

Figure 3 indicates the physical architecture of the test bed used for this guide. All VMware ESXi* hypervisor nodes have three separate network interface cards (NICs) for management, virtual machine, and storage network interfaces. For the sake of cost effectiveness and simplicity, a single network file system (NFS) store was used as shared storage for virtual machine images. Both VMware vCenter Server* and VMware vCenter Database* were installed on the same machine with the default database setting. VMware vShield Manager* 4.1 was deployed with the OVF template on one of the hosts within the VMware ESXi host cluster.

The Intel® Xeon® processor 5500 and 5600 series, Intel's latest processor technology, was used for the test bed. These processors provide a foundation to design more efficient cloud data centers that can achieve greater performance and at the same time use less energy and space, to dramatically reduce operating costs.¹ The Intel® Xeon® processor 5600 series delivers substantial increases in performance and energy efficiency over the previous generation Intel® Xeon® processor 5500 series, while it continues to support features from the previous generation that enable it to respond intelligently to workloads:

- **Intel® Virtualization Technology²** increases manageability, security, and flexibility in IT environments, and improves system utilization as it consolidates multiple compute environments. The abstraction of the underlying hardware enables new usage models which reduce costs, increase management efficiency, alleviate security issues, and improve computing infrastructure resiliency.

- **Intel® Turbo Boost Technology** boosts performance as needed through dynamic adjustments to core frequency to increase execution speed for peak workloads.
- **Intel® Intelligent Power Technology** adjusts core frequencies to conserve power when demand is lower.
- **Intel® Trusted Execution Technology (Intel® TXT)** is a hardware solution that validates the behavior of key components within a server or PC at startup. Known as the “root of trust,” the system checks the consistency in behaviors and launch time configurations against a “known good” sequence. Using this verified benchmark, the system can quickly assess whether any attempts to alter or tamper with the launch time environment have been made. (Currently requires VMware ESXi 4.1 U1 only)
- **Intel® Hyper-Threading Technology** improves throughput and reduces latency for multithreaded applications

and for multiple workloads that run concurrently in virtualized environments.

Each host in a VMware vCloud Director* cluster must meet certain software and hardware prerequisites. In addition, a database must be available for use by all hosts in the cluster. Each cluster requires access to VMware vCenter Server*, VMware vShield Manager*, and one or more VMware ESXi* hosts. For more information on configuration, software prerequisites, supported databases, disk, memory and network requirements please see the *VMware vCloud Director Installation and Configuration Guide* (http://www.vmware.com/pdf/vcd_10_install.pdf).

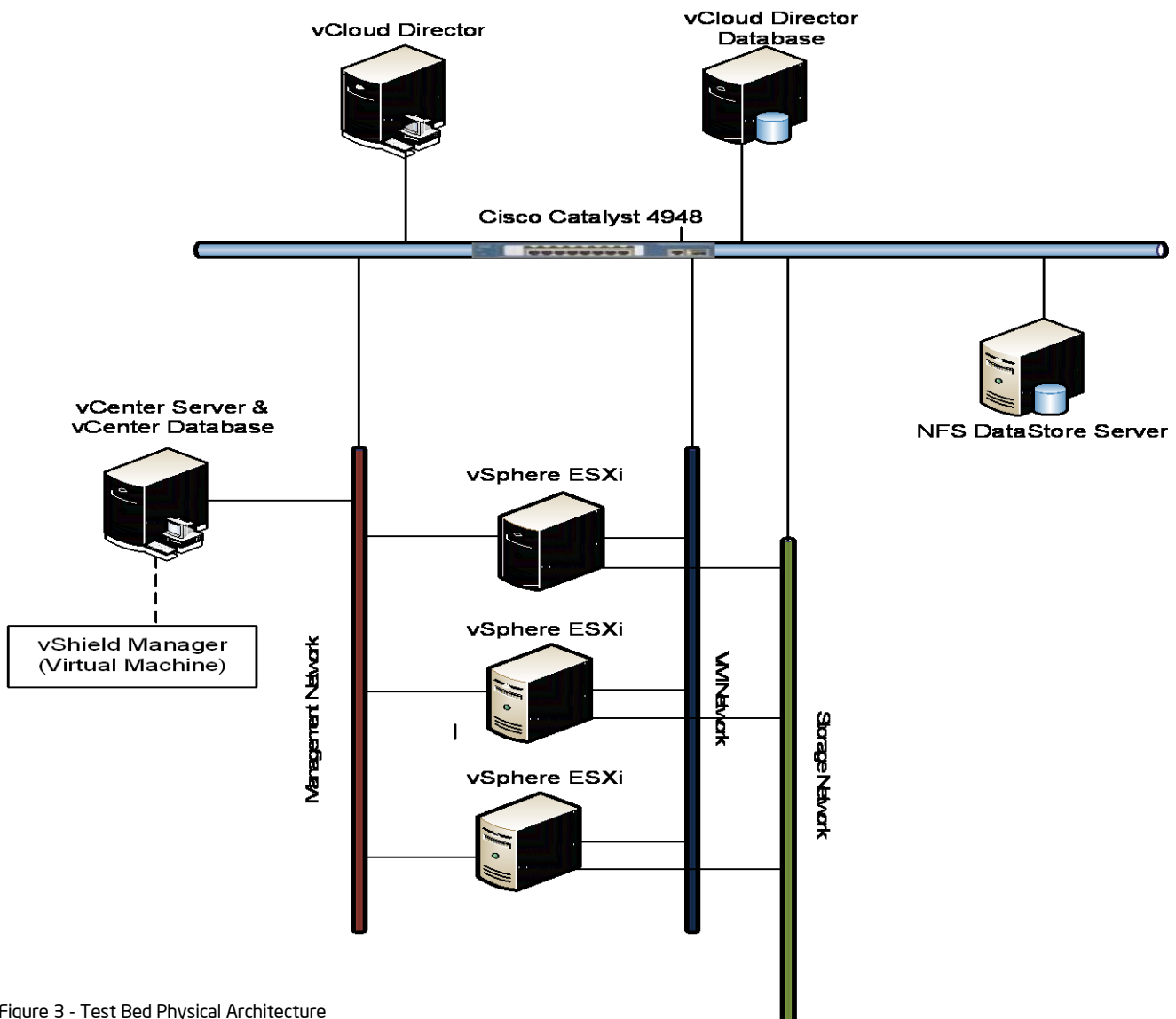


Figure 3 - Test Bed Physical Architecture

Table 2 shows specifications of systems used to build the cloud test bed.

System	Processor Configuration	Detail Configuration
3 VMware vSphere* Hypervisor (VMware ESXi*) nodes VMware VMWare ESXi* 4.1.0	Intel® Xeon® Processor See the product page at http://www.intel.com/p/en_US/products/server/processor/xeon5000	TAROX ParX* R2080i ⁸ with Intel® Server Board S5520UR Processor: Intel® Xeon® processor 5650 ³ ; 2.66 GHz; 2-way x 6 cores = 12 cores Memory: 24 GB RAM Storage: 147 GB HDD
1 Storage Subsystem	Intel® Xeon® Processor	1 Storage EMC Celerra* NS-120 Storage: 15x600 GB HDD configured as 3x RAID 5
1 VMware vCloud Director* Database Windows Server* 2008 R2 (64bit) Oracle* 11g Enterprise Edition	Intel® Xeon® Processor See the product page at http://www.intel.com/p/en_US/products/server/processor/xeon5000	TAROX ParX* R1080i ⁹ Intel® Server Board S5520UR Processor: Intel Xeon 5620 Memory: 24 GB RAM Storage: 3 x147 GB HDD
1 VMware vCenter* Server and VMware vCenter* Database VMware vCenter* Server 4.1.0 VMware vSphere* Client 4.1.0	Intel® Xeon® Processor See the product page at http://www.intel.com/p/en_US/products/server/processor/xeon5000	TAROX ParX* R1080i Intel® Server Board S5520UR Processor: Intel Xeon processor 5620 Memory: 24 GB RAM Storage: 3 x 147 GB HDD
1 VMware vCloud Director* RHEL* 5.4 (64bit) Update 4	Intel® Xeon® Processor See the product page at http://www.intel.com/p/en_US/products/server/processor/xeon5000	TAROX ParX* R1080i Intel® Server Board S5520UR Processor: Intel Xeon processor 5620 Memory: 24 GB RAM Storage: 3 147 GB HDD

Table 2 - Cloud Test Bed Hardware and Software Components

Logical Architecture

In a cloud infrastructure, a VMware vCloud Director* cluster is linked with one or more VMware vCenter Server* installations, a VMware vShield Manager* server, and an arbitrary number of VMware ESXi* hosts. The VMware vCloud Director cluster and its database manage access to VMware vCenter resources by VMware vCloud clients. Figure 4 is a schematic representation of a simple cloud infrastructure. The diagram shows a VMware vCloud Director cluster of four server hosts. Each host runs a group of services called a VMware vCloud* cell. All hosts in the cluster share a single database. The entire cluster is connected to three VMware vCenter instances and the VMware ESX hosts they manage. Each VMware vCenter instance is connected to a VMware vShield Manager host, which provides network services to the cloud. The VMware vCloud Director installation and configuration process establishes an initial set of connections to a VMware vCenter Server, VMware ESX hosts, and VMware vShield Manager. Additional VMware vCenter, VMware vShield Manager, and VMware ESX hosts can be connected to the VMware vCloud Director cluster at any time.

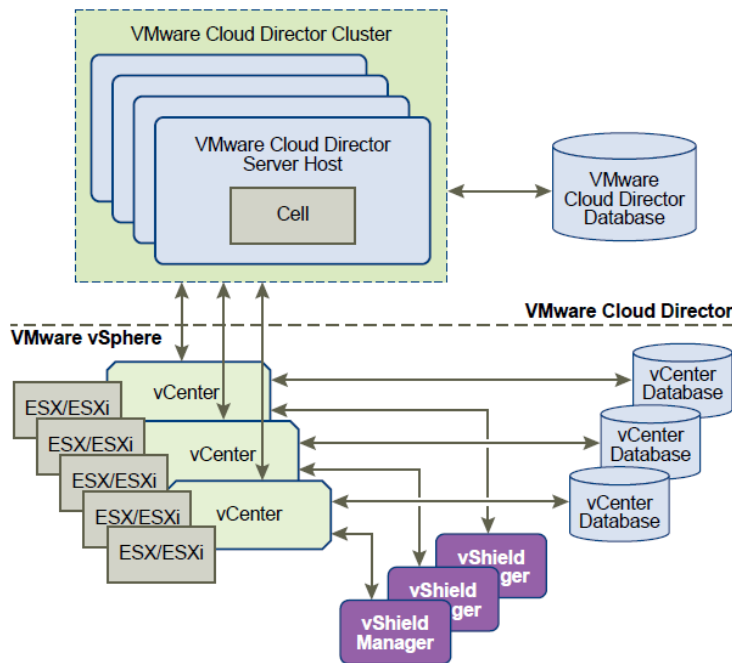


Figure 4 - VMware vCloud* Director Architecture Diagram

Technical Review

Installation and Configuration

In the test bed, a single instance of VMware vCloud Director* was configured to a single VMware vCenter* installation with three hypervisor nodes. The sections that follow provide a brief overview of the above steps. Detailed instruction on the setup can be obtained from VMware's website, at http://www.vmware.com/pdf/VMware_vCloud_Director_10_install.pdf.

VMware vSphere* Hypervisor

VMware vCloud Director* installation relies on the compute, storage, and network capacity provided by the underlying VMware ESX* or VMware ESXi* 4.0 Update 2 or 4.1 nodes. In the test bed installation, both types of VMware hypervisors co-existed without any issues. Refer to *VMware vSphere Hardware Compatibility Guide*, <http://www.vmware.com/resources/compatibility>, for the list of VMware certified hardware.

VMware vCenter* Server

Install VMware vCenter Server* 4.0 Update 2 or 4.1 and VMware vSphere* Client 4.1 Update 2 or higher on a Windows Server* 2008 R2 system. Create a cluster and add the VMware ESX*/ESXi* hosts created in the above step. Configure the VMware Distributed Resource Scheduler (DRS) setting based on the requirements, and setup "Enhanced vMotion Compatibility (EVC)" based on the processors in the VMware ESX hosts that will be added into the clusters. For example, if the clusters will contain only Intel® Xeon® processor 5500 and 5600 series servers, "Intel® Xeon® Core™ i7" can be selected as the EVC Mode configuration. This mode will support Flex Migration of VMs

between the Intel® Xeon® processor 5500 and 5600 series systems. Ensure that all required configurations necessary for live VM migration of virtual machines between the hosts are completed⁴.

VMware vShield Manager*

VMware vShield Manager* provides the required network and security services to the VMware vCloud Director*. A separate instance of VMware vShield Manager (version 4.1) is required for each VMware vCenter* that is added to the VMware vCloud Director. VMware pre-bundles VMware vShield Manager as an OVF template, which can be imported into VMware vCenter. After network configuration, the VMware vShield Manager VM is up and running.

Oracle Database*

VMware vCloud Director* requires a database to store the information and share it with other VMware vCloud Director cells⁵ within the VMware vCloud Director cluster. VMware supports both Oracle Database* 10g Standard/Enterprise Release 2 and Oracle Database 11g Standard/Enterprise. In the test bed, the Oracle Database 11g Enterprise edition installed on a Windows Server* 2008 R2 system. Ensure all required privileges are assigned to the new user created as per the installation document⁶. This user will be employed during configuration of the VMware vCloud Director to establish the link with the Oracle database.

VMware vCloud Director* Installation and Configuration

Ideally a VMware vCloud Director* cluster will have several hosts, each of which will run the VMware vCloud services and each of which is called a VMware vCloud Director cell. These individual cells will be connected to the same Oracle* database created in the above step. These individual hosts will run Red Hat* Enterprise Linux (RHEL*) 5 Update 4 or Update 5. After the installation of the VMware vCloud Director services, configure the network and database settings. To connect to the database, use the credentials of the new user created during the installation of the database. Do not use the SYSTEM account for this step.

