VMware vCloud® Architecture Toolkit

Private VMware vCloud Implementation Example

Version 2.0.1

October 2011

vmware®

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Overview 7
1.1 Business Requirements 7
1.2 Use Cases 8
1.3 Document Purpose and Assumptions 8
1.4 vCloud Components 10
1.5 Abstractions and VMware vCloud Constructs 11
2. vSphere Design 12
2.1 Architecture Overview 12
2.2 Site Considerations 16
2.3 Management Cluster Design 16
2.4 Resource Group Design 21
3. vCloud Design – Provider Constructs 32
3.1 Provider Virtual Datacenters 32
3.2 External Networks 36
3.3 Network Pools 36
3.4 Users and Roles 37
4. vCloud Design – Consumer Constructs 38
4.1 Organizations 38
4.2 Organization Virtual Datacenters 38
4.3 Organization Networks 40
4.4 Catalogs 42
4.5 vApps 43
4.6 Organization Users and Roles 47
5. vCloud Security 49
5.1 vSphere Security 49
5.2 Additional Security Considerations 50
6. vCloud Management 51
6.1 vSphere Host Setup Standardization 51
6.2 VMware vCloud Director Logging 51
6.3 vShield Edge Logging 52
6.4 vSphere Host Logging 53
6.5 vCloud Monitoring 54

7. Extending vCloud 55
7.1 vCloud Connector 55
7.2 vCloud API 56
7.3 Orchestrating vCloud 57
7.4 VMware Service Manager Cloud Provisioning (VSM CP) 57
8. Metering 59
8.1 Silver Level of Service – Cost Configuration 60
8.2 Gold Level of Service – Cost Configuration 61
Appendix A: Bill of Materials 62

List of Figures

Figure 1. VMware vCloud Director Abstraction Layer 11
Figure 2. vSphere Logical Architecture Overview 14
Figure 3. vCloud Physical Design Overview 15
Figure 4. vSphere Logical Network Design – Management Cluster 20
Figure 5. vSphere Logical Network Design 24
Figure 6. Provider Virtual Datacenters and vSphere Resources 32
Figure 7. Organization Virtual Datacenter 39
Figure 8. Organization Network Design 41
Figure 9. Catalog Architecture 42
Figure 10. vApp Connectivity Options 45
Figure 11. vCloud Connector 55
Figure 12. vCloud API Logical Representation 56
Figure 13. vCloud Orchestration 57
Figure 14. VMware Service Manager 58
Figure 15. vCenter Chargeback Logical Diagram 59

List of Tables

Table 1. Document Sections 9
Table 2. vCloud Components 10
Table 3. Document Sections for vCloud Components 13
Table 4. vCenter Management 16
Table 5. Management Virtual Machines 16
Table 6. Management Component Resiliency 17
Table 7. vSphere Clusters – Management Cluster 18
Table 8. Host Logical Design Specifications – Management Cluster 19
Table 9. Virtual Switch Configuration – Management Cluster 19
Table 10. Virtual Switch Configuration Settings – Management Cluster 20
Table 11. Shared Storage Logical Design Specifications – Management Cluster 21
Table 12. Resource Group Clusters 21
Table 13. vSphere Cluster Configuration 22
Table 14. Host Logical Design Specifications 23
Table 15. Virtual Switch Configuration 24
Table 16. vdSwitch01 Teaming and Failover Policies 25
Table 17. Storage Logical Design Specifications – Cloud Compute Cluster 1 26
Table 18. Storage Logical Design Specifications – Cloud Compute Cluster 2 26
Table 19. Compute Cluster Shared Storage Physical Design 27
Table 20. vSphere Clusters – Cloud Compute Datastores 28
Table 21. Datastore Size Estimation Factors – vcdgold-Compute01 Cluster 29
Table 22. Datastore Size Estimation Factors – vcdsilv-Compute01 Cluster 29
Table 23. SIOC Disk Shares 30
Table 24. NewCo Provider Virtual Datacenters 33
Table 25. Provider Virtual Datacenter to vSphere Mapping 34
Table 26. vCloud External Networks 36
Table 27. Provider Users and Roles 37
Table 28. NewCo vCloud Organizations 38
Table 29. Organization Virtual Datacenter Configuration 39
Table 30. EIT Organization Networks 41
Table 31. AES Organization Networks 41
Table 32. Virtual Machine Sizing and Distribution 46
Table 33. EIT Users and Roles 48

Table 34. AES Users and Roles 48
Table 35. Virtual Switch Security Settings 49
Table 36. VMware vCloud Director Monitoring Items 54
Table 37. NewCo Chargeback Billing Policies 60
Table 38. NewCo Pay-As-You-Go Fixed Cost Model 60
Table 39. Reservation Cost Model 61
Table 40. Management Cluster Inventory 62
Table 41. Cloud Resources Inventory 64

1. Overview

This private VMware vCloud® implementation example uses a fictitious corporation, New Company (NewCo), to provide a detailed implementation example for a private VMware vCloud. It is intended to provide architects and engineers who are interested in implementing a private vCloud with a reference implementation that conforms to VMware best practices, and describes the logical and physical design of the components of a vCloud. Each document section elaborates on different aspects and key design decisions of this Infrastructure as a Service (IaaS) solution. This document provides a baseline that is extensible for future usage patterns.

NewCo is a large software manufacturer specializing in accounting and financial software for small- to medium-sized businesses. NewCo operates a large primary datacenter and has virtualized nearly 85% of all workloads over the past four years. NewCo is currently challenged with developing a self-service internal vCloud to increase the speed with which the Enterprise Information Technology (EIT) and Application Engineering Solutions (AES) departments can bring applications and services to market. To provide their internal business units with a more agile environment so that they can quickly react to changing market conditions, NewCo wants to move towards a private vCloud model.

1.1 Business Requirements

The NewCo vCloud design has the following characteristics and provides:

- Compute capacity to support about 700 virtual machines and approximately 500 vApps, which are estimated for deployment or migration from vSphere within the first year.
- Definition and creation of five predefined vApps that will be composed of existing virtual machines and will serve as initial vApp building blocks for template creation.
- Secure multitenancy for EIT and AES departments including tenant network isolation and permitting business units within NewCo to share compute resources. Two distinct levels of service are available for consumers to choose from; both can be expanded based on increased demand.
- An end user-facing self-service portal where Infrastructure as a Service can be consumed from a catalog of predefined applications (vApp templates).
- The ability to rapidly provision complex multitier applications or entire environments to respond to dynamic business requirements.
- Maintain and enforce the current physical network isolation between production and development networks across the virtual and vCloud infrastructure.
- A chargeback mechanism, so resource consumption can be metered and the associated cost provided back to the appropriate organization or business unit.

See the *Private VMware vCloud Service Definition* for additional details.

1.2 Use Cases

The target use case for the NewCo vCloud includes the following workloads:

- Development
- Pre-production
- Demonstration
- Training
- Tier 2 and Tier 3 IT infrastructure applications

1.3 Document Purpose and Assumptions

This private vCloud implementation example is intended to serve as a reference for architects, and assumes a level of familiarity with VMware products, including VMware vSphere®, VMware vCenter™, and VMware vCloud® Director™ (VCD). It covers both logical and physical design considerations for all VMware vCloud infrastructure components. Each document section elaborates on different aspects and key design decisions of the IaaS solution.

The vCloud architecture described in this document is covered in the sections listed in Table 1.

Table 1. Document Sections

Section	Description
1. Overview	Requirements, overview, and inventory components that comprise the vCloud solution.
2. vSphere Design	• Management cluster – vSphere and vCenter components that support running workloads. • Resource group – vSphere and vCenter components for vCloud consumption comprised of one or more vSphere clusters. Both sections are organized by compute, networking, and shared storage. Logical and physical design specifications and considerations are covered.
3. vCloud Design – Provider Constructs	• VMware vCloud Director provider objects and configuration. • Relationship of vCloud Director provider objects to vSphere objects.
4. vCloud Design – Consumer Constructs	• VMware vCloud Director organization objects and configuration. • Relationship of consumer objects to underlying provider objects.
5. vCloud Security	Considerations that apply to vCloud Director security.
6. vCloud Management	Considerations that apply to vCloud Director management components.
7. Extending vCloud	Available options for increasing the functionality, automation, and orchestration of the vCloud.
8. Metering	VMware vCenter Chargeback™ design and configuration.

This document is not intended as a substitute for VMware product documentation. See the installation and administration guides for the appropriate product and version for additional information.

1.4 vCloud Components

Table 2 lists the components that comprise the vCloud.

Table 2. vCloud Components

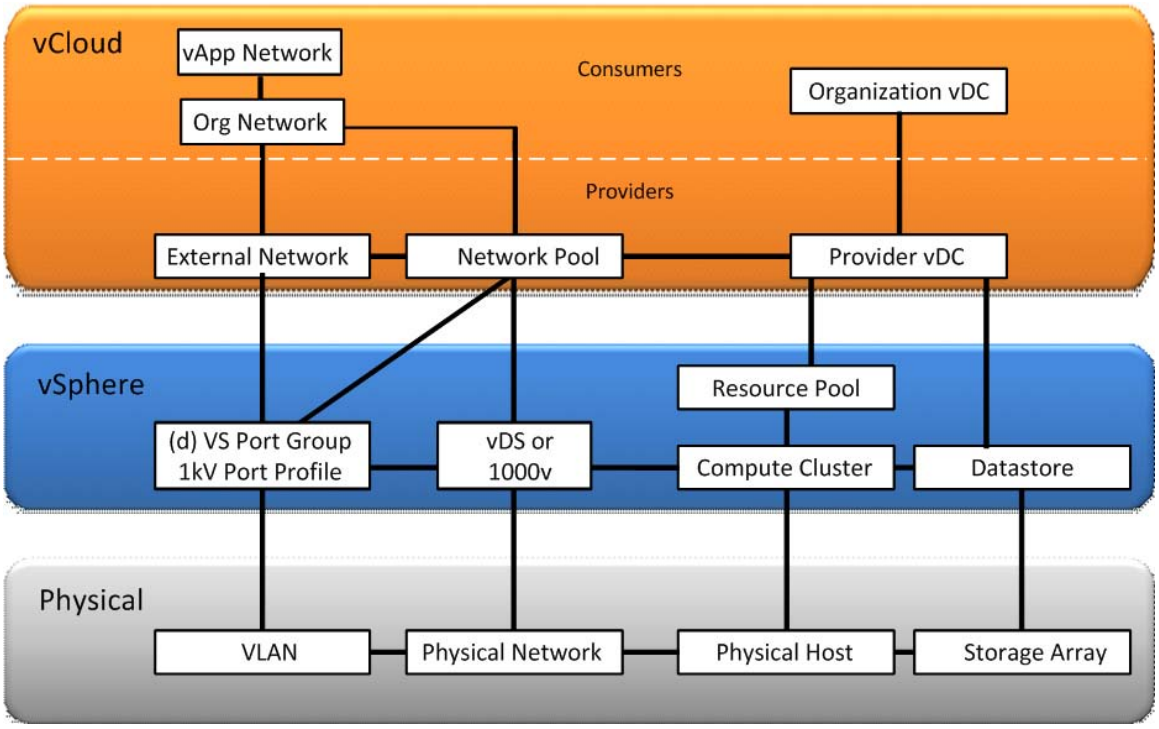
vCloud Component	Description
VMware vCloud Director	Abstracts and provides secure resource and workload isolation of underlying vSphere resources. Includes: • VMware vCloud Director Server (one or more instances, each installed on a Linux virtual machine and referred to as a *cell*). • VMware vCloud Director Database (one instance per clustered set of VMware vCloud Director cells). • vSphere compute, network and storage resources.
VMware vSphere	Foundation of underlying vCloud resources. Includes: • VMware ESXi™ hosts (three or more instances for management cluster and three or more instances for resource cluster, also referred to as Compute Cell). • VMware vCenter Server™ (one instance managing a management cluster of hosts, and one or more instances managing one or more clusters of hosts reserved for vCloud consumption. For a Proof of Concept installation, one instance of vCenter server managing both the management cluster and a single vCloud resource cluster is allowable). • vCenter Server Database (one instance per vCenter Server).
VMware vShield	Provides network security services including Layer 2 isolation, NAT, firewall, DHCP, and VPN. Includes: • VMware vShield Manager™ (one instance per vCenter Server in the vCloud resource cluster). • VMware vShield Edge™ (deployed automatically as virtual appliances on hosts by VMware vCloud Director).
VMware vCenter Chargeback	Provides resource metering and cost models. Includes: • vCenter Chargeback Server (one instance). • vCenter Chargeback Database (one instance). • vCenter Chargeback data collector (one instance). • vCloud data collector (one instance). • vShield Manager data collector (one instance)
VMware vCenter Orchestrator™	Provides infrastructure automation and integration capabilities.

1.5 Abstractions and VMware vCloud Constructs

Key features of the vCloud architecture are resource pooling, abstraction, and isolation. VMware vCloud Director further abstracts the virtualized resources presented by vSphere by providing the following logical constructs that map to vSphere logical resources:

- *Organization* – A logical object that provides a security and policy boundary. Organizations are the main method of establishing multitenancy and typically represent a business unit, project, or customer in a private vCloud environment.
- *Virtual datacenter* – Deployment environments in which virtual machines run.
- *Organization virtual datacenter* – An organization's allocated portion of provider virtual datacenter resources including CPU, RAM, and storage.
- *Provider virtual datacenter* – vSphere resource groupings of compute, storage, and network that power organization virtual datacenters.