Connect VMware vCloud Director* with vCenter* and vShield Manager*

Once the network and database configuration is completed successfully, login to the VMware vCloud Director* with the credentials configured. Next, the VMware vCenter Server* instance(s) need to be added to this VMware vCloud Director cell, which will provide the required compute, storage, and network resources, and to VMware vShield Manager* for the network and security services. Figures 6 and 7 show the VMware vCloud Director's verification flow to configure VMware vCenter Server and VMware vShield Manager.

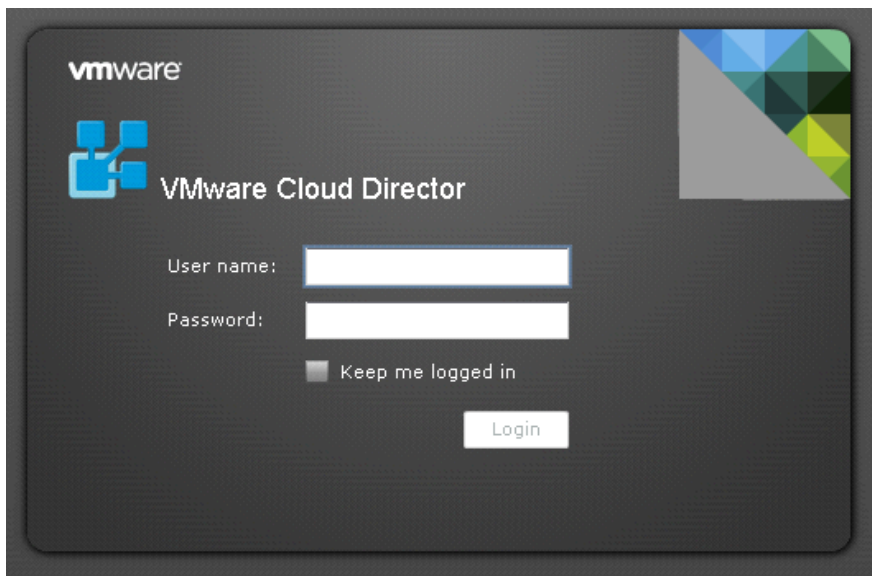


Figure 5 - VMware vCloud* Director Login Screen (Login with Administrator Credentials)

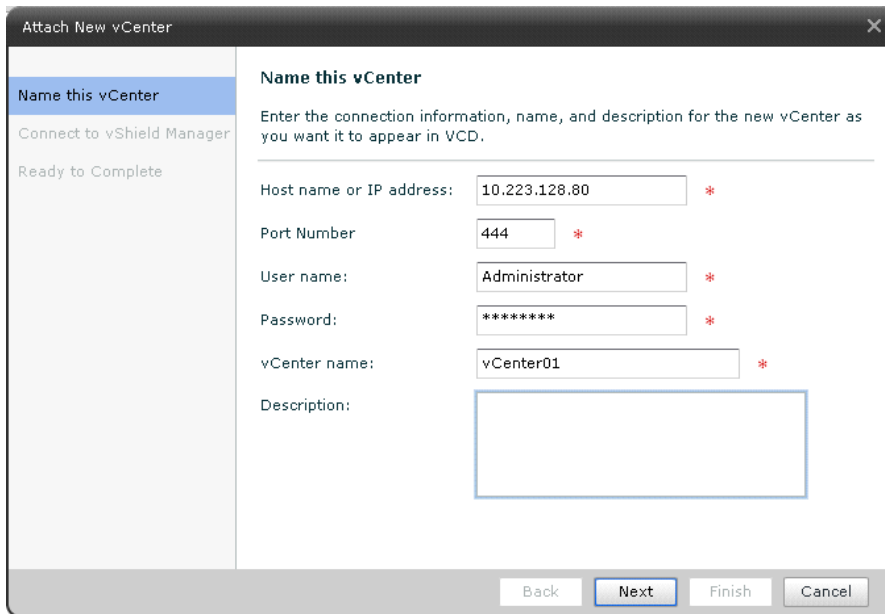


Figure 6 - Attach a VMware vCenter* Server

To connect VMware vCloud Director* to VMware vCenter Server* and VMware vShield Manager*, these steps were performed:

1. Attach a VMware vCenter Server* instance by clicking "Manage & Monitor".
2. Click "vCenter" on the left panel under VMware vSphere resources.
3. Follow the wizard, and enter the relevant VMware vCenter Server information. Because Internet Information Services (IIS) was also run on the same system, which used the default hypertext transfer protocol secure (HTTPS) port (443), the VMware vCenter Server instance was set up to use port 444 for HTTPS.

4. Enter the relevant VMware vShield Manager* information, then click “Finish” to complete.

Attach New vCenter

Connect to vShield Manager

vShield Manager is required for network services in VCD. Enter the connection information for the vShield Manager that is associated with this vCenter.

Host name or IP address: *

User name: *

Password: *

Back Next Finish Cancel

Figure 7 - Connect to vShield Manager* Screen

5. Verify VMware vCenter Server* has been added.

Name	Status	vCenter S...	Port Nu...	Ve...
vCenter01	✓	10.223.128.80	444	4.1.0

Figure 8 - VMware vCenter Server*

Use Case Details

Overview

To provide greater clarity of VMware vCloud Director* behavior, a set of illustrative use cases were tested. Use cases describe system behavior from an actor's point of view. The actors in these brief scenarios are the cloud administrator (from either enterprise IT or a service provider), the organizational unit (OU) administrator, or the end user of the cloud. These use case scenarios are:

- Set Up Provider VDCs.
- Set Up External Networks.
- Set Up Network Pools.
- Set Up Organizations and Users.
- Set Up Organization VDCs.
- Set Up Catalogs.
- Dynamic Scaling of Compute Resources.
- Separation of Duties.
- Termination of vApp or Service.
- Notifications.
- Use of Infrastructure as a Service (IaaS).

When the above tasks are performed:

- A private cloud solution will be functioning; VMware vCloud Director* will allow pooling of VMware vSphere* virtualized infrastructure together and offer standardized services for an organization.
- A private cloud will promote efficiency through automation, agility, and lower total cost of ownership.

Set Up Provider VDCs

The first cloud infrastructure object created is called a Provider Virtual Data Center (Provider VDC).

A Provider VDC is a combination of compute and storage resources. Compute and storage resources with specific characteristics, such as cost and performance, can be combined to create a Provider VDC. When this is done, a pool of compute and storage resources can be tiered into multiple service offerings, each implemented by one or more Provider VDCs. For example, the following tiers of service (Provider VDCs) can be created:

1. Combine the fastest storage, for instance, enterprise flash drives (EFD), and the fastest compute resources, and offer a Platinum Provider VDC.
2. Combine the slowest storage, for instance, serial advanced technology attachment (SATA), with compute resources, and offer a Bronze Provider VDC.

The compute resource for a Provider VDC comes from a VMware vSphere* cluster or resource pool. A Provider VDC can be scaled-up when more VMware ESXi*/ESX* servers are added to the VMware vSphere clusters and more data-stores are added to the clusters. The maximum size of a Provider VDC is 32 hosts. Scaling-up a Provider VDC is outside the scope of this guide. These steps were performed:

1. Follow the Wizard and select the VMware vCenter* resource pool to use.

Add Provider vDC

Select Resource Pool

The resource pool of the Provider VDC supplies compute and memory resources, memory, and vCenter services, such as high availability (HA) and fault tolerance (FT).

Select a vCenter and a resource pool: If it is not listed, you must attach a vCenter.

vCenter	Resource Pool	VC Path
vCenter01	Ent_RP	EnterPrise Cluster/Ent_RP
	EnterPrise Cluster	EnterPrise Cluster

The following external networks are available to the resource pool you selected:

Network	Gateway	Subnet	DNS

Selected resource pool: Ent_RP

Back Next Finish Cancel

Figure 9 - Add Provider VDC

- To create provider VDCs, follow the Wizard and select the VMware vCenter* resource pool to use.
- Select the appropriate data stores for this Provider VDC.

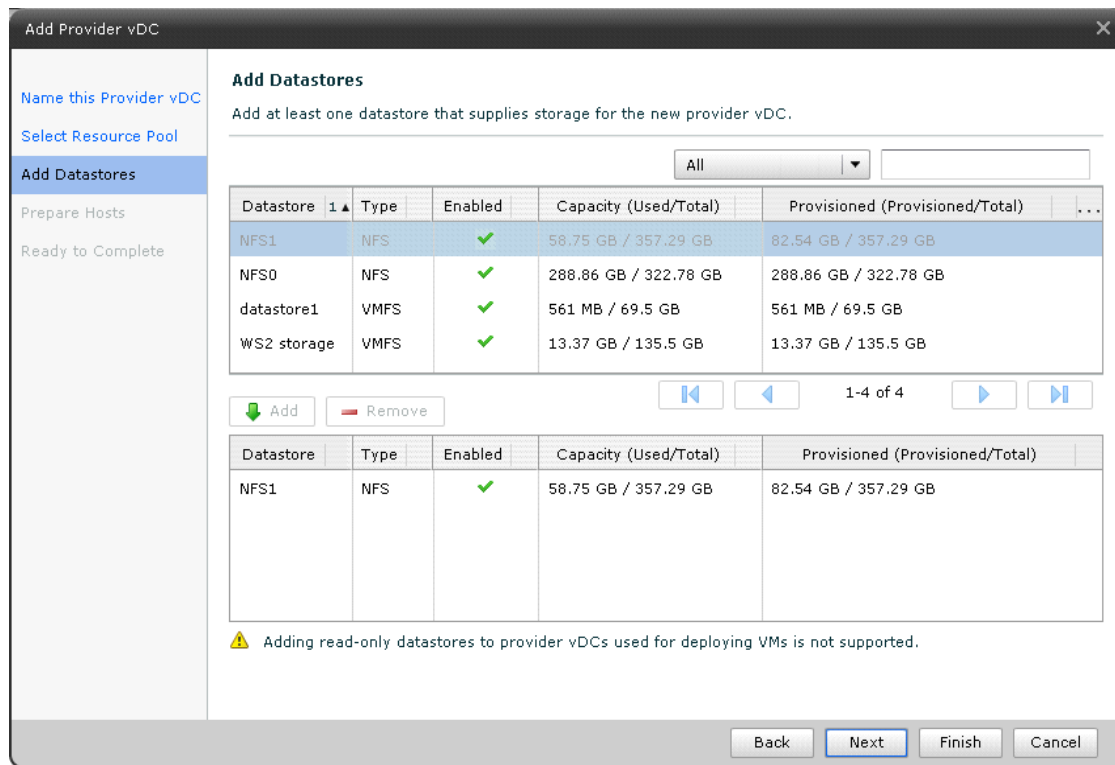


Figure 10 - Select Data Store

- Provide the required credentials for VMware vCloud Director* to ready the hosts.

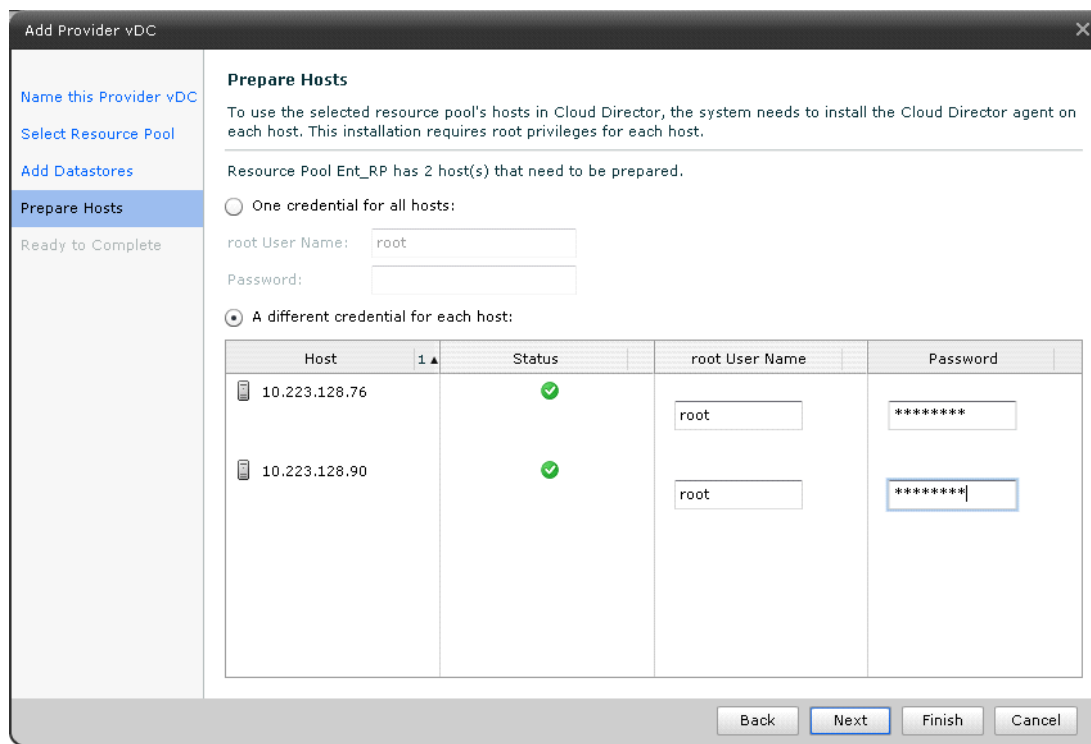


Figure 11 - Credentials

When a Provider VDC is created, the VMware vCloud Director creates a system VDC resource pool under the resource pool assigned to the VDC. The system VDC is used to host VMware vShield Edge* devices which provide network address translation (NAT) services between organizations, networks, and external networks without consumption of organizations' resources.