Figure 1. VMware vCloud Director Abstraction Layer



2. vSphere Design

2.1 Architecture Overview

The vSphere resource**s** are organized and separated into:

- A management cluster containing all core components and services needed to run the vCloud.
- Two compute clusters that represent dedicated resources each for a predefined level of service for vCloud consumption. Each cluster of ESXi hosts is managed by a vCenter Server, and is under the control of vCloud Director.

Reasons for organizing and separating vSphere resources along these lines are:

- Facilitates quicker troubleshooting and problem resolution. Management components are contained in a relatively small and manageable three-node vSphere cluster.
- Allows for different vSphere feature utilizations and configurations that are specific and more appropriate for one group of workloads over another.
- Provides resource isolation between workloads running in the vCloud and the actual systems used to manage the vCloud.
- Separates the management components from the resources they are managing.
- Eliminates potential resource contention between vCloud and management workloads, which can have amplified effects. Resources allocated for vCloud use have little reserved overhead.
- vCloud resources can be consistently and transparently managed, carved up, and scaled horizontally.

The components that comprise the vCloud are described in the following sections.

Table 3. Document Sections for vCloud Components

vSphere Design Section	vCloud Components
Section 2.3, Management Cluster Design	• vCenter Server 5.0, vCenter cluster, and ESXi 5.0 hosts. • vCenter Chargeback Server 1.6.2. • vCenter Chargeback data collectors. • vShield Manager 5.0. • Microsoft SQL Server 2008 Enterprise (x64) SP3. • vCenter Database. • vCloud Director Database. • VMware vCenter™ Update Manager Database. • vCenter Chargeback Database. • VMware vCloud Director 1.5 cells. • vCenter Orchestrator 5.0.
Section 2.4, Resource Group Design	• vCenter Servers and vCenter Databases. • vCenter clusters and ESXi hosts. • vShield Edges deployed on demand.

The high-level logical architecture is illustrated in Figure 2.

Figure 2. vSphere Logical Architecture Overview

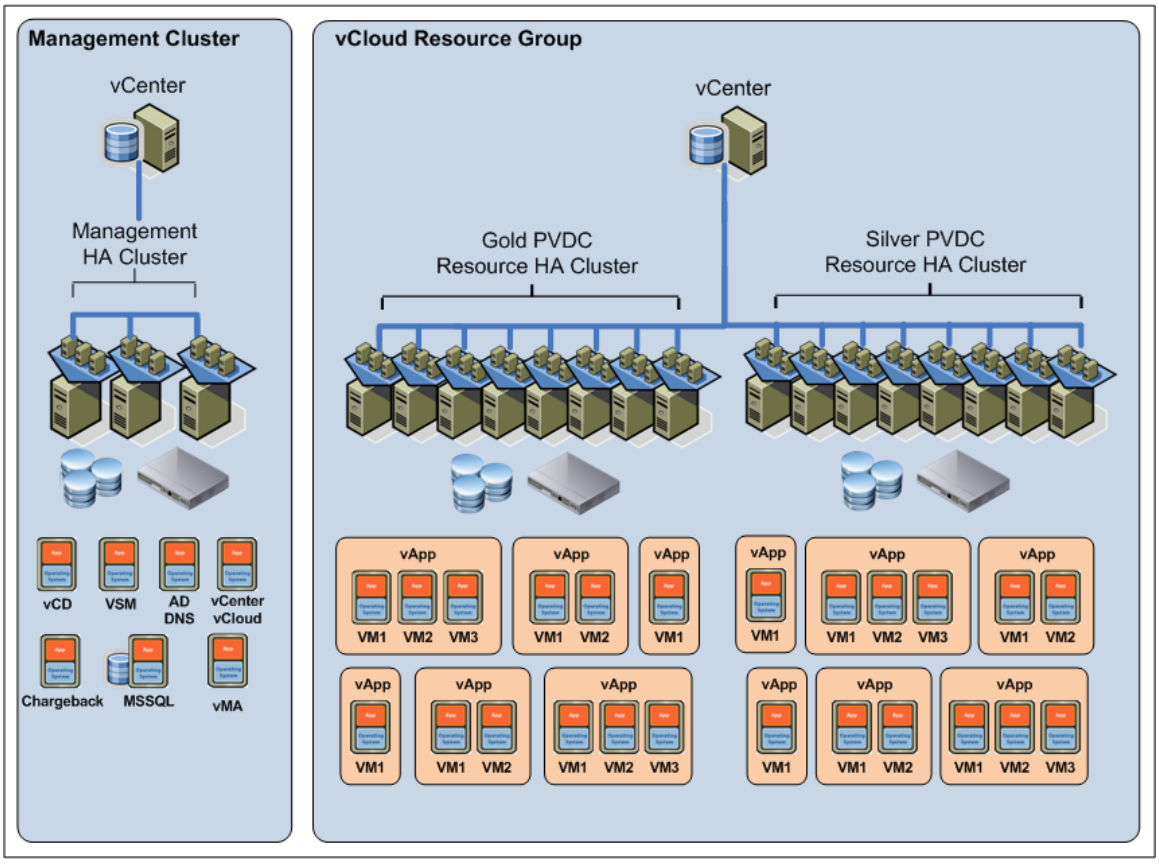
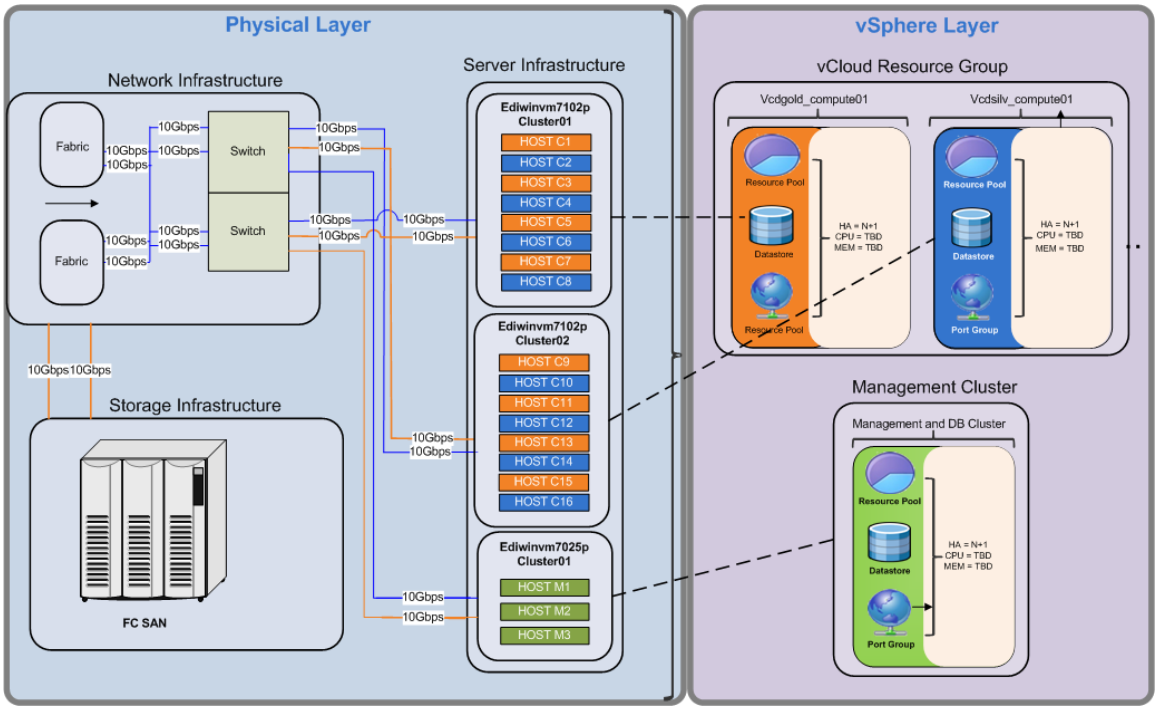


Figure 3 shows the physical design that corresponds to the logical architecture.

Figure 3. vCloud Physical Design Overview



The design calls for the use of blade server technology with three chassis initially dedicated to the vCloud environment. The physical design represents the networking and storage connectivity from the blade chassis to the fabric and SAN as well as the physical networking infrastructure. Connectivity between the blade servers and the chassis switching is different and is not shown here. Two chassis will initially be populated with eight blades each for the vCloud resource clusters, with an even distribution between the two chassis of blades belonging to each resource cluster.

In vSphere 5, VMware High Availability (HA) leverages Fault Domain Manager (FDM) which replaces the Legato AAM-based HA technology. FDM supports all existing HA functionality with no regression in behavior and is transparent to vCloud Director. For the initial release of FDM in vSphere 5, the total number of hosts in a cluster remains at 32. Therefore, cluster sizing guidance for vCloud environments remains the same. Because FDM requires a single master host, as opposed to AAM's five primary nodes, there is no need to add hosts to clusters in a specific order or stripe blade servers across separate chassis. If the master host fails, the remaining slave hosts participate in an election to choose a new master. The decision to alternate blade servers within a specific chassis across the two vSphere resource clusters is based on considerations outside vSphere.

2.2 Site Considerations

The management cluster and the two vCloud resource clusters both reside within a single physical datacenter in Edison, NJ. Although NewCo is considering a Phase II project to expand their vCloud offering to a hybrid model, the scope of this design is a private vCloud within a single physical datacenter. Secondary and/or DR sites are out of scope for this engagement.

Table 4. vCenter Management

Site	vCenter	Datacenter	Purpose
Edison	Ediwinvm7102p	Edivcdc01	Provides compute resource clusters for vCloud management components.
Edison	Ediwinvm7025p	Edidc01	Provides compute resource clusters for non-cloud vSphere workloads and the vCloud management cluster.

2.3 Management Cluster Design

The vSphere management cluster design encompasses the ESXi hosts contained in the management cluster. The scope is limited to only the infrastructure supporting the vCloud management component workloads. The virtual machines that will run in the management cluster are listed in Table 5.

Table 5. Management Virtual Machines

Virtual Machine	Purpose
Edilxvm70225p	vCenter 5.0 dedicated to the non-cloud vSphere environment including the management cluster for vCloud.
Edilxvm7101p	vCloud Director 1.5 cell running vCloud Director Service.
Ediwinvm7102p	vCenter 5.0 dedicated to vCloud Director and managing vCloud resources.
Ediwinvm7103p	Microsoft SQL Server 2008 Ent (x64) SP3 to be used for: • vCloud Director Database (Edilxvm7101p). • vCenter 5 Database (Ediwinvm7102p). • vCenter Update Manager Database. • vCenter 1.6.2 Chargeback Database (Ediwinvm7104p).
Ediwinvm7104p	vCenter Chargeback 1.6.2 (patch 2) server.
Ediwinvm7105p	Microsoft Active Directory, DNS, and DHCP Server.
Ediwinvm7107p	vShield Manager 5.0.
Ediwinvm7111p	vCenter Orchestrator 5.0.
Ediwinvm7112p	vSphere Management Assistant (vMA).

2.3.1 Management Component Resiliency Considerations

The following management components rely on HA, VMware Fault Tolerance (FT), and third-party clustering for redundancy.

Table 6. Management Component Resiliency

Management Component	HA Enabled	VM Monitoring	FT	vCenter Heartbeat	MCS Failover Cluster
vCenter Server	Yes	Yes	No	Yes	No
VMware vCloud Director	Yes	Yes	No	N/A	No
vCenter Chargeback Server	Yes	Yes	No	N/A	No
vShield Manager	Yes	Yes	Yes	N/A	No
Microsoft SQL Server 2008 R2 Standard (x64)	Yes	Yes	No	N/A	Yes
vCenter Orchestrator	Yes	Yes	No	N/A	No
Active Directory	Yes	Yes	No	N/A	No

2.3.2 vSphere Clusters

The management cluster is comprised of the following vSphere HA and VMware Distributed Resource Scheduler (DRS) clusters.

Table 7. vSphere Clusters – Management Cluster

Attribute	Specification
Cluster Name	Edivchadrs01
Number of ESXi Hosts	3
VMware DRS Configuration	Fully automated
VMware DRS Migration Threshold	Moderate (3 of 5)
VMware HA Enable Host Monitoring	Yes
VMware HA Admission Control Policy	Enabled (percentage based)
VMware HA Percentage	• 33% CPU • 33% memory • (N+1 for 3 host cluster)
VMware HA Admission Control Response	Disallow virtual machine power on operations that violate availability constraints
VMware HA Default VM Restart Priority	N/A
VMware HA Host Isolation Response	Leave powered on
VMware HA Enable VM Monitoring	Yes
VMware HA VM Monitoring Sensitivity	Medium

2.3.3 Host Logical Design

Each ESXi host in the management cluster has the following specifications.

Table 8. Host Logical Design Specifications – Management Cluster

Attribute	Specification
Host type and version	VMware ESXi 5 Installable
Processors	2 x Intel Xeon x5630 2.53GHz (4 core)
Storage	• Local for ESXi binaries • SAN LUN for virtual machines
Networking	802.1q Trunk Port Connectivity participating in the following VLANs: • VLAN 100 management network (Console) • VLAN 200 vMotion (non-routable)
Memory	48GB

2.3.4 Network Logical Design

This network design section defines how the vSphere virtual networking is configured for ESXi hosts in the management cluster.

Following best practices, the network architecture must meet the following requirements:

- Separate networks for vSphere management, virtual machine, and VMware vSphere® vMotion® traffic.
- Redundant vSwitch uplinks with at least two active physical NIC adapters each.
- Redundancy across different physical adapters to protect against NIC or PCI slot failure.
- Redundancy at the physical switch level.
- A mandatory standard vSwitch in the management cluster.

Table 9. Virtual Switch Configuration – Management Cluster

Switch Name	Switch Type	Function	Physical NIC Ports
vSwitch0	Standard	• Management Console • vMotion • Management virtual machines	2 x 10 GigE (teamed for failover)

Figure 4 depicts the virtual network infrastructure design for the vSphere management cluster.

Figure 4. vSphere Logical Network Design – Management Cluster

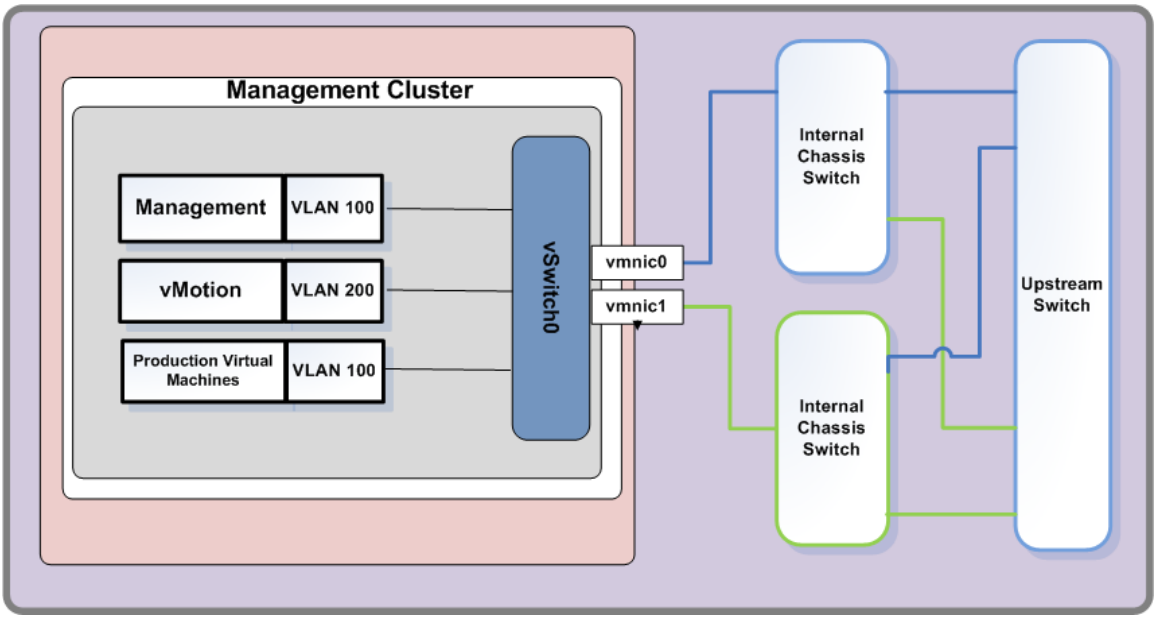


Table 10. Virtual Switch Configuration Settings – Management Cluster

Parameter	Port Group	Setting
Load Balancing	All	Route based on originating port ID
Failover Detection	All	Link status
Notify Switches	All	Enabled
Failback	All	No
Failover Order	• Management • vMotion • Management virtual machines	• vmnic0 = Active • vmnic1 = Active

2.3.5 Shared Storage Logical Design

This section defines how the vSphere datastores are configured in the vSphere management cluster. Different LUNs from the same storage system are used for the management cluster and the vCloud resource clusters.

Following best practices, the shared storage architecture must meet the following requirements:

- Storage paths are redundant at the host (connector), switch, and storage array levels.
- All hosts in the vCloud management cluster have access to the same datastores.

Table 11. Shared Storage Logical Design Specifications – Management Cluster

Attribute	Specification
Number of Initial LUNs	• 2 dedicated • 2 VMFS for virtual machine disk file storage
LUN Size (VMFS)	750GB
Zoning	Single-initiator, single-target
VMFS Datastores per LUN	1
VMs per LUN	<10 (distribute redundant virtual machines)

2.3.6 vCloud Director Transfer Storage

To provide temporary storage for uploads and downloads, a 300GB NFS network share is presented to the vCloud Director cell. Although the current design calls for a single vCloud Director cell, the design calls for an NFS volume for this purpose to provide an easy migration path to a load balanced multicell configuration. The transfer server NFS volume must have write permissions for root. Each host must mount this storage at `$VCLOUD_HOME/data/transfer` (by default this is `/opt/vmware/cloud-director/data/transfer`).

2.4 Resource Group Design

The resource group design represents the two vSphere HA DRS clusters and infrastructure used to run the vApps that are provisioned and managed by vCloud Director. In this section the scope is limited to only the infrastructure dedicated to the vCloud workloads.

The vCloud resource group is made up of the following vSphere clusters.

Table 12. Resource Group Clusters

Cluster Name	vCenter Server Name	# of Hosts	HA Percentage
VCDGold_Compute01	vcd_vc01.example.com	8	13%
VCDSilv_Compute01	vcd_vc01.example.com	8	13%

2.4.1 vSphere Clusters

Both vCloud resource clusters are configured similarly with the following specifications.

Table 13. vSphere Cluster Configuration

Attribute	Specification
Resource Cluster Names	vcdgold_compute01 vcdsilv_compute01
Number of ESXi Hosts	8
VMware DRS Configuration	Fully automated
VMware DRS Migration Threshold	Moderate (3 of 5)
VMware HA Enable Host Monitoring	Yes
VMware HA Admission Control Policy	Enabled (percentage based)
VMware HA Percentage	• 13% CPU • 13% memory • (N+1 for 8 host cluster)
VMware HA Admission Control Response	Disallow virtual machine power on operations that violate availability constraints.
VMware HA Default VM Restart Priority	N/A
VMware HA Host Isolation Response	Leave Powered On
VMware HA Enable VM Monitoring	Yes
VMware HA VM Monitoring Sensitivity	Medium

2.4.2 Host Logical Design

Each ESXi host in both vCloud resource clusters has the following specifications.

Table 14. Host Logical Design Specifications

Attribute	Specification
Host type and version	VMware ESXi 5 Installable
Processors	2 x Intel Xeon x5650 2.66 GHz (6 core)
Storage	Local for ESXi binaries
Networking	802.1q trunk port connectivity participating in the following VLANs: • VLAN 100 management network (Console) • VLAN 200 vMotion (non-routable) • VLAN 140 production virtual machines • VLAN 136 development virtual machines • VLAN 1254 VCD-NI transport network
Memory	96GB

2.4.3 Network Logical Design

The network design section defines how the vSphere virtual networking is configured for the vCloud resource group clusters.

Following best practices, the network architecture must meet the following requirements:

- Separate networks for vSphere management, virtual machine, and vMotion traffic.
- Maintain isolation of the production network from other VLANs across physical and virtual networking infrastructure.
- vdSwitch with a minimum of two active physical adapter ports.
- Redundancy across physical adapters to protect against NIC or PCI slot failure.
- Redundancy at the physical switch level.
- Maintain isolation across physical, virtual, and vCloud networks.

Table 15. Virtual Switch Configuration

Switch Name	Switch Type	Function	NIC Ports
vdSwitch01	Distributed	• External networks • Network pools	2 x 10 GigE NIC

When using the distributed virtual switch, dvUplink ports are the number of physical NIC ports on each host. The physical NIC ports are connected to redundant physical switches.

Figure 5 depicts the virtual network infrastructure design.

Figure 5. vSphere Logical Network Design

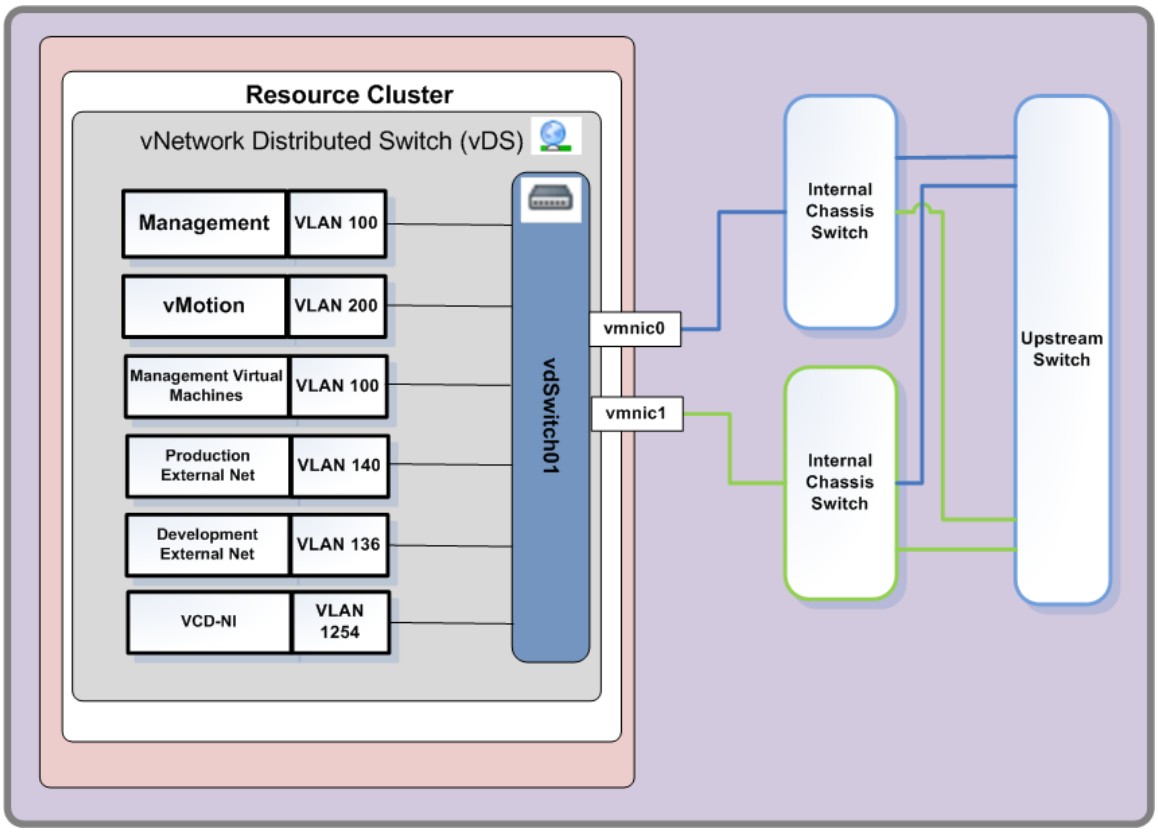


Table 16. vdSwitch01 Teaming and Failover Policies

Parameter	Port Group	Setting
Load Balancing	All	Route based on physical NIC load
Failover Detection	All	Link status only
Notify Switches	All	Enabled
Failback	All	No
Failover Order	Management vMotion Production external net Development external net VCD-NI Transport net	vmnic0 = Active vmnic1 = Active

Table 6. vdSwitch01 Security Policies

Parameter	Port Group	Setting
Promiscuous Mode	All	Reject
MAC Address Change	All	Reject
Forged Transmits	All	Reject

Table 6. vdSwitch01 General Policies

Parameter	Port Group	Setting
Port binding	Production external net	Ephemeral – no binding
Port binding	Development external net	Ephemeral – no binding

Port Groups created by vCloud Director for the Routed and Isolated Organization networks are not included in these tables. vCloud Director creates these Port Groups automatically on vdSwitch01 based on demand and configures the appropriate settings automatically. The settings for these Port groups should not be changed manually in the VMware vSphere® Client™.

2.4.4 Shared Storage Logical Design

This shared storage design section defines how the vSphere datastores are configured in the vSphere resource clusters, which provide storage capacity for vCloud provider virtual datacenters.

Following best practices, the shared storage architecture must meet the following requirements:

- Storage paths are redundant at the host (HBA), switch, and storage array levels.
- All hosts in a cluster have access to the same datastores.

Table 17. Storage Logical Design Specifications – Cloud Compute Cluster 1

Attribute	Specification
Cluster	VCDgold_Compute01
Number of Initial LUNs	10 dedicated **Note** Within the first year, based on expected utilization, NewCo will need to increase the number of LUNs.
LUN Size	900GB
Zoning	Single-initiator, single-target
VMFS Datastores per LUN	1
VMs per LUN	12 – 15 (simultaneous active virtual machines)

Table 18. Storage Logical Design Specifications – Cloud Compute Cluster 2

Attribute	Specification
Cluster	VCDsilv_Compute01
Number of Initial LUNs	8 dedicated
LUN Size	1.5TB
Zoning	Single-initiator, single-target
VMFS Datastores per LUN	1
VMs per LUN	17-20 (simultaneous active virtual machines)

2.4.5 Shared Storage Physical Design

This section outlines the physical design specifications for the shared storage system that provides block level storage to the vCloud resource clusters.

Table 19. Compute Cluster Shared Storage Physical Design

Attribute	Specification
Vendor and model	Midrange FC SAN
Type	Active/Active
Multipathing Plug-in (MPP)	SAN Vendor Plug-in
Path Selection Plug-in (PSP)	Round robin (rr)
Max speed rating of switch ports	4GB

2.4.6 vCloud Resource Datastore Considerations

The most common aspect of LUN and datastore sizing is the limit to implement for the number of virtual machines per datastore. The reason for limiting this number is to minimize the potential for SCSI locking due to metadata updates, and to spread the I/O across as many storage processors and LUN queues as possible. The impact of SCSI locking is dramatically reduced in the NewCo design through the use of VMware Storage APIs-Array Integration (VAAI) and the ATS primitive. All virtual machines on the same datastore share a common storage queue, which can present a bottleneck as the number of virtual machines per datastore increases. Most mainstream storage vendors provide VMware-specific guidelines for this limit. In the past, VMware has recommended an upper limit of 15 virtual machines (active) per VMFS datastore regardless of storage platform. In a vSphere 5 environment using VAAI and ATS this limit is generally much higher, but 15 is a good starting point. The number of virtual machines per LUN is also influenced by the size and I/O profile of the virtual machine as well as the selected storage solution and disk types.