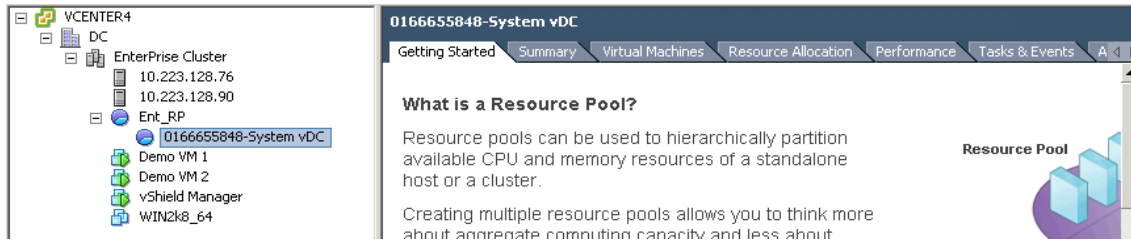


Figure 12 - VMware vSphere* Environment after Creation of Provider VDCs in VMware vCloud Director*

Manage & Monitor		Provider vDCs						
Organizations								
Cloud Resources								
Cloud Cells								
Provider vDCs								
Organization vDCs								
External Networks								
Organization Networks								
Network Pools								

Name	Status	Enabled	Org vDCs	Datastores	Resource Pool	vCenter
VCD1	✓	✓	1	1	Enterprise Cluster	vCenter01

Figure 13 - Provider VDC Screen

5. Validate to ensure Provider VDCs are created and enabled. VMware vCloud Director* prepares the hosts associated with the resource pools used to create Provider VDCs. Ensure host spanning is enabled (click the Manage & Monitor tab, then click on the "Hosts."

Set Up External Networks

External networks are used in VMware vCloud Director* to give external connectivity to vApps. vApps live in organizations (which will be introduced later), so in a sense these networks are "external" to the organization in which the vApps live. An external network is a port group in VMware vSphere* which carries external VM traffic. This port group can be associated with a VLAN tag to ensure network isolation. For instance, for vApps in the cloud to connect to vApps outside their own organization or to an external network service like the Internet or a shared storage network that are in a VMware vSphere environment, an external network must be created and the vApp connected to it.

1. Create a new external port group for VMware vCenter Server* and VMware vSphere* network.

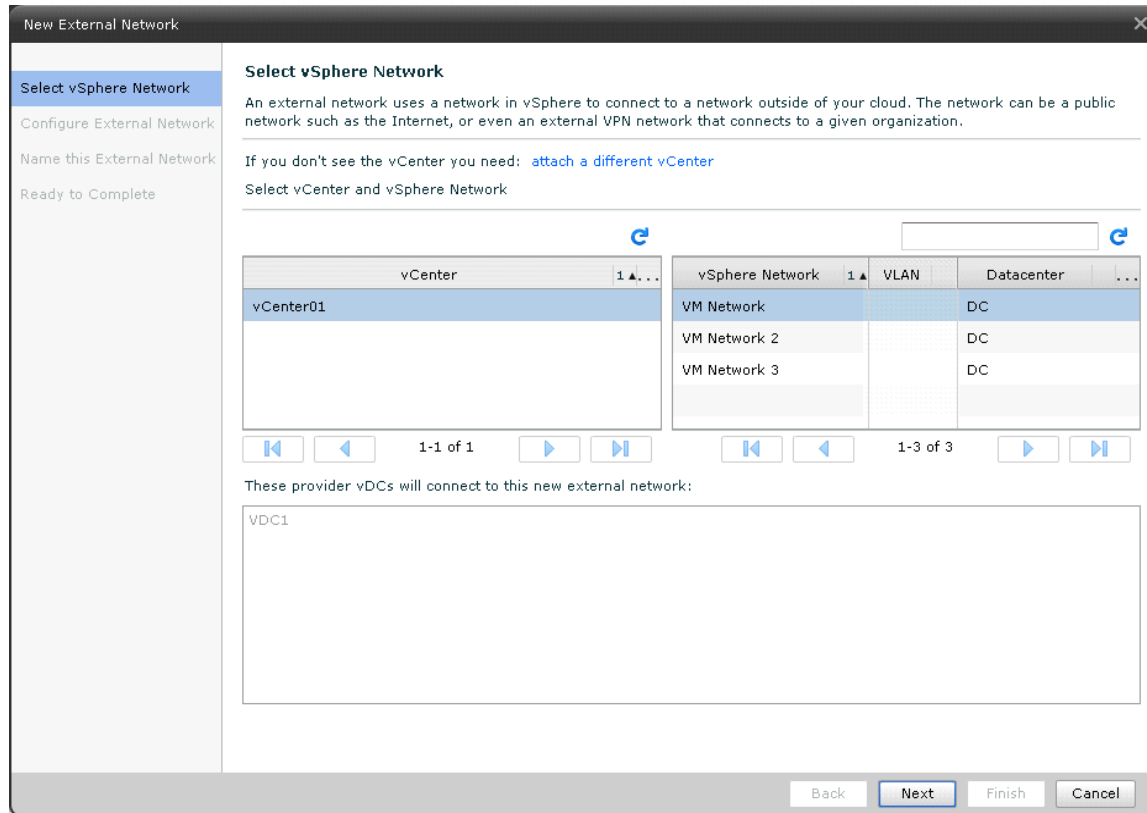


Figure 14 - VMware vSphere* Network

2. Add appropriate details to configure external network, then click "Finish".

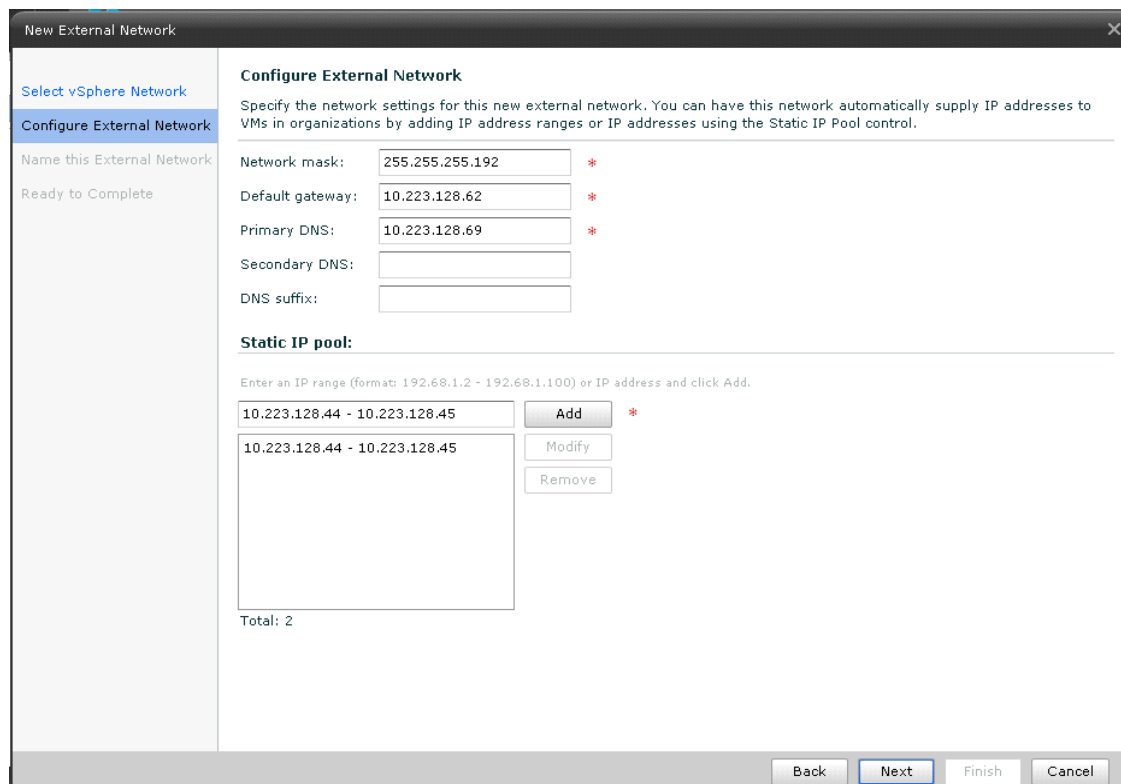
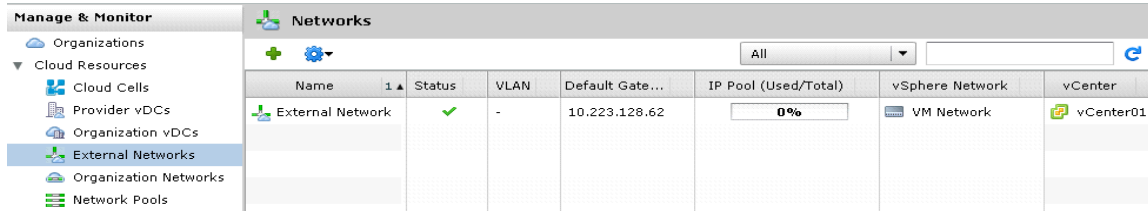


Figure 15 - Configure External Network

3. Validate to ensure external network is created and enabled.



Name	Status	VLAN	Default Gate...	IP Pool (Used/Total)	vSphere Network	vCenter
External Network	✓	-	10.223.128.62	0%	VM Network	vCenter01

Figure 16 - External Network Configuration

Set Up Network Pools

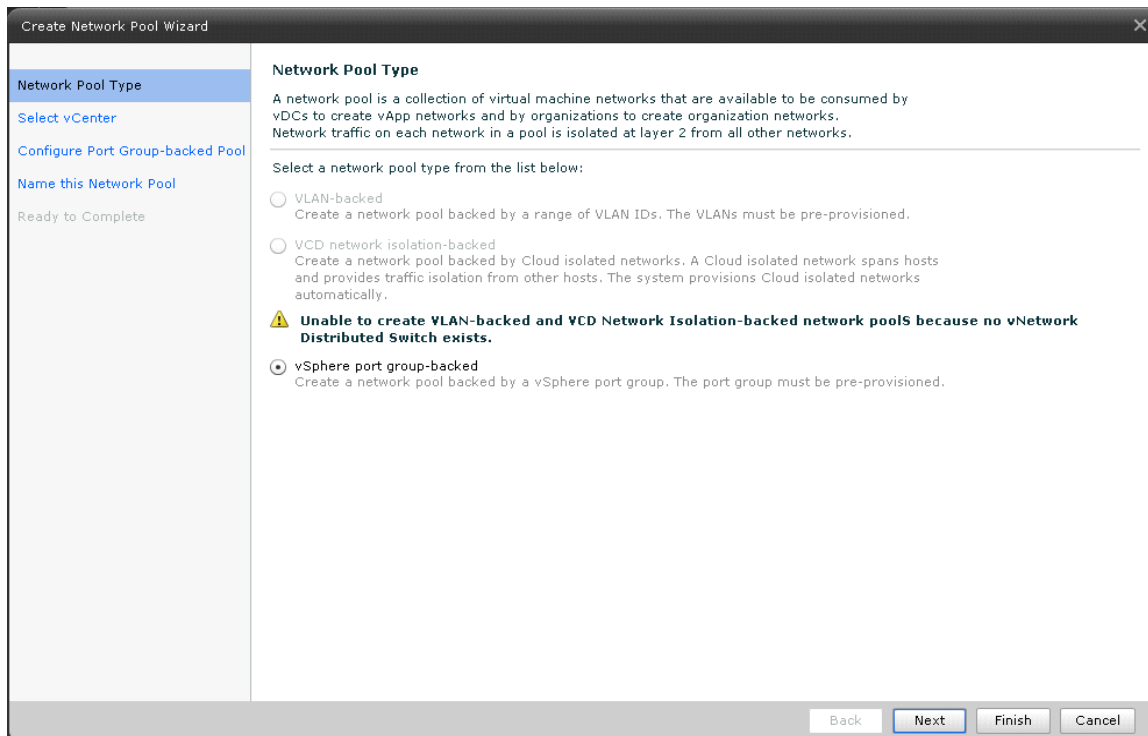
Network pools are collections of isolated Layer 2 networks that provide the building blocks necessary to create organization and vApp networks, and they are the key enabler to self-provision networks in the cloud. Organization networks are used for connectivity of vApps within an organization and vApp networks are used for connectivity of VMs within a vApp. Networks from a network pool are created dynamically by VMware vCloud Director each time the user creates an organization or vApp network, and the networks can be backed by VLANs, VMware vCloud Director* Network Isolation technology (VCDNI), or port groups.

To create a VLAN backed network pool requires a virtual dedicated server (vDS) and a range of VLAN IDs available to all hosts being managed by VMware vCloud Director on that vDS. Each time a user creates a network in VMware vCloud Director, a new port group is created on the vDS and a VLAN tag is attached to the port group. VMware vCloud Director manages the VLAN tags as a pool. The tags are sequentially assigned and returned back to the pool when the networks are deleted.

To create VCDNI network pools, a vDS attached to the VMware ESXi*/ESX* hosts in the cloud is needed. VMware vCloud Director uses a MAC-in-MAC encapsulation technique to create an isolated Layer 2 network without use of a VLAN. Each time a user creates a VCDNI Network, a new port group is created on the vDS and the port group is removed when the network is deleted.

To create port group backed network pools, a pre-configured set of port groups either on a vDS or on a standard vSwitch is needed. These port groups must be isolated, either with VLANs or with separate physical uplinks. VMware vCloud Director manages the port groups as a pool and creates a new network on a port group when a user creates a network. It returns the port group back to the pool when the network is destroyed. To set up network pools, these steps were performed:

1. Select the VMware vSphere* port group-backed network pool type.



Create Network Pool Wizard

Network Pool Type

A network pool is a collection of virtual machine networks that are available to be consumed by vDCs to create vApp networks and by organizations to create organization networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Select a network pool type from the list below:

- ☐ VLAN-backed
Create a network pool backed by a range of VLAN IDs. The VLANs must be pre-provisioned.
- ☐ VCD network isolation-backed
Create a network pool backed by Cloud isolated networks. A Cloud isolated network spans hosts and provides traffic isolation from other hosts. The system provisions Cloud isolated networks automatically.
- ☒ **Unable to create VLAN-backed and VCD Network Isolation-backed network pools because no vNetwork Distributed Switch exists.**
- ☒ vSphere port group-backed
Create a network pool backed by a vSphere port group. The port group must be pre-provisioned.