When VMware vCloud Director provisions virtual machines it automatically places the virtual machines on datastores based on the free disk space of each of the associated datastores in an organization virtual datacenter. The exception to this is when *fast provisioning* is used—in this case, datastores with the original or a Shadow virtual machine is preferred over those that do not. Due to this placement mechanism, the datastore sizing is based on an estimate of how many average size virtual machines can fit in a datastore, taking into account sufficient overhead for VMkernel swap, snapshots, and overhead.

When considering the number of virtual machines to place on a single datastore, consider some of the following factors in conjunction with any recommended VMs-per-LUN ratio:

- Average virtual machine workload/profile (in particular, the amount of I/O).
- Typical VMDK size (including configuration files, logs, swap files, and snapshot files).
- VMFS metadata updates.
- Maximum requirement for IOPs and throughput per LUN (dependent on storage array and design).
- Maximum RTO, if a LUN is lost (backup and restore design).

If we approach this from an average I/O profile it would be tempting to create all LUNs the same—for example, as RAID 5, and let the law of averages take care of I/O distribution across all the LUNs and virtual machines on those LUNs. Another approach is to create LUNs with different RAID profiles based on anticipated workloads to provide differentiated levels of service. These levels of service are represented at the vSphere level by an HA/DRS cluster and its associated mapped storage and network objects. The vCloud logical design maps provider virtual datacenters to these clusters. To achieve the two levels of service, NewCo will start with two underlying vSphere vCloud compute clusters with separate storage LUNs from the same array mapped to each cluster.

Table 20. vSphere Clusters – Cloud Compute Datastores

Cluster Name	Datastores	Qty	RAID	Size
VCDgold_Compute01	Cx02fc-vcdgold01-xx	10	5	900GB
VCDsilv_Compute01	Cx02fc-vcdsilv01-xx	8	5	1.5TB

Where xx = the LUN ID for that device.

Based on a preliminary analysis of I/O profiles in the existing vSphere environment, VMware recommends RAID 5 storage profiles for the LUNs to be used for VMFS datastores. If storage performance becomes an issue, NewCo must create an additional storage tier-specific provider virtual datacenter to address specific organization or business unit requirements. Another option is to create datastores of a size that will result in few virtual machines per datastore.

For the initial design, the vcdgold-Compute01 cluster will have smaller datastores with fewer virtual machines per datastore. This should result in a reduced level of storage contention as well as faster recovery of the virtual machines on that LUN, or lower RTO. The vcdsilver-compute01 cluster will have larger datastores with more virtual machines, which could increase storage contention and the RTO, but is more appropriate for this reduced level of service and associated cost.

For additional information regarding vSphere storage design, see *VMware Scalable Storage Performance* (http://www.vmware.com/files/pdf/scalable_storage_performance.pdf).

2.4.7 Datastore Sizing Estimation

An estimate of the typical datastore size can be approximated by considering the following factors.

Table 21. Datastore Size Estimation Factors – vcdgold-Compute01 Cluster

Variable	Value
Maximum Number of virtual machines per datastore	12–15
Average size of virtual disks per virtual machine	60GB
Average memory size per virtual machine	2GB
Safety margin	20% (to avoid warning alerts)

For example:

`((12 * 60GB) + (15 * 2GB))+ 20% = (720GB + 30GB) * 1.2 =` **`900GB`**

Table 22. Datastore Size Estimation Factors – vcdsilv-Compute01 Cluster

Variable	Value
Maximum Number of virtual machines per datastore	17-20
Average size of virtual disks per virtual machine	60GB
Average memory size per virtual machine	2GB
Safety margin	20% (to avoid warning alerts)

For example:

`((17 * 60GB) + (17 * 2GB))+ 20%=(1,054GB + 210GB)*1.2 =`**`1,516GB`**

2.4.8 Storage I/O Control

Storage I/O Control (SIOC) provides Quality of Service (QoS) for VMFS datastores and allows intelligent and dynamic performance management across all nodes within an HA/DRS cluster. Enabling SIOC on all datastores in a cluster prevents virtual machines from monopolizing storage I/O and provides a share based weighting mechanism that provides adequate performance based on an Administrator-configured share allocation. SIOC enables this functionality by dynamically allocating portions of individual ESXi host's I/O queues to virtual machines running on the vSphere hosts based on shares assigned to the virtual machines. NewCo vSphere administrators can mitigate the performance loss of critical workloads during peak load periods by setting higher I/O priority (by means of disk shares) to those virtual machines running them. Establishing these I/O priorities for specific virtual machines results in better performance during periods of congestion for these workloads as well as more predictable storage performance overall.

SIOC does not support raw device mappings (RDM) or datastores with multiple extents. SIOC is enabled in the NewCo vCloud environment for both vCloud computer clusters, all with a congestion threshold of 25 milliseconds. To direct SIOC to produce the intended results the design calls for each provider virtual datacenter to be backed by one or more vSphere HA/DRS clusters (not resource pools), which is a vCloud Director best practice. This has the effect of limiting the SIOC host I/O queue adjustments to the boundaries of a single provider virtual datacenter.

The NewCo design provides the ability for administrators to assign shares to specific virtual machines where a prioritized level of storage queue access is desired. These virtual machines are to be determined, but the two high level groupings are outlined in Table 23.

Table 23. SIOC Disk Shares

Cluster Name	Congestion	Default Shares	High VM Shares
VCDgold_Compute01	30ms	Normal(1000)	High(2000)
VCDsilv_Compute01	30ms	Normal(1000)	High(2000)

2.4.9 Storage vMotion

Storage vMotion in ESXi 5.0 has been improved to support migration of linked clones which is the technology used to implement *fast provisioning* in vCloud Director. In a vCloud Director environment, the migration of linked clones can only be invoked in the vCloud Director layer, through the REST API `Relocate_VM` method. In vCloud Director 1.5, the API call is the only method to migrate vApps provisioned through fast provisioning. It is not supported to invoke Storage vMotion migration of linked clone virtual machines in the vSphere layer. When invoking the `Relocate_VM` API to migrate linked clones, be sure that the target organization virtual datacenter is part of the same provider virtual datacenter as the source organization virtual datacenter, or is backed by a provider virtual datacenter that has the same datastore where the source vApp resides. If the condition is not met, the API call will fail.

Be aware of the following when leveraging Storage vMotion in a vCloud environment:

- Source and destination datastores for Storage vMotion should both reside within the same provider virtual datacenter or vSphere cluster.
- For provider virtual datacenters that leverage fast provisioning, linked clones become full clones when virtual machines are migrated using Storage vMotion.

2.4.10 Storage DRS

Storage DRS leverages Storage vMotion to automatically migrate virtual machines between datastores if performance thresholds are exceeded. The NewCo design does not use Storage DRS because it is not supported by vCloud Director 1.5. Although you can enable Storage DRS on datastores that support a vCloud Director provider virtual datacenter, vCloud Director provisioned linked clones will be ignored by Storage DRS.

2.4.11 Storage APIs – Array Integration

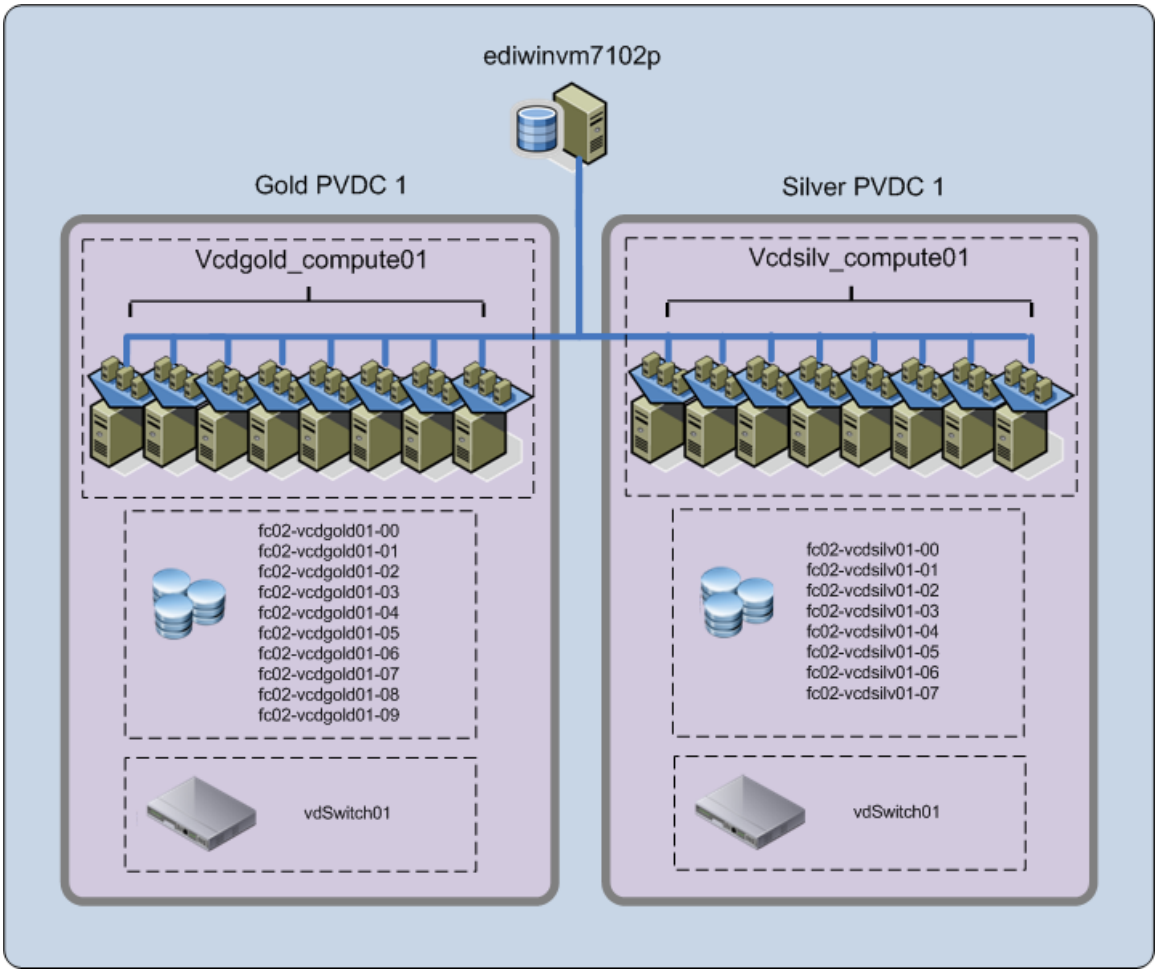
The storage vendor at NewCo offers a plug-in for Storage APIs-Array Integration (VAAI) on the FC SAN servicing the vCloud Director environment. This functionality can provide large performance boosts for vCloud environments, especially with vApp deployments. Storage APIs-Array Integration enables storage-based hardware acceleration. This functionality allows vSphere to pass storage primitives to supported arrays, offloading functions such as full copy, block zeroing, and locking. Storage API-Array Integration improves storage task execution times, network traffic utilization, and CPU host utilization during heavy storage operations. The vSphere environment at NewCo leverages the SAN vendor's API plug-in to enhance storage performance.

3. vCloud Design – Provider Constructs

3.1 Provider Virtual Datacenters

A vCloud provider virtual datacenter represents a predefined set of pooled infrastructure including compute, network, and storage that corresponds to a level of service to be consumed. The following diagram shows how the provider virtual datacenters map back to vSphere resources. Each provider virtual datacenter maps to only one vSphere cluster, but will map to multiple datastores and networks.

Figure 6. Provider Virtual Datacenters and vSphere Resources



Multiple provider virtual datacenters are used to map to different types and tiers of resources.

- Compute – This is a function of the mapped vSphere clusters and the resources that back it.
- Storage – This is a function of the underlying storage types of the mapped datastores.
- Networking – This is a function of the mapped vSphere networking in terms of speed and connectivity.

Multiple provider virtual datacenters are created for the following reasons:

- To provide a tiered level of service such as faster processors, use a different allocation model, or higher redundancy such as N+2 instead of N+1.
- To provide a tiered storage model. Each provider virtual datacenter maps to datastores on storage with different characteristics.
- To expand the compute capacity available to a specific level of service or organization virtual datacenter by adding multiple clusters to a provider virtual datacenter. This feature only works with the Pay-as-You-Go allocation model.

Table 24. NewCo Provider Virtual Datacenters

Provider Virtual Datacenter	Latest Hardware Version	CPU Capacity	Memory Capacity	Storage Capacity
Gold	Version 8	223GHz	672GB	9TB
Silver	Version 8	223GHz	672GB	12TB

ESXi 5.0 introduces a new generation of virtual hardware with virtual machine hardware version 8. All ESXi nodes within the vSphere clusters that are mapped to the provider virtual datacenters above will be running ESXi 5.0, allowing these new features to be leveraged by the virtual machines used to build vApps including:

- 32-way virtual SMP
- 1TB of virtual machine RAM
- Software support for 3D graphics to run Windows Aero
- USB 3.0 device support
- UEFI virtual BIOS

Table 25. Provider Virtual Datacenter to vSphere Mapping

Provider Virtual Datacenter	Resource Pool	Datastores	vSphere Networks
Gold	VCDgold_Compute01	Fc02-vcdgold01-00	Production external
		Fc02-vcdgold01-01	Development external
		Fc02-vcdgold01-02	
		Fc02-vcdgold01-03	
		Fc02-vcdgold01-04	
		Fc02-vcdgold01-05	
		Fc02-vcdgold01-06	
		Fc02-vcdgold01-07	
		Fc02-vcdgold01-08	
		Fc02-vcdgold01-09	
Silver	VCDsilv_Compute01	Fc02-vcdsilv01-00	Production external
		Fc02-vcdsilv01-01	Development external
		Fc02-vcdsilv01-02	
		Fc02-vcdsilv01-03	
		Fc02-vcdsilv01-04	
		Fc02-vcdsilv01-05	
		Fc02-vcdsilv01-06	
		Fc02-vcdsilv01-07	

3.1.1 Provider Virtual Datacenter Sizing

Each NewCo provider virtual datacenter corresponds to one and only one vSphere HA/DRS cluster. While a vSphere 5 cluster can scale to 32 hosts, typically 8–12 is a good starting point that allows for future growth. The recommendation is to start with eight hosts in a cluster and add hosts to the cluster as dictated by customer consumption and utilization metrics such as when utilization reaches ~60%. In a provider virtual datacenter that leverages the fast provisioning feature and iSCSI or Fibre Channel based storage, the vSphere cluster size backing a provider virtual datacenter is limited to eight nodes. Through the concept of pooled and abstracted infrastructure, capacity can be added to the vCloud through this method allowing for expansion of provider virtual datacenters and the corresponding clusters without impacting running vApps. If expanding an existing cluster is not an option, VMware recommends that a new provider virtual datacenter and corresponding cluster be deployed.

The design calls for two clusters initially sized at eight hosts each. A single vCenter 5 system is limited to 1,000 ESXi hosts and 10,000 powered on virtual machines if spread across more than one VMware datacenter. In this configuration, each vCenter hierarchy acts as a large resource pool that can scale up through the addition of hosts to existing vSphere clusters, or by adding additional vSphere clusters and associated provider virtual datacenters. Multiple clusters can be managed by the same VMware vCloud Director and usually represent different levels of service.

Based on analysis of the existing vSphere environment NewCo averages a 5:1 vCPU to Physical CPU Core ratio for their virtual machines. The size of the existing vSphere clusters and hosts provides approximately 168 usable cores across both vSphere clusters or provider virtual datacenters based on the host hardware configuration and N+1 HA availability. Based on the estimated vCPU to pCPU ratio of 5:1 this should provide the ability to run 840 virtual machines of similar size and performance characteristics in the vCloud. To increase this number of virtual machines on the existing infrastructure, NewCo must increase the vCPU to pCPU ratio that they are willing to support. The risk associated with an increase in CPU overcommitment is that mainly degraded overall performance that can result in higher than acceptable vCPU ready times. The vCPU to pCPU ratio is based on the amount of CPU over-commitment for the available cores with which NewCo is comfortable. For virtual machines that are not busy, this ratio can be increased without any undesirable effect on virtual machine performance. Monitoring of vCPU ready times helps identify if the ratio needs to be increased or decreased on a per cluster basis. A 5:1 overall ratio is a good starting point for a multicore system. It is anticipated that this ratio may be a little lower (4:1) in the VCDgold_Compute01 cluster and slightly higher (6:1) in the VCDsilv_Compute01.

It is recommended to keep datastore “types” uniform for a given provider virtual datacenter (port speed, RAID, storage protocol, others). Mixing storage from different tiers (for example, FC and SATA in same provider virtual datacenter) creates confusion when deploying new virtual machines and vApps. There is a high possibility of a template being provisioned on FAST (higher tier) and a working copy of the template on a SATA (lower tier) datastore.

3.1.2 Provider Virtual Datacenter Expansion

In vCloud Director 1.5, the concept of *elastic virtual datacenters* was introduced, allowing a provider virtual datacenter to recognize compute, network, and storage resources from multiple resource pools or vSphere clusters. In vCloud Director 1.5, only Pay-As-You-Go organization virtual datacenters can be backed by multiple resource pools or vSphere clusters. Organization virtual datacenters that use the Reservation Pool or Allocation Pool model cannot be backed by elastic virtual datacenters. For provider virtual datacenters mapped to a reservation-backed or allocation-backed organization virtual datacenters (Gold provider virtual datacenter 1), capacity can only be added by incrementally adding capacity to an existing vSphere cluster such as additional hosts or networks. In contrast, the “Silver PVDC 1” virtual datacenter can be expanded by building entire additional vSphere clusters and incorporating these resources into the provider virtual datacenter, which immediately makes these resources available to the mapped Pay-As-You-Go organization virtual datacenters for both EIT and AES organizations. For consistency, all datastores that are mapped to the underlying vSphere clusters beneath an elastic provider virtual datacenter should be added to the provider virtual datacenter.

3.1.3 Provider Virtual Datacenter Storage

When creating the provider virtual datacenter, the vCloud administrator adds all of the shared storage LUNs available to the HA/DRS cluster to which the provider virtual datacenter is mapped. Storage LUNs are typically mapped only to the hosts within an HA/DRS cluster to facilitate vMotion and DRS. vCloud Director 1.5 does not understand datastore clusters introduced in vSphere 5, so datastores should be added individually to provider virtual datacenters.

For the Gold provider virtual datacenter, this means adding the 10 shared storage LUNs from the SAN with the naming standard Fc02-vcdgold01-xx, where xx is the LUN ID. For the Silver provider virtual datacenter, this means adding the eight shared storage LUNs from the SAN with naming convention Fc02-vcdsilv01-xx, where xx is the LUN ID. It is recommended to keep all of the LUNs within a provider virtual datacenter with the same performance and RAID characteristics to provide a consistent level of service to consumers. Only shared storage should be used to allow for vMotion and DRS to function.

3.2 External Networks

A vCloud external network is a logical construct that maps directly to a vSphere port group that has multiple vmnic uplinks to a physical network. This construct represents an external connection for communication in and out of the vCloud. Organization networks can be configured to leverage external networks for connectivity to a corporate LAN or a dedicated WAN connection. NewCo provides the following vCloud external networks for the initial implementation.

Table 26. vCloud External Networks

VCD External Net	vSphere Net	VLAN	Subnet	Allocated IP Addresses
NewCo-Prod-Ext	Production_140	140	192.168.20.0/24	192.168.20.50 – 192.168.20.80
NewCo-Dev-Ext	Development_136	136	192.168.101.0/24	192.168.101.50 – 192.168.101.80

vApps in both organizations within the NewCo vCloud may need access to one or the other external network as vApps in each may be used for production or development. To leverage both of these external networks there are two organization networks in each organization, each with a connection to its respective external network. Each external network is assigned a range of 30 IP addresses from the appropriate subnet for automatic assignment to vShield Edge devices or vApps on direct connected organization networks.

3.3 Network Pools

Network pools are a construct in vCloud Director and represent a preconfigured, vCloud-controlled pool of Layer 2 isolated networks that are automatically used to provide isolation between different organizations or even between vApps within an organization. Aside from the Layer 2 isolation function, they also enable self-service by allowing the complicated underlying networking configuration to be abstracted from the application owner at time of instantiation.

The NewCo design provides a single VMware vCloud Director-Network Isolation-backed pool to be used for organization isolation and vApp fencing. For the VCD-NI-backed pool, VMware recommends isolating the transport network that is used for communication between virtual machines on the same isolated Layer 2 network that reside on different ESXi hosts. This separation can be accomplished by separating external and organization networks using two separate vdSwitches or by designating a dedicated transport VLAN to be used for this purpose. VMware recommends the transport VLAN be a VLAN that is not in use within the NewCo infrastructure for increased security and isolation. For the initial implementation, a dedicated transport VLAN on the same vdSwitch was used (VLAN 1254) and trunked in to each of the ESXi uplink ports as an additional participating VLAN.

VCD-NI leverages MAC-in-MAC encapsulation to provide isolation within an ESXi host and across the physical network. This encapsulation adds 24 bytes to the Ethernet frame headers used to communicate across the physical network between ESXi hosts in the same provider virtual datacenter. To avoid any potential performance issues associated with fragmented Ethernet frames, VMware recommends increasing the MTU size for this network to at least 1524 bytes. For this increase to be effective it was made in the following locations:

- Network pool properties
- vDSwitch properties
- Physical switch ports used for vdSwitch01 uplinks

3.4 Users and Roles

For security purposes, the vCloud administrators are a separate role and log into a different context than the vCloud consumers who exist within an organization. As a provider construct, the vCloud administrator role has the ability to modify all organizations within the vCloud as well as create and configure objects that vCloud consumers cannot.

For security purposes, the role of system administrator should be reserved for a limited group of vCloud administrators. Because this role has the ability to create and destroy objects as well as make configuration changes that can negatively impact multiple organizations, users who possess this role should be knowledgeable about storage, networking, virtualization, and vCloud.

The design calls for a single local account (vcloudadmin) to be used as a backup for accessing VCD, and the primary access method is managed by adding members to the Active Directory vcloudadmins group in the NewCo ds domain. Three people are initially included in this group.

Table 27. Provider Users and Roles

Account	User/Group	Type	Role
vcloudadmin	User	Local	System Administrator
NewCods\vcloudadmins	Group	LDAP	System Administrator

4. vCloud Design – Consumer Constructs

4.1 Organizations

The initial design calls for the inclusion of two separate security and policy boundaries that map to two distinct departments within NewCo. EIT provides the Information Systems department with both production and test/dev workloads for testing new solutions and software components. AES is used by the developers in Application Engineering to rapidly provision and then decommission workloads based on the existing policies and development lifecycles within the department. Each organization will have a unique and self-descriptive URL (no spaces) for ease of access. Although these organizations will initially correlate to separate business units at NewCo, in the future NewCo will also leverage dedicated organizations to represent a discrete project for a limited period of time.

Table 28. NewCo vCloud Organizations

Organization	Description
EIT	Enterprise Information Technology
AES	Application Engineering Solutions

4.2 Organization Virtual Datacenters

An organization virtual datacenter is a subset of provider virtual datacenter that is backed by a pool of compute, memory, storage, and network resources. An organization virtual datacenter can be expanded by a vCloud system administrator to provide additional capacity (compute, network, and storage) up to the existing capacity of the underlying provider virtual datacenter. At NewCo, this expansion would need to be requested by an organization and the corresponding chargeback costs would increase automatically through the regular synchronization by the Chargeback vCloud data collector.

There will be two levels of service available to both organizations. The method of creating this level of service is done through the use of organization virtual datacenters. The following diagram shows the organization virtual datacenter design at NewCo.

Figure 7. Organization Virtual Datacenter

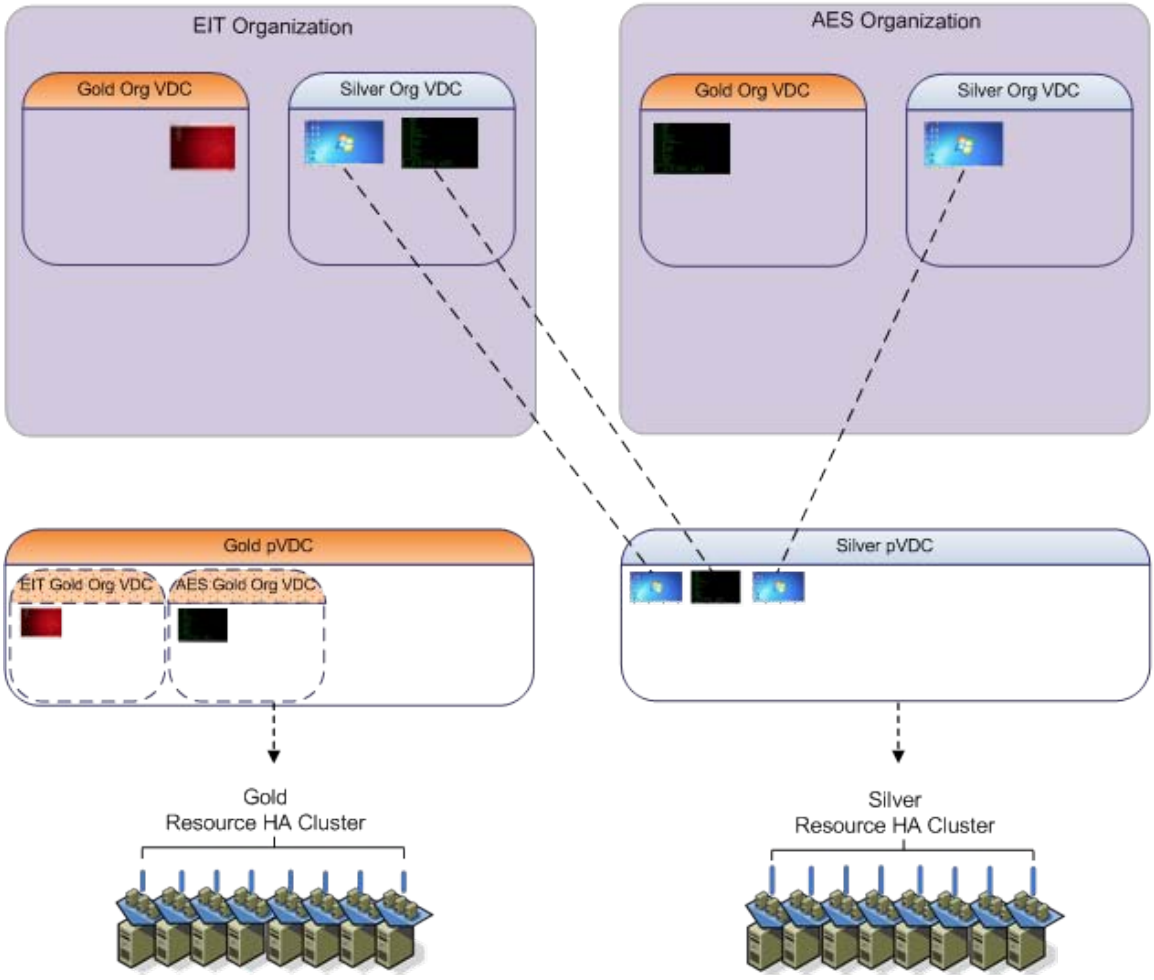


Table 29. Organization Virtual Datacenter Configuration

Organization Virtual Datacenter	Allocation Model	CPU/RAM Guarantee	CPU/RAM Allocation	vCPU GHz	Max VM	SAN Limit
EIT Gold	Reservation	N/A	80GHz/200GB	N/A	100	4,000GB
EIT Silver	PAYG	0%/75%	N/A	.26	N/A	None
AES Gold	Reservation	N/A	40GHz/100GB	N/A	60	4,000GB
AES Silver	PAYG	0%/75%	N/A	.26	N/A	None

4.2.1 Fast Provisioning

Fast provisioning is a feature in vCloud Director 1.5 that enables faster provisioning of vApps through the use of vSphere linked clones. A linked clone uses the same base disk as the original, with a chain of delta disks to keep track of the differences between the original and the clone.