Ready to Complete

Back Next Finish Cancel

Figure 17 - Create Network Pool

- After selecting the appropriate VMware vCenter* and VMware vSphere* port group, name the network, then click "Finish".

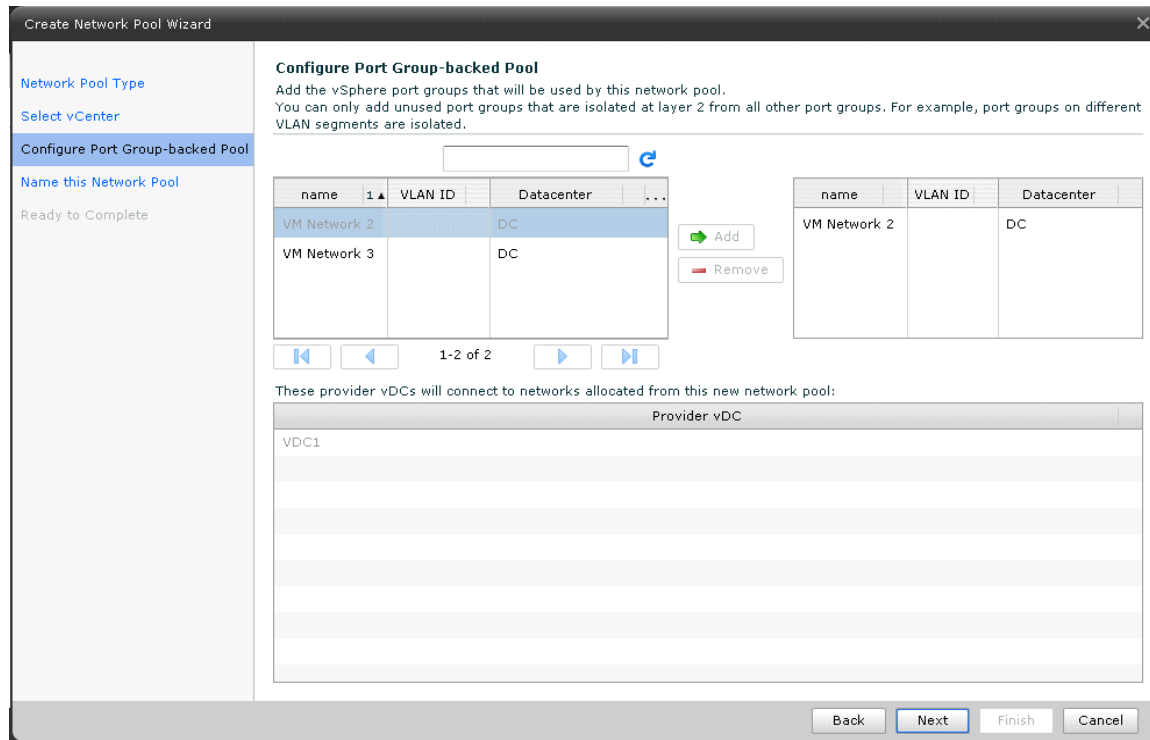


Figure 18 - Configure Network Pool

- Validate to ensure network pool is created and enabled.

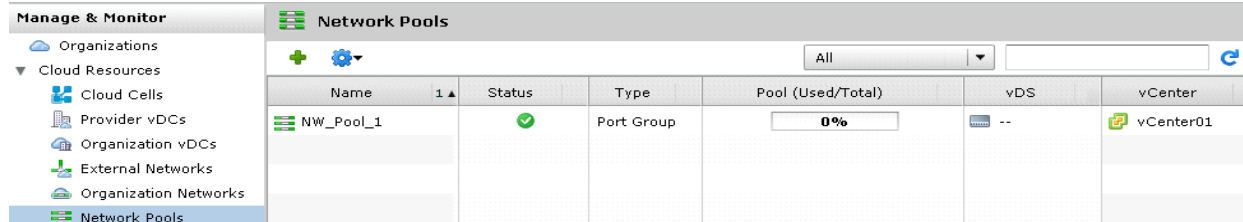


Figure 19 - Validation of Network Pools

Set up Organizations and Users

VMware vCloud Director* allows organizations to be created to separate groups of users from each other and different policy controls to be applied. For example, separate organizations can be created for Finance, Sales, IT, and HR. Each organization can contain different groups of users, and have its own set of resources and policies. VMware vCloud Director creates a separate URL for each organization where users of that organization log in. Inside organizations, users and groups can be created. Users can be authenticated in three different ways:

- Locally against the VMware vCloud Director* database.
- System wide through VMware vCloud Director* Active Directory or LDAP server.
- Through an organization specific active directory or LDAP server.

4. Create a new organization. For this evaluation, local users were defined and authenticated against the VMware Cloud Director* database.

The screenshot shows the 'New Organization' wizard in VMware vCloud Director. The left sidebar contains the following steps: 'Name this Organization' (selected), 'LDAP Options', 'Add Local Users', 'Catalog Publishing', 'Email Preferences', 'Policies', and 'Ready to Complete'. The main content area is titled 'Name this Organization' and includes a help icon. Below the title is a descriptive paragraph: 'An Organization is the fundamental VCD grouping. An Organization contains users, the vApps they create and the resources the vApps use. An organization can be a department in your own company or an external customer you're providing Cloud resources to.' The form contains the following fields and labels:

- Organization name:** A text input field containing 'IntelIT' with a red asterisk indicating a required field.
- Default organization URL:** A text input field containing the URL 'https://vcloudsd-1.lab.epi-ind.com/cloud/org/IntelIT/'.
- Organization full name:** A text input field containing 'IntelIT' with a red asterisk indicating a required field.
- Description:** A large text area for entering a description.

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

Figure 20 - Create New Organization

5. Add new user details and allow publishing of catalog to all organizations. Create two users, one as "Organization Administrator" and another as "vApp user."

New User

Credentials

User name: *

Password: *

Confirm password: *

☒ Enable

Role

Roles available to this user:

▼

Contact Info

Full name:

Email address:

Phone:

IM:

Quotas

Stored VM quota: ☐ ☒ Unlimited

Running VM quota: ☐ ☒ Unlimited

Figure 21 - Add New User

6. Complete relevant lease, quota, and limits, then click "Finish".

New Organization

Leases

Specify the maximum time that vApps and vApp templates can run and be stored in this organization's vDC(s).

vApp leases:

Maximum runtime lease: 7 Days *

How long vApps can run before they are automatically stopped.

Maximum storage lease: 30 Days *

How long stopped vApps are available before being automatically cleaned up.

Storage cleanup: Move to Expired Items

vApp template lease:

Maximum storage lease: 90 Days *

How long vApp templates are available before being automatically cleaned up.

Storage cleanup: Move to Expired Items

Quotas

Quotas define how many VMs a user in the organization can store and power on in a vDC. They can be changed by an organization administrator.

Running VM quota: ☐ 1 ☒ Unlimited

Stored VM quota: ☐ 1 ☒ Unlimited

Limits

These limits provide a defense against Denial of Service attacks. Resource intensive operations, such as copy, move, upload, Add to My Cloud, Add to Catalog, and so on, can be contained at a maximum number. Simultaneous connections to a VM through the VMRC console can also be limited, although this does not limit user-created connections through protocols such as VNC or RDP.

Number of resource intensive operations per user: ☐ 1 ☒ Unlimited

Number of resource intensive operations per organization: ☐ 1 ☒ Unlimited

Back Next Finish Cancel

Figure 22 - User Details

7. Validate to ensure the organization is created and enabled.

Name	Enabled	vDCs	Can Publish	Catalogs	vApps	Running VMs	Users
IntelIT	✓	0	✓	0	0	0	2
Sales	✓	0	✓	0	0	0	2

Figure 23 - Validate Organizations

8. View VMware vSphere* VMs and templates to see organizations created.

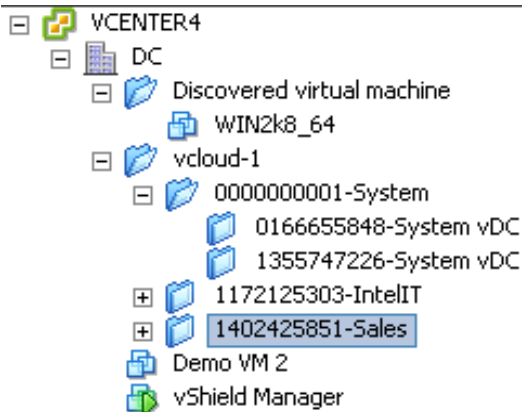


Figure 24 - VMware vSphere* VMs and Templates View

Set Up Organization VDCs

Organization VDCs are created so organizations can use resources from Provider VDCs. An organization VDC is a resource container of compute and storage resources which has a specific service level agreement (SLA) and cost associated depending on which Provider VDC it is created from. An organization VDC can grow to be as large as a Provider VDC and can use resources through multiple organization VDCs created from multiple Provider VDCs. There are three ways to consume resources from a Provider VDC:

1. Pay Per VM:
 - There is no upfront resource allocation.
 - Organization VDC resources are allocated only as users create vApps.
 - Set limits to cap usage.
 - Guarantee a percentage of the resources being used to prevent over commitment of compute and memory across the cloud.
2. Reservation Pool:
 - Organization VDC is allocated a “container” set of resources.
 - Organizations can use advanced VMware vSphere* resource management controls, such as Shares and Reservations, to manage over-commitment of their resources between their workloads. Some more sophisticated aspects of resource management are owned by the cloud tenant and not the cloud operator.
3. Allocation Pool:
 - Organization VDC is allocated a “container” set of resources.
 - Organizations have a very simple model of resources, and advanced resource management controls, such as Shares and Reservations, are managed by the cloud operator, which enables a more coherent resource management across organizations.

To set up organization VDCs, these steps were performed:

1. Select required organizations.

New Organization vDC

Select Organization

An organization vDC provides an organization with the resources it needs. For which organization is this organization vDC being created?

Organization:

Organization	Full Name	Description
IntelIT	IntelIT	
Sales	Sales	

1-2 of 2

Back Next Finish Cancel

Figure 25 - Select Organization

2. Select the Provider VDC.

New Organization vDC

Select Provider vDC

You can allocate resources to an organization by creating an Organization vDC that is partitioned from a Provider vDC. From which Provider vDC is this Organization vDC partitioned?

Provider vDC:

Provider vDC	Processor (Used/Total)	Memory (Used/Total)	Storage (Used/Total)
VDC1	0%	0%	16.44%

1-1 of 1

The following networks are available to the Provider vDC you selected:

Network	Gateway	Subnet	DNS
External Network	10.223.128.62	255.255.255.192	10.223.128.69

Selected Provider vDC: VDC1

Back Next Finish Cancel

Figure 26 - Provider VDC

3. Select the “Pay-As-You-Go” allocation model with the default settings.

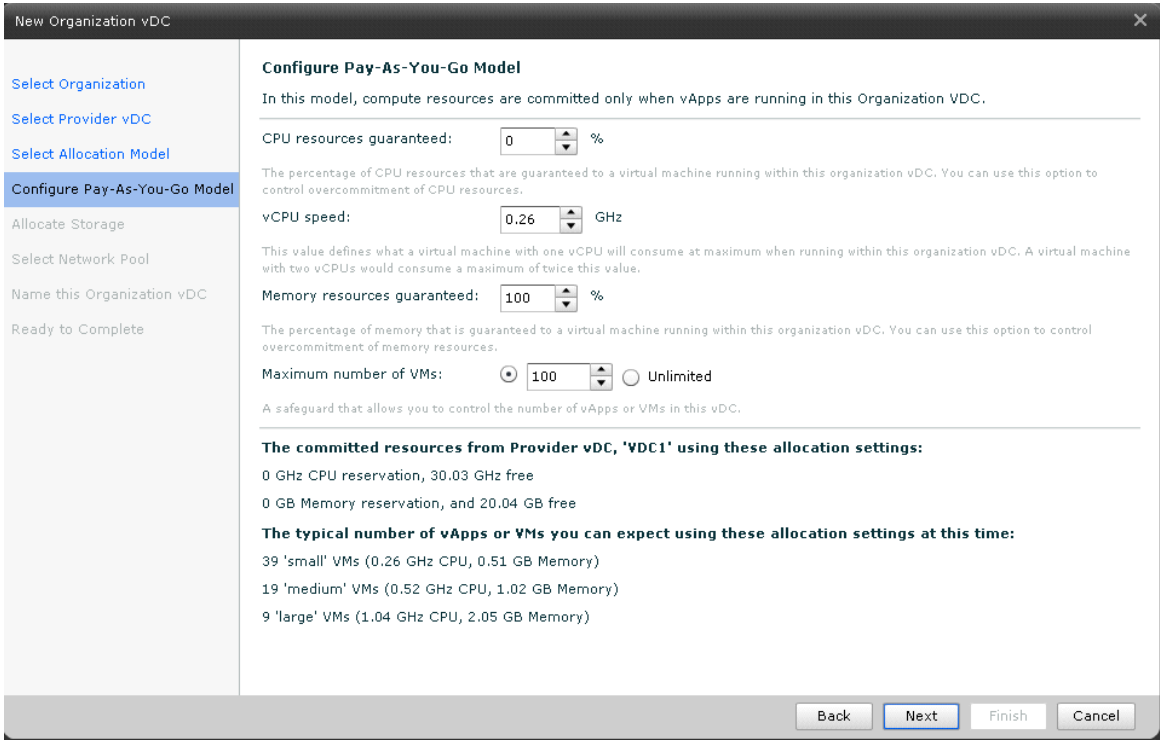


Figure 27 - Provider Configuration

4. Enable thin provisioning for storage allocation. Leave the network pool blank, provide a name for the organization VDC and click “Finish.”