Fast provisioning is enabled by default when allocating storage to an organization virtual datacenter. If an organization administrator disables fast provisioning, all provisioning operations result in full clones.

Fast provisioning is enabled on both Gold and Silver organization virtual datacenters within both the AES and EIT organizations. It is recommended to either enable or disable fast provisioning on all organization virtual datacenters (and in turn all datastores) allocated to a provider virtual datacenter for both manageability and chargeback purposes. For the same reasons, it is recommended to keep datastores separate for fast provisioning and full clone vApp workloads. All organization virtual datacenters created from the same dedicated provider virtual datacenter should have **Enable Fast Provisioning** selected.

The use of fast provisioning and Fiber Channel storage limits the vSphere cluster size that is mapped to the Gold and Silver provider virtual datacenter to eight nodes, but because the Silver organization virtual datacenters use the Pay-As-You-Go allocation model, compute capacity can be added by building additional eight-node vSphere clusters to back the Silver provider virtual datacenter.

Placement of virtual machine disk files in a vCloud environment is based on available free capacity across datastores that are mapped to a provider virtual datacenter. In the case of organizational virtual datacenters that are leveraging fast provisioning, placement will first consider the location of the base or shadow virtual machines until the datastore reaches a preset “Disk space threshold” which is set for each datastore, and enforces the amount of free space in a datastore. After this threshold is reached the datastore is no longer be considered as a valid target for a clone operation regardless of where the new virtual machines base or shadow disk is located.

4.2.2 Thin Provisioning

VMFS thin provisioning can be configured within vCloud Director at the organization virtual datacenter level. VMFS thin provisioning will not be enabled for any of the four organization virtual datacenters. The NewCo design uses array level thin provisioning in the SAN controllers dedicated to vCloud which is enabled for the storage pools and all LUNs mapped to the vCloud resource clusters. Allocation of virtual machines to individual datastores within a provider virtual datacenter is based on available capacity. Using the array level thin provisioning provides a more predictable population of virtual machines within the datastores assigned to a particular provider virtual datacenter.

4.3 Organization Networks

As the name implies, an organization network exists only within a specific organization. There are three types of organization networks: isolated, external direct connect, and external routed. The NewCo design calls for the use of external routed organization networks with connectivity to a corresponding external NewCo network (production or development) through a vShield Edge security appliance. Each organization has one or more external NAT-routed networks available to provide both connectivity to other vApps within the organization and external network access through the network gateway, which is a vShield Edge security appliance. Future use cases may require the need for an isolated organization network for sandbox purposes, but this is not a current requirement.

The following networks were used for the design:

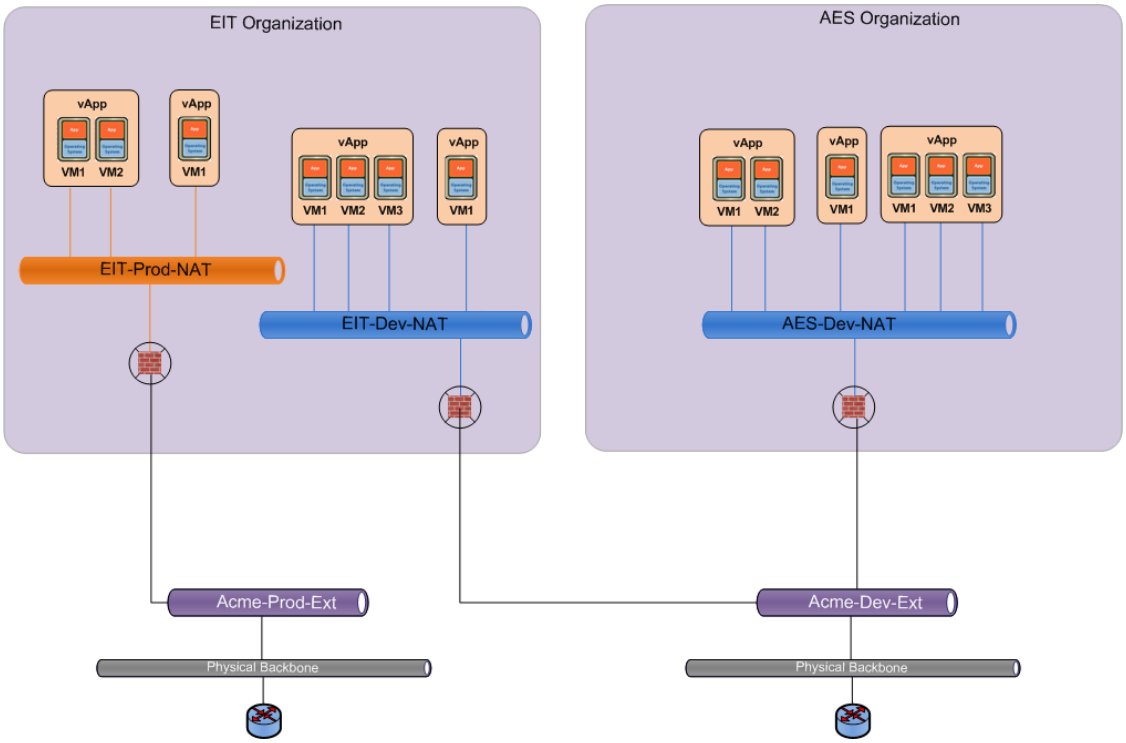
Table 30. EIT Organization Networks

Name	Type	Connection	Net Pool	Subnet
EIT-Prod-NAT	NAT/routed	NewCo-Prod-Ext	VCDNI_1	192.168.20.0/24
EIT-Dev-NAT	NAT/routed	NewCo-Dev-Ext	VCDNI_1	192.168.101.0/24

Table 31. AES Organization Networks

Name	Type	Connection	Net Pool	Subnet
AES-Dev-NAT	NAT/routed	NewCo-Dev-Ext	VCDNI_1	192.168.109.0/24

Figure 8. Organization Network Design



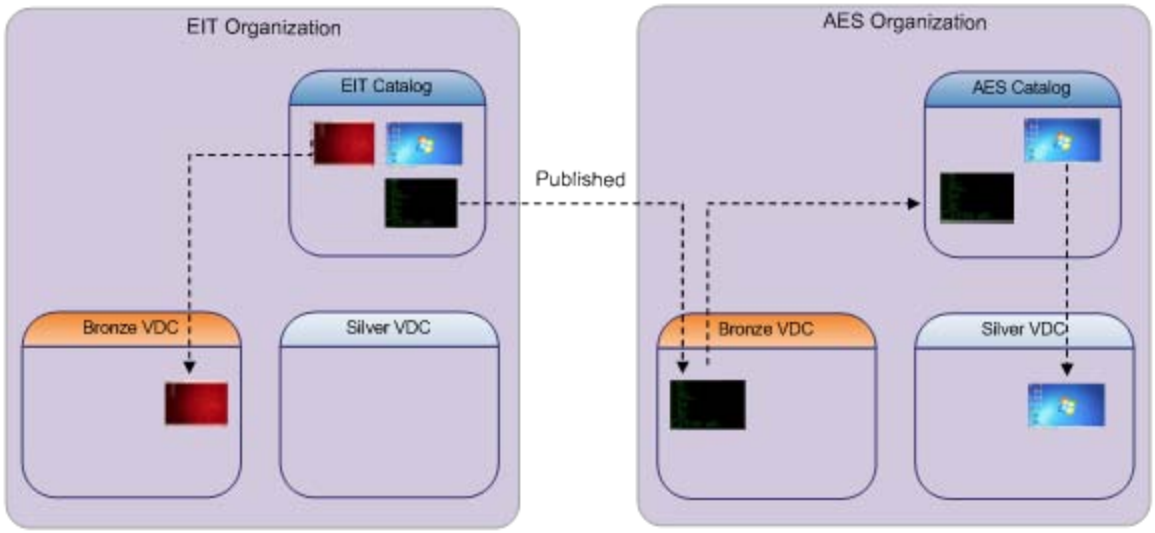
This architecture provides connectivity to the existing external networks and preserves VLANs by sharing the same VLAN for the Internet among multiple organizations. The vShield Edge is needed to provide NAT and firewall services for the two organizations.

After the external networks have been created, a VMware vCloud Director Administrator can create the organization networks. Where appropriate for network isolation or network services, the vShield Edge (VSE) device is needed and deployed automatically to perform address translation between the different networks. The VSE can be configured to provide for port address translation to jump hosts located inside the networks or to gain direct access to individual hosts.

4.4 Catalogs

The catalog construct is an organization-specific object where vApp templates that represent complex multitier applications or services for deployment within an organization can be stored. The NewCo design calls for one catalog for each organization. The AES catalog is shared to all users within the AES organization while the EIT catalog is both shared to all users within EIT organization as well as published to all organizations. In this way, the EIT catalog acts as the master catalog for all organizations. The EIT catalog is published across all organizations and is intended to provide some of the operating system building blocks that can be deployed, customized, and then recaptured as an additional catalog item. This is to provide a global library of standardized vApp templates for all organization users to deploy. This promotes reusability of common assets built to corporate standards in the case of private enterprise vCloud, and provides standardized chargeable/free templates to be consumed by tenants in the case of a public vCloud.

Figure 9. Catalog Architecture



The following operational process illustrates how this works:

1. EIT organization's catalog author creates and builds a vApp template that consists of a single Windows 2008 Server R2 x64 virtual machine.
2. An AES vApp author logs in to the AES organization and creates a new vApp.
3. The AES vApp author has the ability to browse the AES catalog as well as the EIT catalog because it has been published.
4. The AES vApp author deploys two of the building block "Windows 2008 Server Enterprise R2" vApps from the EIT catalog into the Bronze virtual datacenter in the AES organization.
5. The AES vApp author logs in to the two recently deployed virtual machines and adds applications to these building blocks as well as changes some of the configuration parameters such as additional hard disks or more memory.

6. The AES vApp author then creates a new vApp comprised of these two virtual machines.
7. The AES vApp author notifies the catalog author to add this new vApp to the AES catalog for developers to consume.

4.5 vApps

vApps are a new construct in vCloud Director and are used to represent a multitier application comprised of one or more virtual machines. In addition to representing the virtual machines that comprise an application the vCloud Director vApp construct allows for the representation and inclusion of the following metadata:

- Startup and shutdown sequence of virtual machines including start and stop delays.
- Runtime and storage Leases for all virtual machines in a vApp.
- Common networking configuration for the vApp.

This multitier application representation also allows for the transport of vApps between multiple environments leveraging the Open Virtualization Format (OVF) or a tool that leverages this format such as vCloud Connector. The Open Virtualization Format is a DMTF accepted standard that can be used to represent and transport virtual images from multiple virtualization vendors and is being adopted in the marketplace as a popular format for import and export.

4.5.1 vApp Design Considerations

A vCloud vApp is very different in the way it is instantiated and consumed in the vCloud than in the vSphere environment. A vApp is a container for a distributed software solution and is the standard unit of deployment in vCloud Director. It has power on operations, consists of one or more virtual machines, and can be imported or exported as an OVF package. A vCloud vApp may or may not have additional vCloud-specific constructs such as vApp networks.

Some of the general design considerations for vApps are:

- Default to one vCPU per virtual datacenter unless SMP is required (multithreaded application virtual machines).
- Always install the latest version of VMware Tools.
- Deploy virtual machines using default shares, reservations, and limits settings unless a clear requirement exists for doing otherwise.
- For virtual network adapters, use VMXNET3 where supported.
- Secure virtual machines as you would physical machines.
- Use standard virtual machine naming conventions.