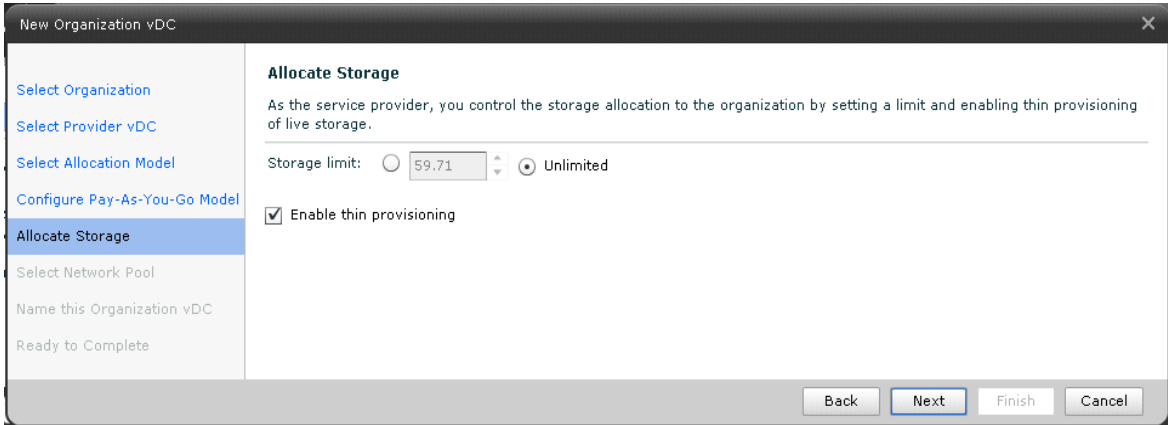


Figure 28 - Storage Allocation

5. Validate to ensure the organizational VDC is created and enabled.

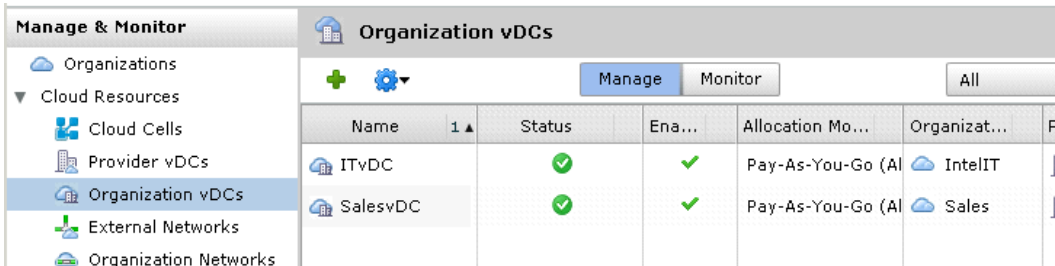


Figure 29 - View VDCs

6. View VMware vSphere inventory, which will show newly created organization VDC folders.

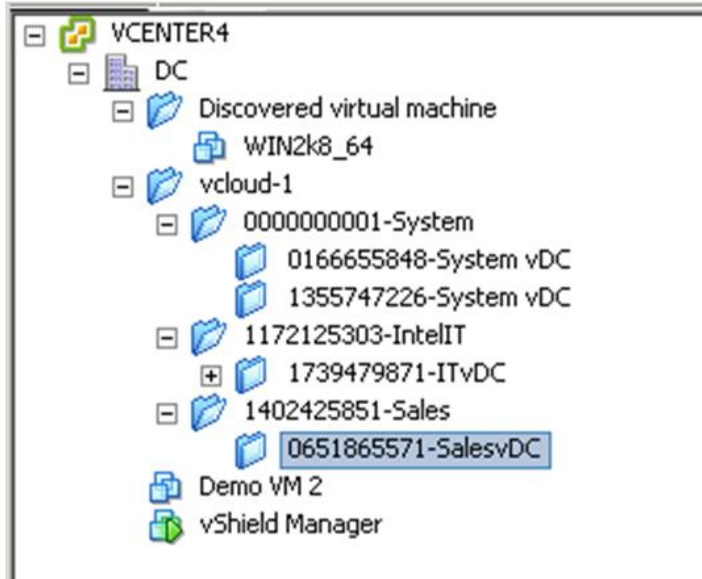


Figure 30 - VMware vSphere* Inventory

Create Organizational Networks

Organization Networks are used by vApps inside the organization to communicate with each other or communicate with shared services outside the organization. Organization networks can be of three different types:

- **Internal:** Connectivity to vApps within the organization. No external connectivity.
- **Externally Routed:** Connectivity to vApps and services on a shared external network. VMware vShield Edge* device is deployed outside the organization to provide NAT and firewall services for vApps inside the organization SETUP CATALOGS.
- **External Direct Connect:** Connectivity to vApps and services on a shared external network. vApps get IP addresses on the external network. No NAT or firewall exists between the organization vApps and other vApps on the external network.

For this scenario, one external direct connect organization network is created.

1. Select the “Direct connection” option to create the external organizational network.

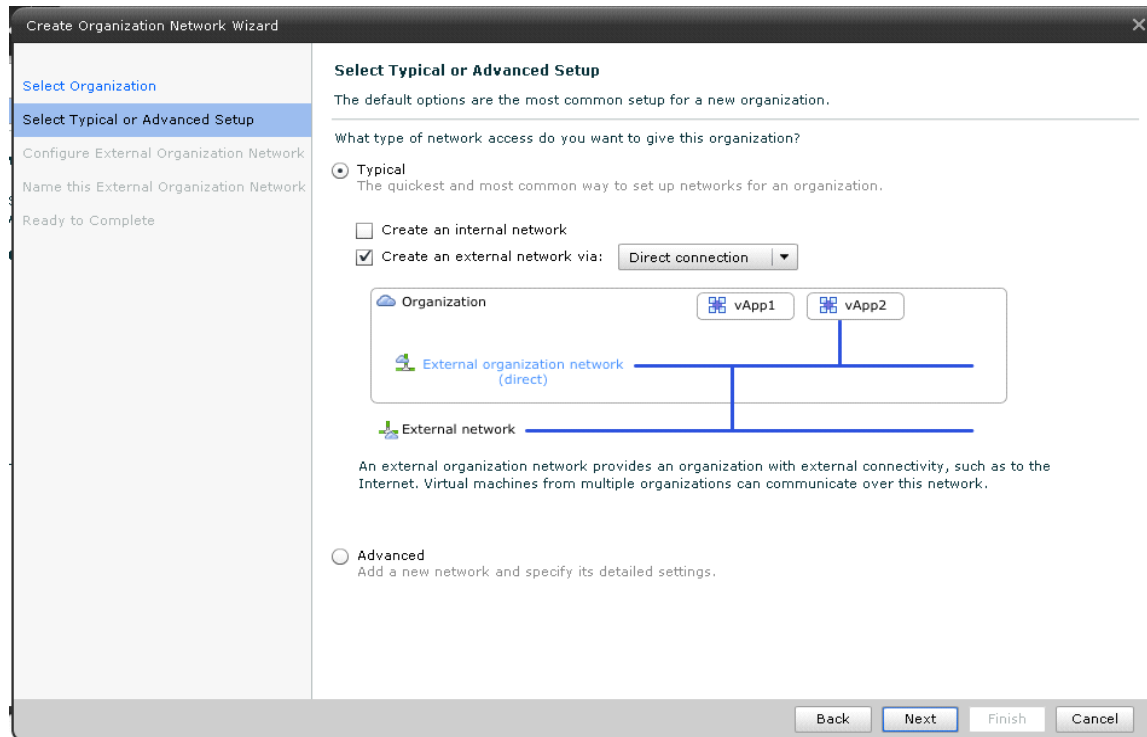


Figure 31 - Create Organizational Network

2. Select the external network, configure with the appropriate information, then click “Finish”.

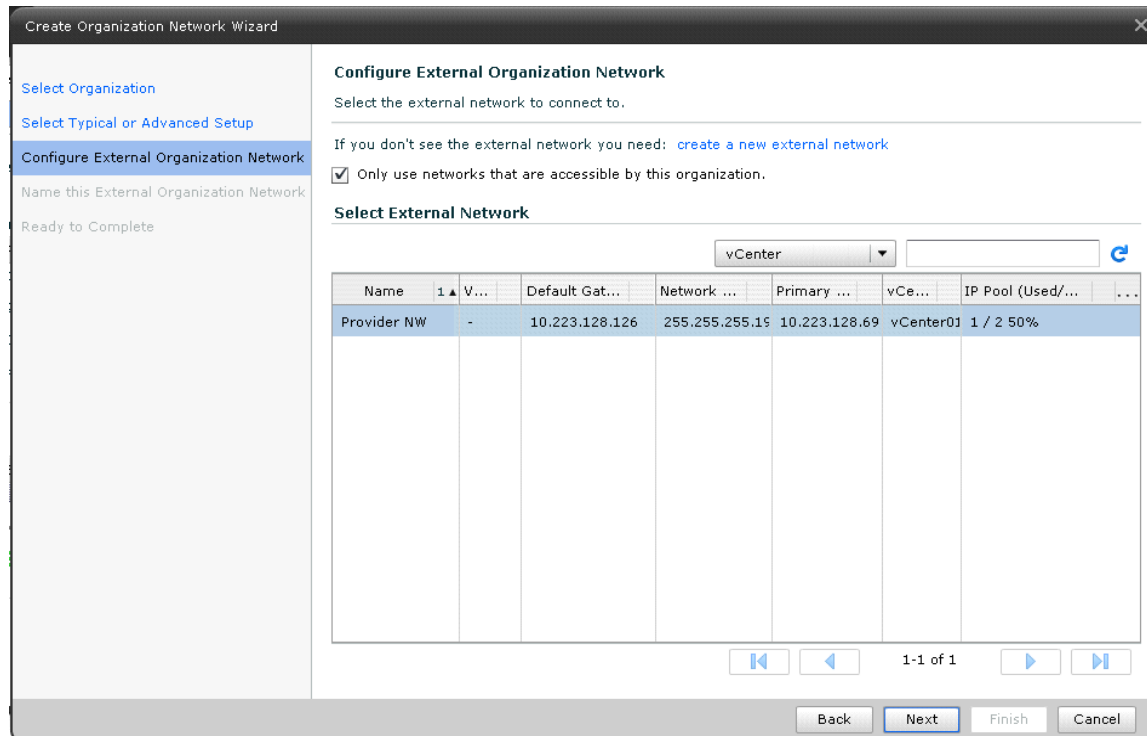


Figure 32 - Configure External Network

3. Validate to ensure the new organizational network is created.

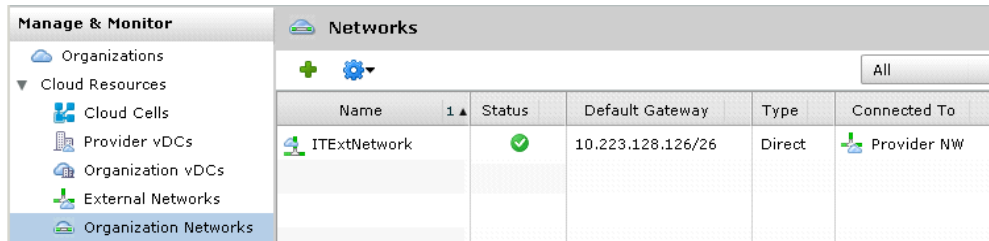


Figure 33 - View Network

Create Catalogs

Catalogs are used to offer vApps and media to end users for self-service. IT can build standardized offerings of VM and application environments and upload them to the catalog. Catalogs are created by organization administrators or catalog authors, and can be shared or published. When a catalog is shared, it can be set up to be accessible by one or more members of an organization. When a catalog is published, it can be accessed by other authorized organizations in the private cloud. vApps can be created in organization catalogs using three methods:

1. A cloud administrator can copy VMs and templates from the underlying VMware vSphere infrastructure.
2. An organization administrator can copy a vApp in OVF format from local disk to the private cloud.
3. An organization administrator, catalog author, or vApp author can create vApps from scratch in the private cloud. They can create VMs and install the guest operating system (GOS) and application. Only organization administrators and catalog authors can add items to the catalog.

For this scenario, VMs and templates were imported from VMware vSphere*. This assumes VMs and templates are available in the VMware vSphere environment to import into VMware vCloud Director*.

1. Select the organization in which a catalog will be created. Click the green plus sign.

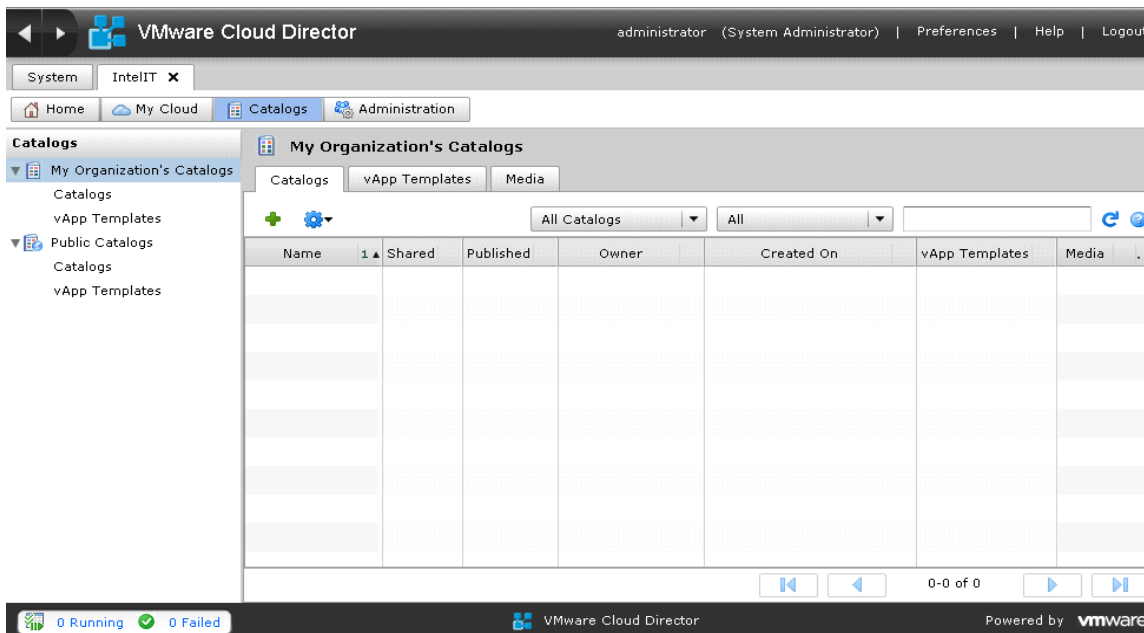


Figure 34 - View Organization Catalog

2. Select appropriate members, access level, publish, then click “Finish”.

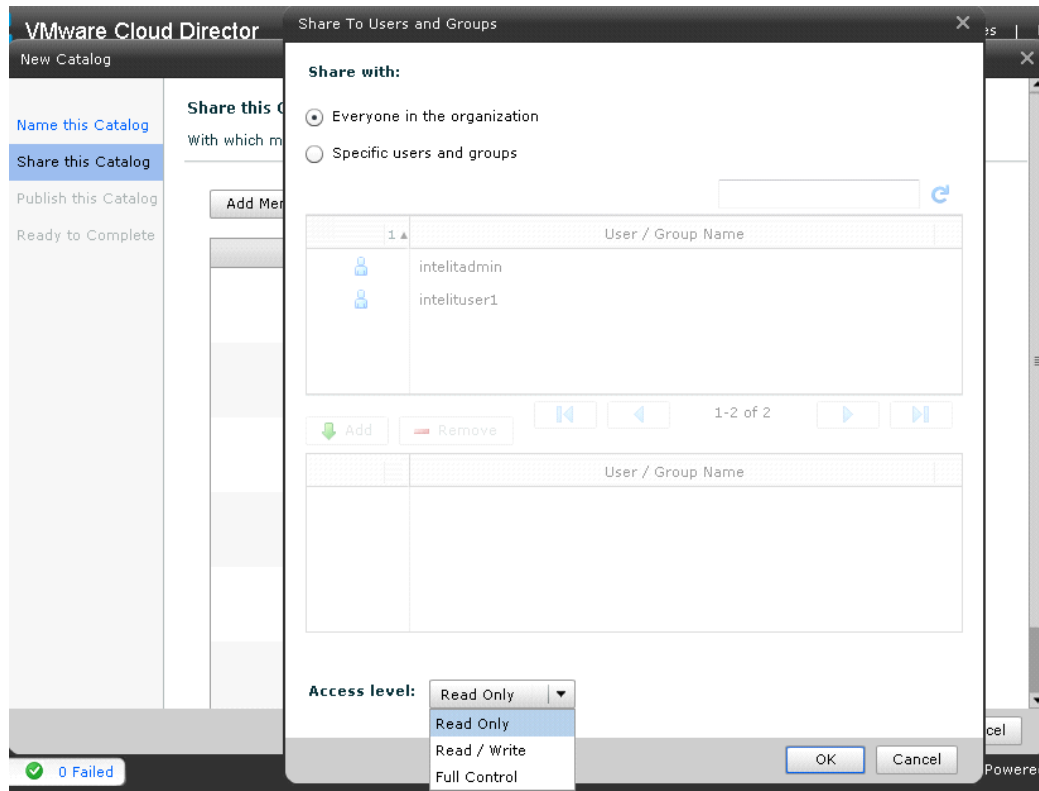


Figure 35 - Select Users/Members

3. Import vApp template from VMware vSphere*.

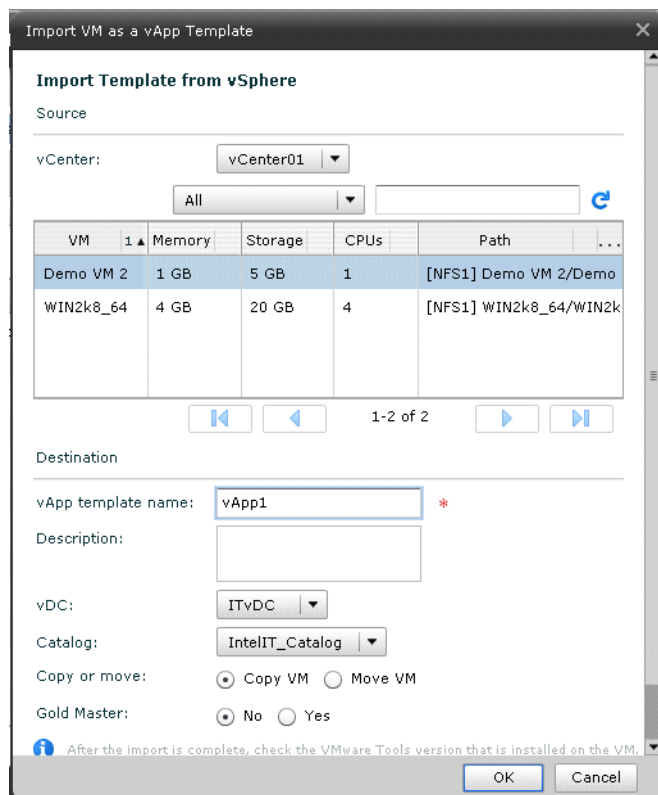


Figure 36 - Import Screen

4. Validate to ensure the catalog is created.

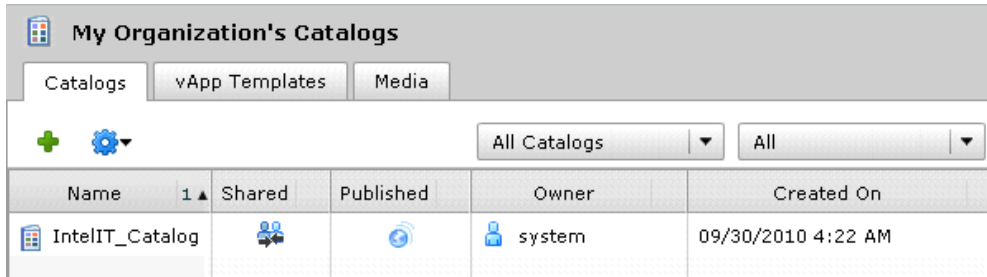


Figure 37 - View Catalog

Use Infrastructure as a Service

Now that the VMware vCloud Director* based cloud is set up and vApp templates are provisioned in the catalog, users can now use Infrastructure as a Service (IaaS). In this final scenario, a user will log into the Intel IT organization, browse the catalog, copy a vApp template from the catalog to the user's cloud (self-service), and connect the vApp to an external network.

1. Login to the appropriate home screen.

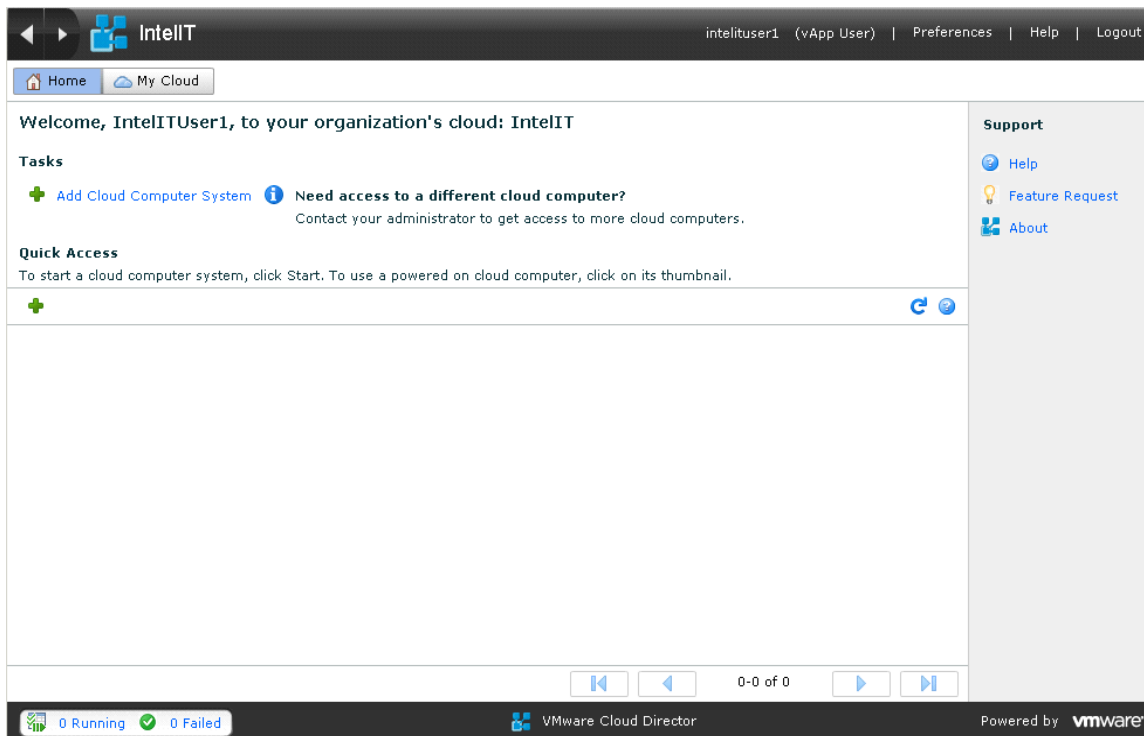


Figure 38 - Home Screen (Self-Service Portal)

2. Select the vApps from the catalog.

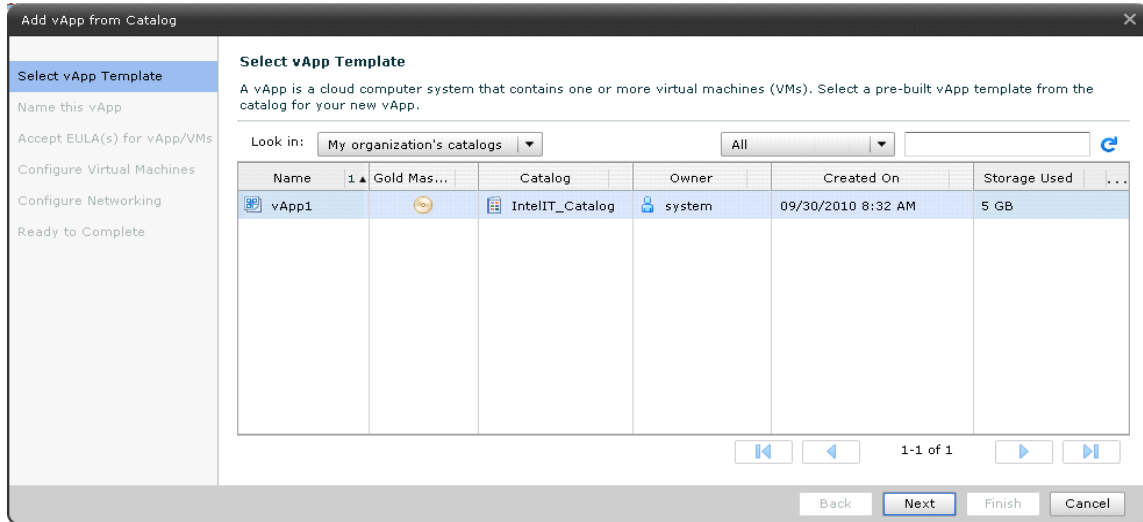


Figure 39 - Template Selection

3. Select the organizational VDC and associated networks, initiate a full copy of the vApp from the catalog to the organization, then click "Start" to power on the vApp.