4.5.2 vApp Networks

A vApp network provides network connectivity to virtual machines within a vApp. Network connectivity in this case can be contained within the vApp or provide access by way of an organization network to the outside world or other vApps within the organization. vApp networks can be created in one of two ways:

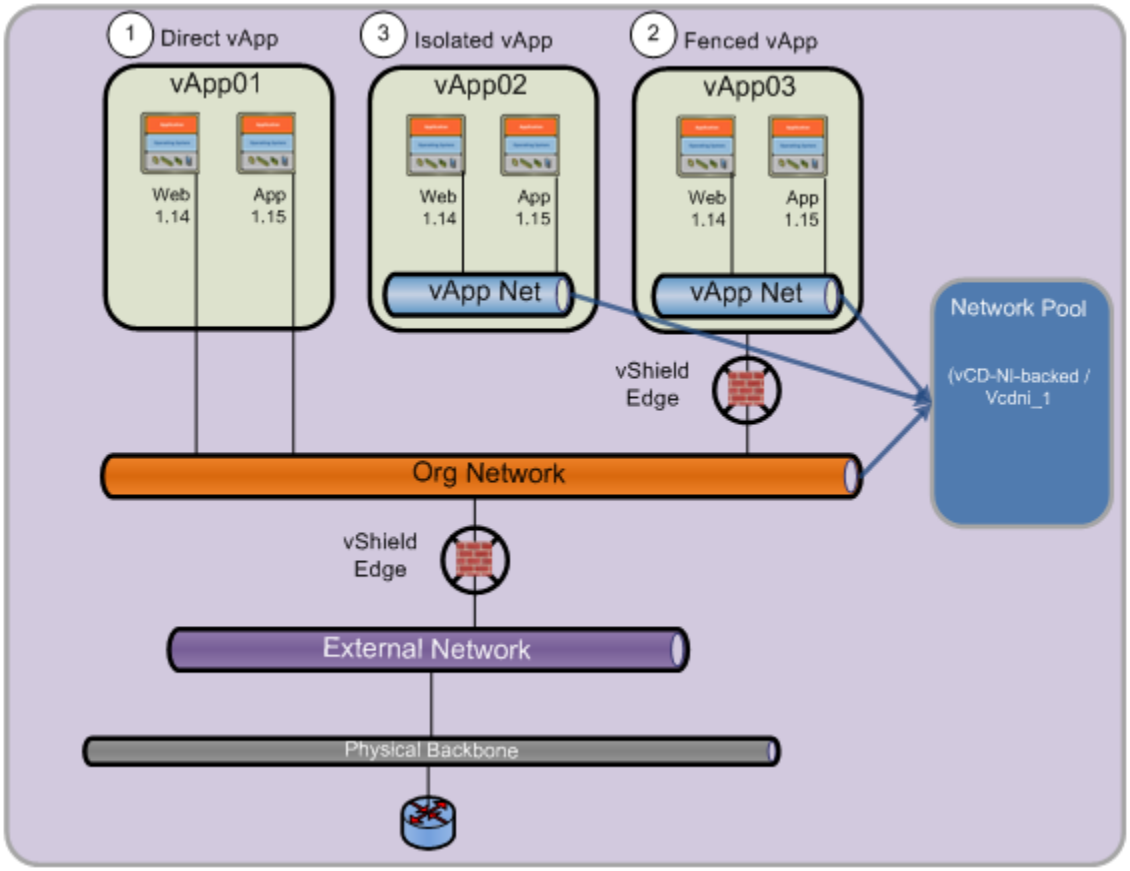
- Dynamically created when a vApp is directly connected to an organization network and deployed in fenced mode during instantiation. There is no flexibility to use the DHCP, NAT, or firewall services at the vApp network level, as it is created automatically and is not available in the UI.
- Manual creation and connection to a provider or organization network and deployed in NAT mode. There is the ability to manually define the DHCP, NAT or firewall service rules at the vApp network level when needed.

Three different types of vApp networks are available for vCloud consumers in the NewCo private vCloud:

- Direct – vApps are directly connected to the parent organization network.
- Fenced – vApps are NAT connected to the parent organization network via vShield Edge. This allows identical virtual machines (IP addresses, hostnames, and so on) to exist in different vApps by isolation of the MAC addresses.
- None (Isolated) – vApps have no external access to a parent organization network or other vApps within the organization.

NewCo vCloud users can connect vApps to the organization networks directly, or where appropriate, use fencing to isolate all of the virtual machines within a specific vApp at Layer 2 to provide quick testing and cloning capabilities without being concerned about duplicate IP addresses or hostnames. The default method for vApps requiring access to the physical network or WAN is a direct connection should be made to the appropriate external organization network. For vApps that require Layer 2 isolation, but still need access to the parent organization network, vApp users are given the ability to *fence* their vApp from the parent organization network.

Figure 10. vApp Connectivity Options



4.5.3 vApp Backup

During the requirements gathering phase it was decided to continue to leverage the existing method of virtual workload backup and recovery. NewCo wants to complete the initial architecture and implementation of the vCloud, and then consider implementing a different backup solution for the vCloud workloads. For the initial deployment NewCo will maintain the same architecture used in the vSphere environment with the exception of a new and dedicated backup network and associated VLAN.

NewCo currently uses backup software agents installed inside the guest operating systems of the virtual machines. For the purposes of enhancing the backup and recovery performance a dedicated backup network will be used in the vCloud environment. These backups are managed by the vCloud provider and include all virtual machines across both vSphere resource clusters.

4.5.3.1. Virtual Machine Backups

In the future, if NewCo chooses to implement an image-level backup strategy, most backup products that support VADP (VMware APIs for Data Protection) to backup vSphere can also be used to backup the virtual machines managed by vCloud Director. With these products you can backup all of the data representing the virtual machines, but cannot capture the metadata of the vApp, including the owner, network, and organization. Without this data a restore of the virtual machines within a vApp requires some manual reconfiguration. vCloud Director 1.5 introduced maintenance for vApps that prevents changes to the properties of virtual machines and vApp metadata for non-system administrator users, which is useful to preserve the state of the vApp during backup and recovery. The simplified steps to perform a virtual machine restore are to shut down the vApp, perform a recovery of *only* the VMDK files associated with the virtual machines in question, and then power on the vApp. Because none of the metadata associated with the vApp or virtual machine configuration (UUID, MAC address) was changed, recovery will have no impact on vCloud Director.

4.5.4 Example Workload Sizing

VMware recommends assessing the planned workloads to assist in sizing. The following is an estimated sizing table that can be used as a reference for future design activities.

Table 32. Virtual Machine Sizing and Distribution

Virtual Machine	Distribution	Virtual Machines	CPU	RAM
Small	55%	385	1	1GB
Medium	36%	252	2	2GB
Large	7%	49	4	4GB
X-Large	2%	14	8	8GB
XX-Large	0% (Future)	0	12	32GB
Total	100%	700	---	---

4.6 Organization Users and Roles

Organization users and roles are specific to the organization where they are defined. The NewCo design calls for both the EIT and AES to leverage the same Active Directory infrastructure at NewCo (NewCoDS.com) for RBAC for the vCloud. Both organizations will leverage Active Directory Groups to designate access to their respective organizations. The appropriate AD groups have been added with the appropriate roles to each organization and ongoing organization access will be controlled by adding or removing users from these groups in Active Directory.

Several design principles and requirements influenced the user and role design:

- Principle of least privilege to accomplish necessary tasks for a particular role.
- The division of responsibilities within an organization.
- Each organization should have a "Local" organization admin user as a backup. This is a risk mitigation measure to avoid outages due to LDAP authentication/connectivity issues, resulting in loss of administration control of the organization vCloud objects.
- There should be at least two organization admin users in an organization to prevent loss of administration control due to account issues such as lost passwords and so on. A lost password can be recovered by a system administrator, but operationally it is better to have a backup organization admin to reduce reliance on the system administrators.

Although vCloud Director allows for many predefined and completely granular customized roles, the initial design calls for the following vCloud Director roles defined in each organization:

- Organization administrator
- Catalog author
- vApp author

4.6.1 Organization Administrator

Initially there are two organization administrators assigned and dedicated to each organization. They are responsible for some common reoccurring administrative tasks such as adding and removing users and groups to the organization, configuring organization policies and settings, and configuring the services or firewall rules on a routed external or internal organization network. Initially, the vCloud system administrators are the backup for this role.

4.6.2 Catalog Author

There are initially two catalog authors assigned and dedicated to each organization and responsible for catalog management within their respective organization. This includes populating the catalog by virtual machine or OVF import or creating from scratch. This role is also responsible for both sharing and publishing the catalogs within their organization. Initially, the organization administrator is the backup for this role.

4.6.3 vApp Author

There are initially approximately 10–20 vApp authors assigned and dedicated to each organization—these users comprise the main consumers of vCloud services and resources. The vApp authors have the ability to create and manage vApps within the organization including reading the catalog items for deploying vApps. As with the other roles, role access will be controlled by adding and removing users from this group in AD. Initially, other vApp authors are the backup for this role.

Table 33. EIT Users and Roles

User/Group	Role	Context
Eit-orgadmin	Organization administrator	Local user
NewCods\eit-orgadmins	Organization administrators	AD group
NewCods\eit-catalogauthors	Catalog authors	AD group
NewCods\eit-vappauthors	vApp authors	AD group

Table 34. AES Users and Roles

User/Group	Role	Context
Aes-orgadmin	Organization administrator	Local user
NewCods\aes-orgadmins	Organization administrators	AD group
NewCods\aes-catalogauthors	Catalog authors	AD group
NewCods\aes-vappauthors	vApp authors	AD group

5. vCloud Security

5.1 vSphere Security

Security is critical for any company. The following sections address host, network, vCenter, and vCloud Director security considerations, with references where applicable.

5.1.1 Host Security

Chosen in part for its limited management console functionality, ESXi is configured by NewCo with a strong root password that is stored following corporate password procedures. After the ESXi hosts are initially prepared by vCloud Director 1.5, the ESXi lockdown mode is also enabled to prevent root access to the hosts over the network, and appropriate security policies and procedures are created and enforced to govern the systems. Because ESXi cannot be accessed over the network, sophisticated host-based firewall configurations are not required.

5.1.2 Network Security

Virtual switch security settings are listed in the following table.

Table 35. Virtual Switch Security Settings

Function	Setting
Promiscuous Mode	Management cluster – Reject Cloud resources – Reject
MAC address changes	Management cluster – Reject Cloud resources – Reject
Forged Transmits	Management cluster – Reject Cloud resources – Reject

5.1.3 vCenter Security

vCenter Server is installed using a local administrator account. When vCenter Server is joined to a domain, this results in any domain administrator gaining administrative privileges to vCenter. VMware recommends NewCo remove this potential security risk by creating a new vCenter Administrators group in Active Directory and assigning it to the vCenter Server Administrator role, making it possible to remove the local Administrators group from this role.

5.1.4 VMware vCloud Director Security

Standard Linux hardening guidelines must be applied to the vCloud Director virtual machine. There is no need for local users, and the root password is only needed during install and upgrades to the vCloud Director binaries. Additionally, certain network ports must be open for vCloud Director use. For further information, see the *vCloud Director Administrators Guide* (https://www.vmware.com/support/pubs/vcd_pubs.html).

5.2 Additional Security Considerations

The following are examples of use cases that require special security considerations:

- End-to-end encryption from a guest virtual machine to its communication endpoint, including encrypted storage using encryption in the guest OS and/or storage infrastructure.
- Provisioning of user accounts and/or access control from a single console.
- Need to control access to each layer of a hosting environment. That is, rules and role-based security requirements for an organization.
- vApp requirements for secure traffic and/or VPN tunneling from a vShield Edge device at any network layer.

For additional details on security and compliance considerations for vCloud see *Operating a VMware vCloud* in the VMware vCloud Architecture Toolkit.

6. vCloud Management

6.1 vSphere Host Setup Standardization

Host profiles can be used to automatically configure network, storage, security and other features. This feature, along with vSphere Auto Deploy, simplifies and automates the installation of ESXi hosts, and is used to standardize all host configurations.

VM Monitoring is enabled on a cluster level within HA and uses the VMware Tools heartbeat to verify that a virtual machine is alive. If a virtual machine fails, causing VMware Tools heartbeat to not be updated, VM Monitoring tests to see if any storage or networking I/O has occurred over the last 120 seconds and, if not, the virtual machine is restarted.

VMware recommends enabling both VMware HA and VM Monitoring on the management cluster and the vCloud resources clusters.

6.2 VMware vCloud Director Logging

Logging is one of the key components in any infrastructure. It provides audit trails for user logins and logouts among other important functions. Logging records various events happening in the servers, and helps diagnose problems, detect unauthorized access, and so on. In some cases, regular log analyses can proactively stave off problems that may turn out to be critical to the business.

Each vCloud Director cell logs audit messages to the database where they are retained for 90 days by default. If log retention is needed for longer than 90 days or centralized logging is required, an external syslog server can be configured and used as a duplicate destination for the events that are logged. Individual components can also be configured to redirect syslog messages to tenant-designated syslog servers.

In vCloud Director, there are two options for logging. The logs can be stored either locally to the server or in a centralized (syslog) location. During the initial installation, the administrator can choose which option to use.

During the initial installation, if a syslog server address is not entered, the logs are stored locally. The syslog server listens on port 514 using the UDP protocol.