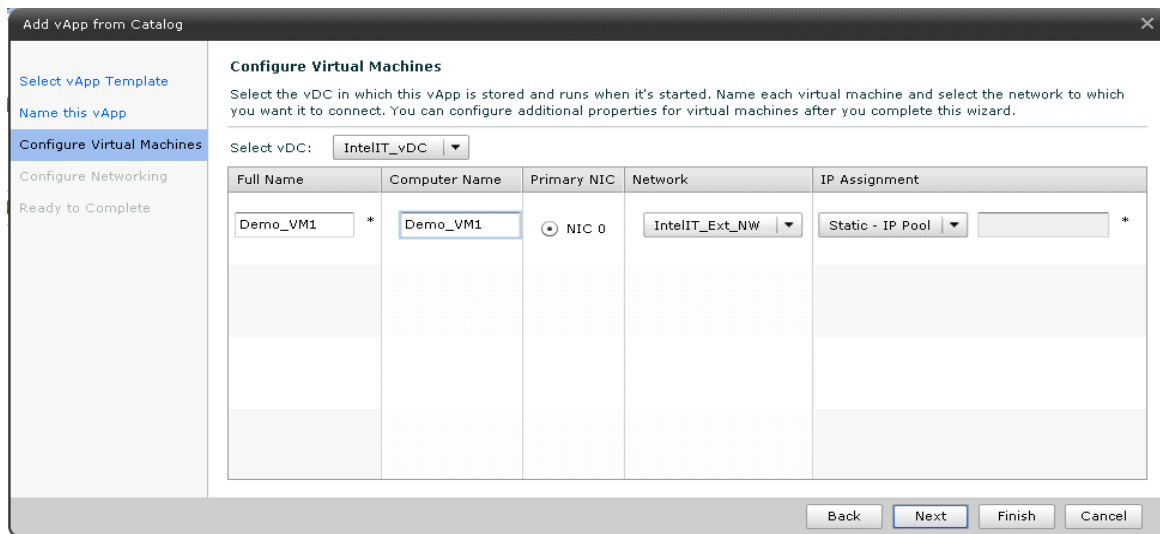


Figure 40 - Configure Virtual Machines

4. Verify the vApp is deployed and powered on. Click on the thumbnail to launch the Remote Console.

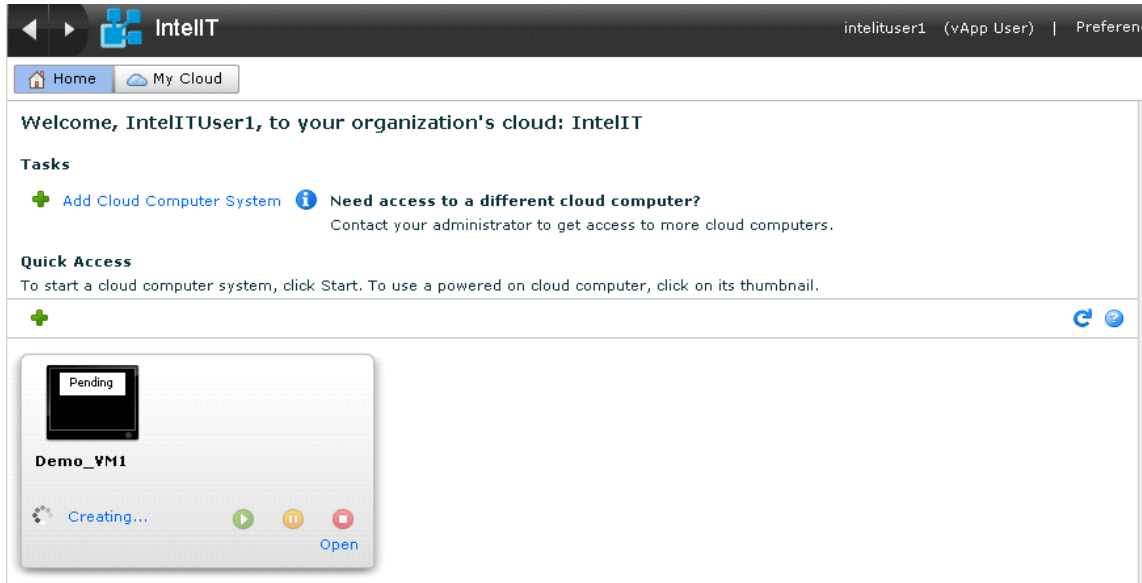


Figure 41 - Deploy vApp

5. Verify vApp is deployed in VMware vSphere*.

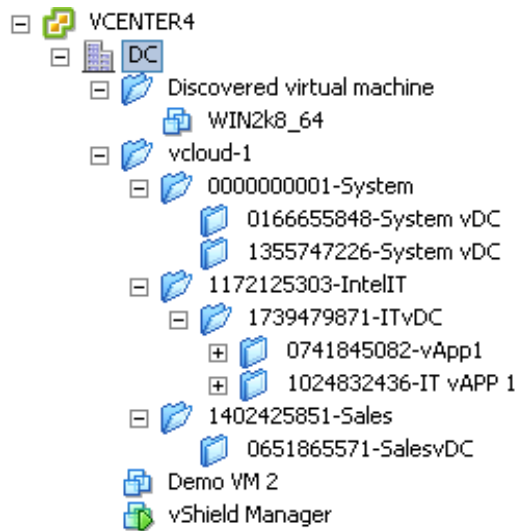


Figure 42 - View vApp

Dynamic Scaling

Now that the IaaS service runs, this test case describes scaling the compute capability of the VMware vCloud Director* as additional VMware ESX* nodes are added to the underlying VMware vCenter*.

1. Figure 43 depicts a new ESX* host has been added to the VMware vCenter*.

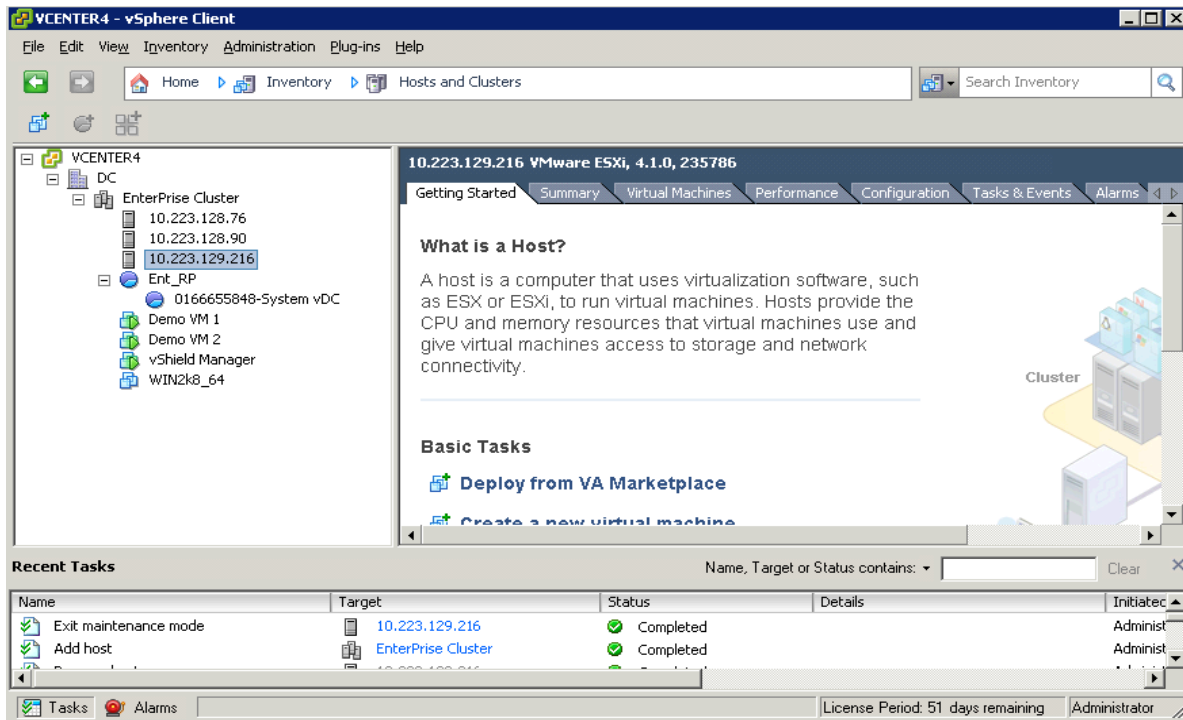


Figure 43 - Add New Host

2. VMware vCloud Director automatically recognizes and prepares the new VMware ESX host. No additional configuration is required.

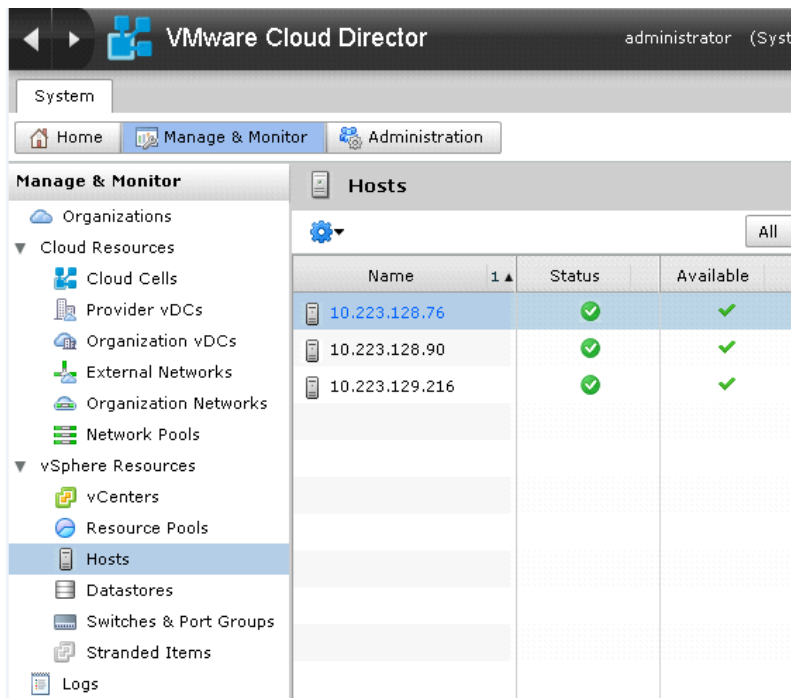


Figure 44 - Manage Hosts

Termination of vApp

The deployed vApps within an organization can be terminated either automatically or manually. When the vApp is initially deployed, the lease period for the vApp can be defined. After the lease period is completed, the vApp is automatically stopped and the resources are freed-up. The administrator or the vApp user also has privileges to delete the vApp at any point in time.

1. View the lease configuration for vApp that is deployed.

Add vApp from Catalog

Select vApp Template

Name this vApp

A vApp is a cloud computer system that contains one or more virtual machines (VMs). Name and describe this vApp and set its leases.

Name: *

Description:

Leases

Runtime lease: Days Expires on: Thu Oct 7 22:54:46 GMT+0530 2010 *

How long this vApp can run before it is automatically stopped.

Storage lease: Days Expires on: Sat Oct 30 22:54:46 GMT+0530 2010 *

When this vApp is stopped, how long it is available before being automatically cleaned up.

Back Next Finish Cancel

Figure 45 - View vApp

2. View how vApp can be manually stopped and deleted if needed.

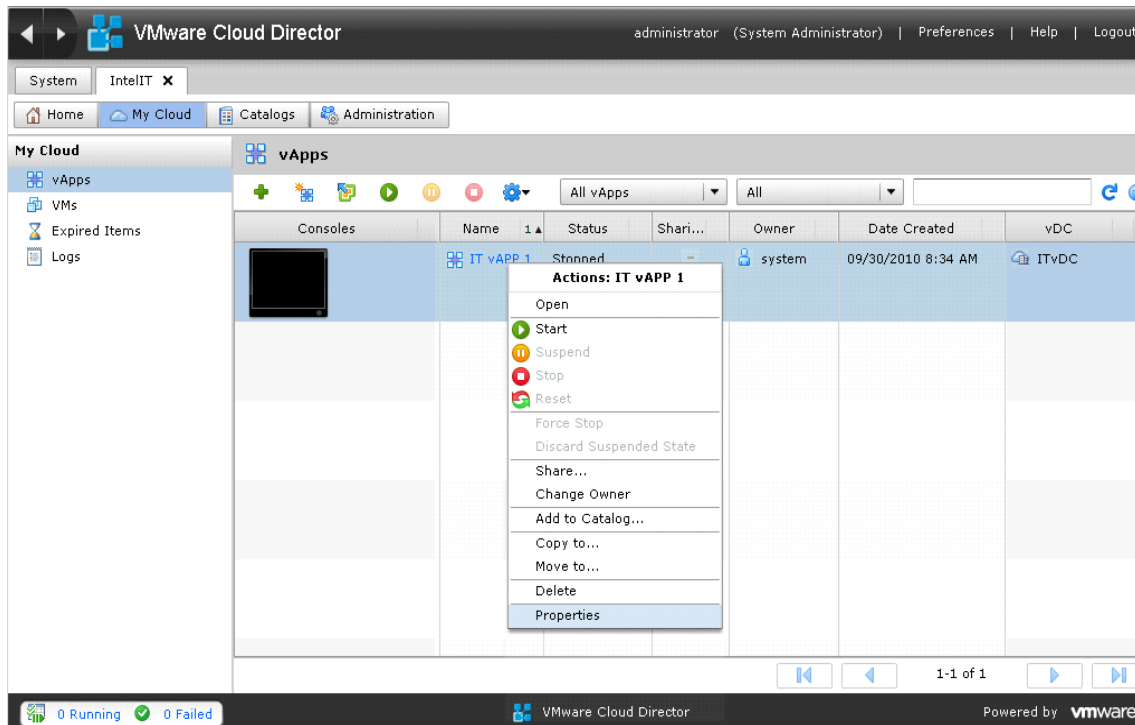


Figure 46 - vApp Properties

Separation of Roles and Responsibilities

VMware vCloud Director* has about five predefined roles that can be assigned to users, each with a certain set of privileges. Figures 47 and 48 show the privileges of users with the administrative role compared to users with the vApp user role. An organization administrator has complete privileges on the organization.

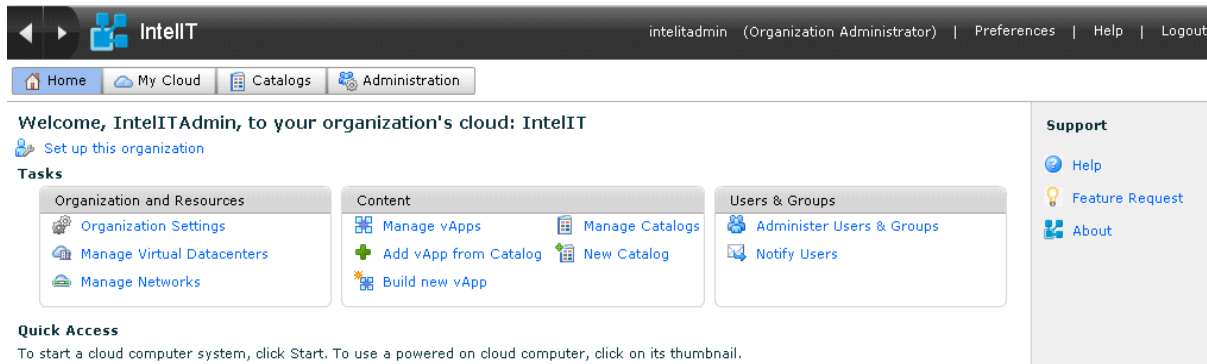


Figure 47 - Organization View

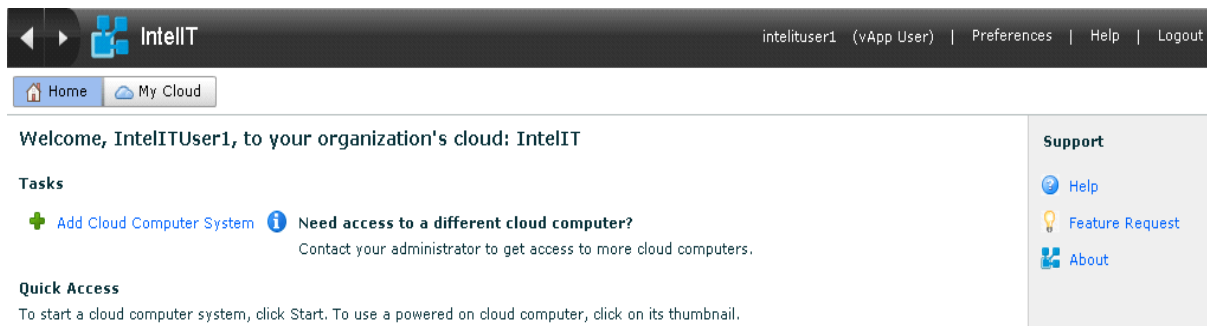


Figure 48 - User Role

A user with a vApp user role can instantiate a new vApp and control the same. Other than that, the user will not have any privileges.

Notification and Alerts

VMware vCloud Director* provides the ability for the system administrator or the organization administrators to send notifications.

1. Login to VMware vCloud Director* console either as "System administrator" or "Organization administrator."
2. Click "Notify Users."
3. View the different options that the system administrator has to send out notifications.

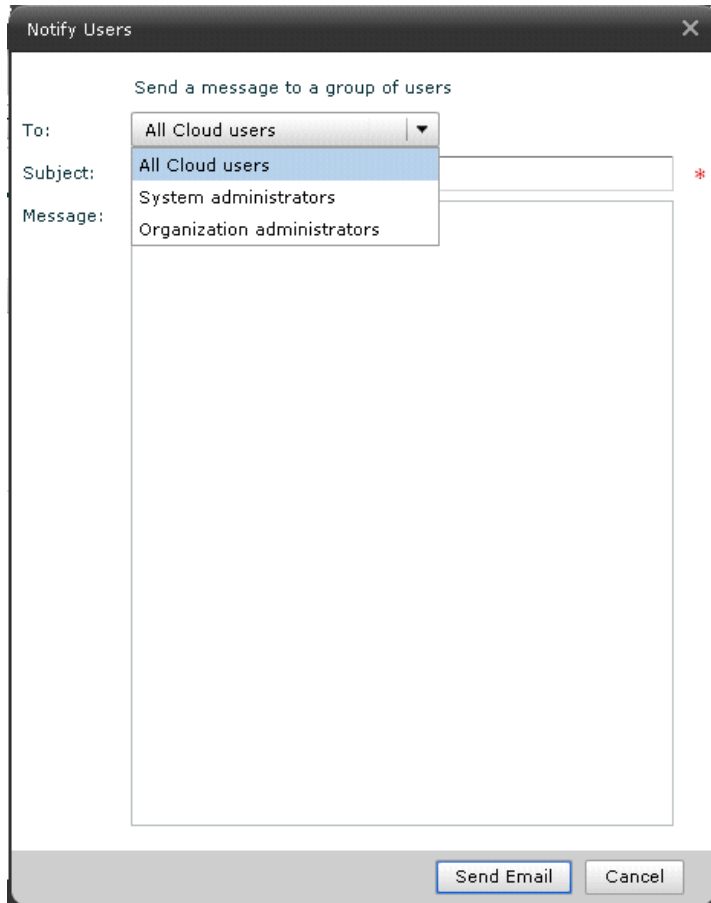


Figure 49 - Notify Users

Next Steps

Scalability of the Application Level

VMware vCloud Director* supports scalability at both physical and application infrastructure levels. Additional VMware vCloud Director cells can be added into the VMware vCloud Director cluster as needed. Additional VMware vCenter* and VMware ESX* servers can also be added to increase the compute capacity of the environment. Explore the application-level scaling where additional VMware vCloud Director cells can be added to the VMware vCloud Director cluster to support scaling of end users who access the VMware vCloud Director either

through the self-service UI or through the VMware vCloud API.

Additional Usage Models

This guide focuses on the usage models that use the basic functionality of VMware vCloud Director*. Additional usage models that integrate other VMware products like VMware vCenter Chargeback* and VMware vCenter Orchestrator* were not explored. With VMware Chargeback, detailed monitoring of the resource usage can be accomplished for billing. VMware Orchestrator can help define usage models with respect to automation of service deployment, notification, etc.

Planning Considerations

Hardware

A full discussion of processor and overall server performance considerations is beyond the scope of this guide. However, it is important to note that the performance of virtual machines that use a virtualized platform is heavily influenced by factors of processor architecture and specific feature sets available in the processor. It is strongly recommended to use high performance server processors equipped with virtualization and I/O support feature sets, such as the Intel® Xeon® processor 5600 series, which also supports Intel® Intelligent Node Manager and Intel® Trusted Execution Technology (Intel® TXT),.

For more details on Intel® Virtualization technologies please refer to http://download.intel.com/business/resources/briefs/xeon5500/xeon_5500_virtualization.pdf.

Network Technology Architecture

For the infrastructure test bed, 1 GbE connections were used for service console/virtual machine and storage. Depending on the customer requirements and usage, production environments might benefit from using 10 GbE for virtual machine networks.

Storage Architecture

For cost effectiveness and simplicity, a NFS store was used as a shared storage to store virtual machine images. For production deployments, other alternatives might need to be chosen based on performance, cost, and other factors. The performance of the storage nodes and hypervisor nodes (when local storage is utilized), as well as the overall power consumption of the cloud deployment, may be favorably impacted by the use of Solid State Drives. This was not specifically tested.

Security

Security is one of the key considerations in today's virtualized or bare-metal server deployments. In a cloud deployment scenario, from the perspective of both service provider and service consumer, recommendations include systems that support Intel® TXT (Intel® Xeon® Processor 5600 series) and software such as VMware vSphere* Hypervisor (VMware ESXi* 4.1) to ensure protection against hacking and unauthorized access.

Software

This guide is not meant to substitute for product documentation. For detailed information regarding installation, configuration, administration, and usage of VMware* products, please refer to the online documentation. Consult the online Knowledge Base regarding any additional

questions. For further assistance, please contact a VMware* sales representative or channel partner. Below are links to online resources, documentation and self-help tools:

- VMware vSphere* and VMware vCenter Server* Resources:
 - Product Overview: <http://www.vmware.com/products/vsphere/>
 - Product Documentation: http://www.vmware.com/support/pubs/vs_pubs.html
 - VMware vSphere* Documentation (including hardware compatibility guides): http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esx40_vc40.html
- VMware* Whitepapers and Technical Papers:
 - vSphere Evaluator guide: <http://www.vmware.com/resource/techresources/10020>
- VMware vCloud Director* Resources:
 - Product Overview: <http://www.vmware.com/products/vcloud-director/>
 - Product Documentation: http://www.vmware.com/support/pubs/vcd_pubs.html
 - Installation and Configuration Guide: http://www.vmware.com/pdf/vcd_10_install.pdf
 - Administrator's Guide: http://www.vmware.com/pdf/vcd_10_admin_guide.pdf
 - User's Guide: http://www.vmware.com/pdf/vcd_10_users_guide.pdf
- VMware vCloud Director Community: <http://communities.vmware.com/community/vmtn/vcd>
- Support Knowledge base: <http://kb.vmware.com>

VMware vCenter Server*, VMware vShield Manager* and VMware vCloud Director*

This guide assumes the following software is installed:

- At least one evaluation or licensed VMware vCenter Server* Standard.
- At least two VMware vSphere* Enterprise Plus evaluations or licensed VMware ESXi*/ESX* Servers.
- One or more VMs in the VMware vSphere* environment with guest operating system (GOS) installed which will be imported into VMware vCloud Director*. For details on installation and configuration of VMware vCenter Server and VMware ESXi/ESX Servers and creation of VMs, please refer to VMware vSphere documentation.
- VMware vShield Manager* 4.1 deployed, licensed, and configured in the VMware vCenter Server*. A license for the VMware vShield Edge* components of VMware vCloud Director* is included with the VMware vCloud Director evaluation. For details on installation of VMware vShield Manager, please refer to the VMware vCloud Director Installation and Configuration Guide.
- VMware vCloud Director* installed and running in a VM or physical machine. For details, refer to the VMware vCloud Director Installation and Configuration Guide.

Additional Information

- Intel® Cloud Builders: <http://software.intel.com/en-us/articles/intel-cloud-builders/>
- Intel® Xeon® processors: <http://intel.com/xeon>
- TAROX comp. profile: <http://www.tarox.de/index.php?id=3628>
- TAROX ParX* Server product range: <http://www.tarox.de/index.php?id=93&L=0>
- TAROX Solutions - contact: <http://www.tarox.de/index.php?id=2659>

Glossary

To avoid ambiguity about the terms used, here are the definitions for some of the specific concepts used in this guide⁷:

- vCloud® Organization: A vCloud® organization is a unit of administration for a collection of users, groups, computing resources, and deployment of service.
- vCloud Users and Groups: An organization can contain an arbitrary number of users and groups. Users can be created by the organization administrator or imported from a directory service such as LDAP.
- Groups must be imported from the directory service. Permissions within an organization are controlled through the assignment of rights and roles to users and groups.
- vCloud® Networks: An organization can be provisioned with one or more networks. These organization networks can be configured to provide services such as DHCP, NAT, and firewalls.
- vCloud VDC: A vCloud® VDC is an allocation mechanism for resources such as storage, processors, and memory. In a VDC, computing resources are fully virtualized, and can be allocated based on demand, service level requirements, or a combination of the two. There are two kinds of VDCs:
 - Provider VDCs: These VDCs contain all the resources available from the vCloud® service provider. Provider VDCs are created and managed by vCloud system administrators.
 - Organization VDCs: These VDCs provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual media, such as floppy disks and CD ROMs.
- vCloud® Catalogs: Catalogs contain references to virtual systems and media images. A catalog can be shared to make it visible to other members of an organization, and can be published to vApp: A vApp contains one or more individual virtual machines, along with parameters that define operational details such as:
 - The order in which individual virtual machines are powered on or off.
 - End-user license agreement terms for each virtual machine.
 - Deployment lease terms (typically inherited from the containing organization) that constrain the vApp's consumption of VDC resources.
 - Access control information which specifies which users and groups can perform operations such as deploy, power on, modify, and suspend on the vApp and the virtual machines it contains.
- How the contained virtual machines are connected to each other and to external networks.

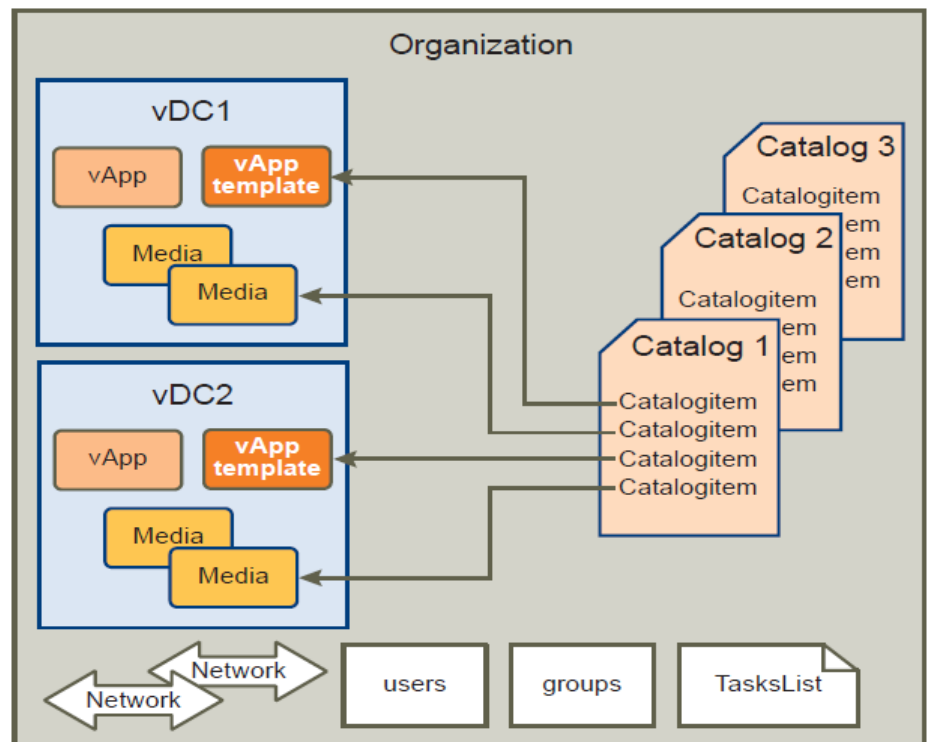


Figure 50 - Logical Definition Map

Endnotes

¹ Intel® Xeon® Processor 5500 series software industry testimonials:
<http://www.intel.com/business/software/testimonials/xeon5500.htm>

² Intel® Virtualization Technology, <http://www.intel.com/technology/virtualization/> and http://download.intel.com/business/resources/briefs/xeon5500/xeon_5500_virtualization.pdf

³ Intel® Xeon® Processor 5000 series product support:
<http://www.intel.com/support/processors/xeon5k/>

³ Intel® Xeon® Processor 5600 series product information:
<http://ark.intel.com/ProductCollection.aspx?series=47915>

⁴ VMware vMotion* Requirements:
http://pubs.vmware.com/vi3/resmgmt/www/help/wwhimpl/common/html/wwhelp.htm?context=resmgmt&file=vc_create_cluster.7.4.html

⁵ VMware vCloud Director* Product Page:
<http://www.vmware.com/products/vcloud-director/>

⁶ *VMware vCloud Director Installation and Configuration Guide*:
http://www.vmware.com/pdf/vcd_10_install.pdf

⁷ *VMware vCloud API Programming Guide*:
http://www.vmware.com/pdf/vcd_10_api_guide.pdf

⁸ TAROX ParX* R2080i Server product information:
<http://www.tarox.de/index.php?id=3631&L=0>

⁹ TAROX ParX* R1080i Server product information:
<http://www.tarox.de/index.php?id=3633&L=0>

To learn more about deployment of cloud solutions, visit <http://software.intel.com/en-us/articles/intel-cloud-builders/>

Disclaimers

^Δ Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

^² Hyper-Threading Technology requires a computer system with an Intel processor supporting Hyper-Threading Technology and an HT Technology enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. See <http://www.intel.com/info/hyperthreading/> for more information including details on which processors support HT Technology.

[◊] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, Xeon, Xeon inside, Intel Data Center Manager, Intel Cloud Builder Test Bed, Intel Trusted Execution Technology, Intel Advanced Encryption Standard-New Instructions, and Intel Intelligent Power Node Manager are trademarks of Intel Corporation in the U.S. and other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

*Other names and brands may be claimed as the property of others.