If local storage was chosen during the installation, the administrator can later change it using the following procedure:

1. Log in to the vCloud Director cell using a vCenter virtual machine console, or using SSH if it is enabled.
2. Change directory to `/opt/vmware/vcloud-director/etc` as follows:

   ```
   cd /opt/vmware/vcloud-director/etc
   ```

3. Make a backup of `log4j.properties` as follows:

   ```
   cp log4.properties {,.original}
   ```

4. Modify the following line by appending the string in **bold**:

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

5. Edit `log4j.properties` with your preferred editor and add the following lines:

```
log4j.appender.vcloud.system.syslog=org.apache.log4j.net.SyslogAppender
log4j.appender.vcloud.system.syslog.syslogHost=remoteSyslogHost.example.com:<PORT>
# For default listening port of 514, <PORT>can be left blank
log4j.appender.vcloud.system.syslog.facility=LOCAL1log4j.appender.vcloud.system.sys
log.layout=com.vmware.vcloud.logging.CustomPatternLayout
log4j.appender.vcloud.system.syslog.layout.ConversionPattern=%d{ISO8601} | %-8.8p |
%-25.50t | %-30.50c{1} | %m | %x%n
log4j.appender.vcloud.system.syslog.threshold=INFO
```

6. Save the file and restart the vCloud Director cell.

```
Servicevmware-vcd restart
```

To enable centralized logging in all of the vCloud Director cells, repeat this procedure for each cell.

6.3 vShield Edge Logging

Remote logging of firewall events to a central syslog host provides a way to greatly increase security and network forensic capabilities. In addition to vCloud Director logs, vShield Edge devices deployed within a vCloud director environment will inherit the default syslog for networks which can be set to the same remote syslog system used by vCloud Director. To specify the remote syslog server for networks in vCloud Director:

1. Log in to the vCloud Director UI as the system administrator.
2. From the Administration Tab, under System Settings, Select General.
3. Under “Default syslog server settings for networks specify up to two syslog servers.
   a. Syslog server 1
   b. Syslog server 2
4. Click Apply.

Any new Routed Organization deployed will inherit the syslog server settings specified above. This will provide a location to send firewall logs for specific Firewall Rules when configured by the Organization or System Administrator. For existing Routed Organization networks you can update the syslog settings for a particular network by completing the following:

1. From the **Organization Administration** tab under **Cloud Resources**, select **Networks**.
2. Right click the network and select **Synchronize syslog server settings**.

6.4 vSphere Host Logging

Remote logging to a central host provides a way to greatly increase administration capabilities. Gathering log files on a central server facilitates monitoring of all hosts with a single tool and enables aggregate analysis and the ability to search for evidence of coordinated attacks on multiple hosts.

Within each ESXi host, syslog behavior is managed by leveraging `esxcli`. These settings determine the central logging host that will receive the syslog messages. The hostname must be resolvable using DNS.

For this initial implementation, all NewCo management and resource hosts will be configured to send log files to two central syslog servers residing in the management cluster. Requirements for this configuration are.

- `Syslog.Local.DatastorePath` – A location on a local or remote datastore and path where logs are saved.
- `Syslog.Remote.Hostname` – A remote server's DNS name or IP address where logs are sent using the syslog protocol. The DNS name for syslog is mgmt-syslog.example.com
- `Syslog.Remote.Port` – A remote server's UDP port where logs are sent using the syslog protocol. Default is port 514.
- #Configure NewCo syslog servers.

  ```
  esxcli system syslog config set --default-rotate 20 --loghost udp://mgmt-syslog1.example.com:514,udp://mgmt-syslog2.example.com:1514
  ```

- #Configure ESXi logs to send to syslog

  ```
  esxcli system syslog config logger set --id=hostd --rotate=20 --size=2048
  esxcli system syslog config logger set --id=vmkernel --rotate=20 --size=2048
  esxcli system syslog config logger set --id=fdm --rotate=20
  esxcli system syslog config logger set --id=vpxa --rotate=20
  ```

6.5 vCloud Monitoring

Monitor the following items through VMware vCloud Director. As of VMware vCloud Director 1.5 this must be done with custom queries to VMware vCloud Director using the Admin API to get the consumption data on the different components. Some of the components in VMware vCloud Director can also be monitored by aggregating the Syslog-generated logs from the different VMware vCloud Director cells that would be found on the centralized log server.

Table 36. VMware vCloud Director Monitoring Items

Scope	Item
System	• Leases • Quotas • Limits
vSphere Resources	• CPU • Memory • Network IP address pool • Storage free space
Virtual Machines/vApps	Not in scope

In addition to the vCloud Director, UI monitoring can be accomplished through a JMX interface.

6.5.1 vCloud Director

As of VMware vCloud Director 1.0, monitoring is performed using custom queries to VMware vCloud Director using the Admin API to capture the summary consumption data on organization virtual datacenter, through MBeans, and through standard Linux and JMX monitoring services running on the vCloud Director guest. Some of the components in VMware vCloud Director can also be monitored by aggregating the Syslog-generated logs from the different VMware vCloud Director cells that would be found on the centralized log server.

6.5.2 vCenter Server

Multiple vCenter Servers are present within a vCloud instance to manage the virtual resources within the management and resource groups. Use of vCenter alerts and health of vpxd service provides advance notice when vCenter Servers are resource constrained or have suffered a fault.

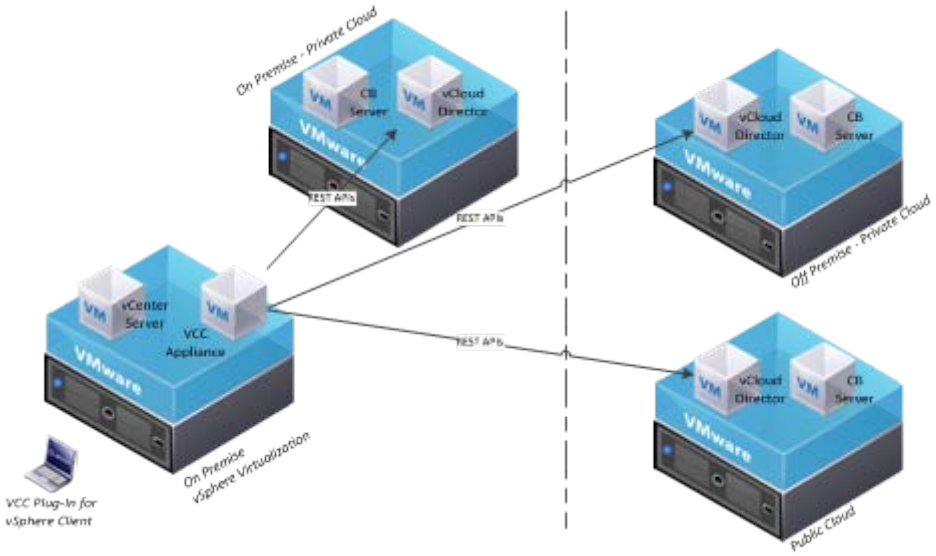
7. Extending vCloud

vCloud Director is intended to be the middleware or operating system of the enterprise datacenter and as such can easily be expanded to provide enhanced functionality, resiliency, integration, or automation. Customers who want to extend the existing functionality can leverage the vCloud Connector, API, vCenter Orchestrator, or VMware Service Manager. Each of these technologies enables you to extend vCloud.

7.1 vCloud Connector

VMware vCloud® Connector (vCC) is a virtual appliance that allows vSphere administrators to move virtual machines between vSphere environments and vCloud environments. vCloud Connector can migrate virtual machines and vApps between local vSphere and vCloud environments as well as remote vSphere and vCloud environments. The origination and destination vCloud can be a public or private vCloud. The vCloud Connector can be used as a migration tool or to establish a hybrid vCloud, including providing administrative capabilities across multiple vSphere and vCloud environments. Figure 11 provides an overview of communication protocols between vCloud Connector and vCloud Director:

Figure 11. vCloud Connector



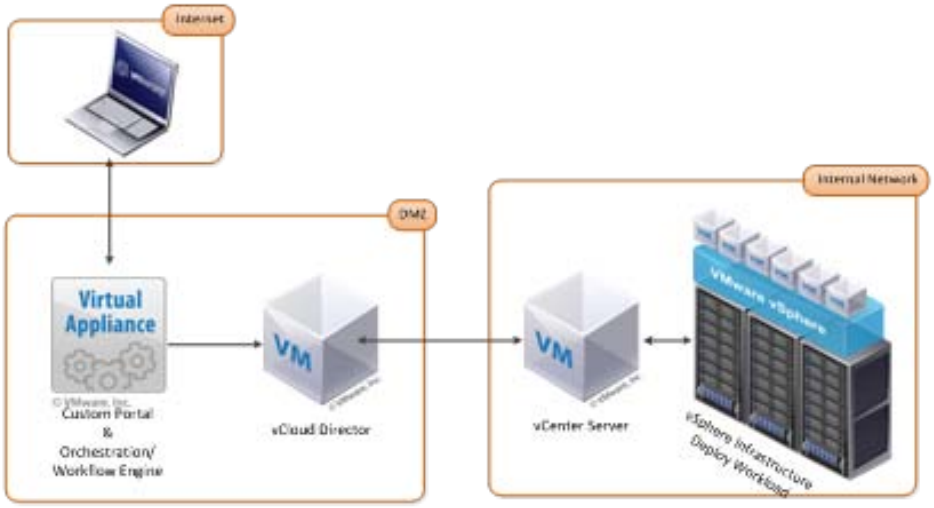
7.2 vCloud API

There are two ways to interact with the vCloud Director cell: using the browser-based UI or through the vCloud API. The browser-based UI has limited customization capability—therefore, to enhance the user experience, a service provider or an enterprise customer can develop a customized portal to integrate with vCloud Director. To enable integration, the vCloud API provides a rich set of calls in vCloud Director.

vCloud APIs are RESTful, which allows for loose coupling of services between the server and consumer, are highly scalable, and use the HTTP or HTTPS protocol for communication. The APIs are grouped into three sections based upon the functionality they provide and type of operation. There are several options available to implement the custom portal using the vCloud API. These are using VMware Service Manager™, vCenter Orchestrator, or by using third-party integrators. Some of these may require customization to design workflows to satisfy customer requirements.

Figure 12 shows a use case where a service provider has exposed a custom portal to end users on the Internet.

Figure 12. vCloud API Logical Representation



End users log into the portal with a valid login and password and are able to select a predefined workload (from a catalog list) to deploy. The user's selection, in turn, initiates a custom workflow that deploys the requested catalog item (for example, vApp) in the vCloud.

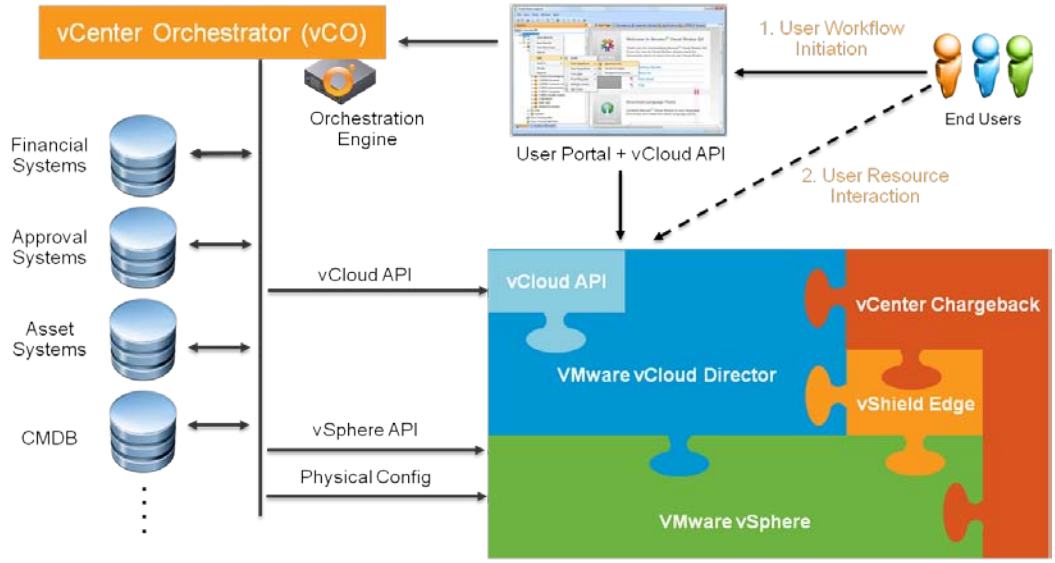
Currently, the vCloud API is available in the form of a vCloud SDK with the following language bindings: Java, C-Sharp, and PHP.

7.3 Orchestrating vCloud

Because vCloud Director leverages core vSphere infrastructure, automation is possible through vCenter Orchestrator. vCenter Orchestrator provides out-of-the-box workflows that can be customized to automate existing manual tasks. Administrators can use sample workflows from a standard workflow library that provides blueprints for creating additional workflows, or create their own custom workflows. Currently there are over 800 tasks that can be automated in vCenter Server using vCenter Orchestrator.

vCenter Orchestrator integrates with vCloud Director through a vCloud Director plug-in that communicates by way of the vCloud API. vCenter Orchestrator can also orchestrate workflows at the vSphere level through a vSphere plug-in.

Figure 13. vCloud Orchestration



7.4 VMware Service Manager Cloud Provisioning (VSM CP)

Customers can build upon the modular nature of vCloud Director to consume vCloud services in different ways including the native vCloud portal, custom developed portals, or an existing portal that leverages the vCloud API. For customers who want to expand on the existing capabilities of vCloud Director without writing a completely new front-end portal, VMware Service Manager can be used to provide an enhanced and extensible presentation layer for vCloud consumption. VMware Service Manager Cloud Provisioning provides a customer-centric portal that exposes service request templates used in deploying vApps and virtual machines into the vCloud using vCloud Director. The primary advantages that VMware Service Manager provides are:

- Front-end self-service catalog portal.
- Governance for lower tier applications.
- Access to owned items as well as the capability to request changes.

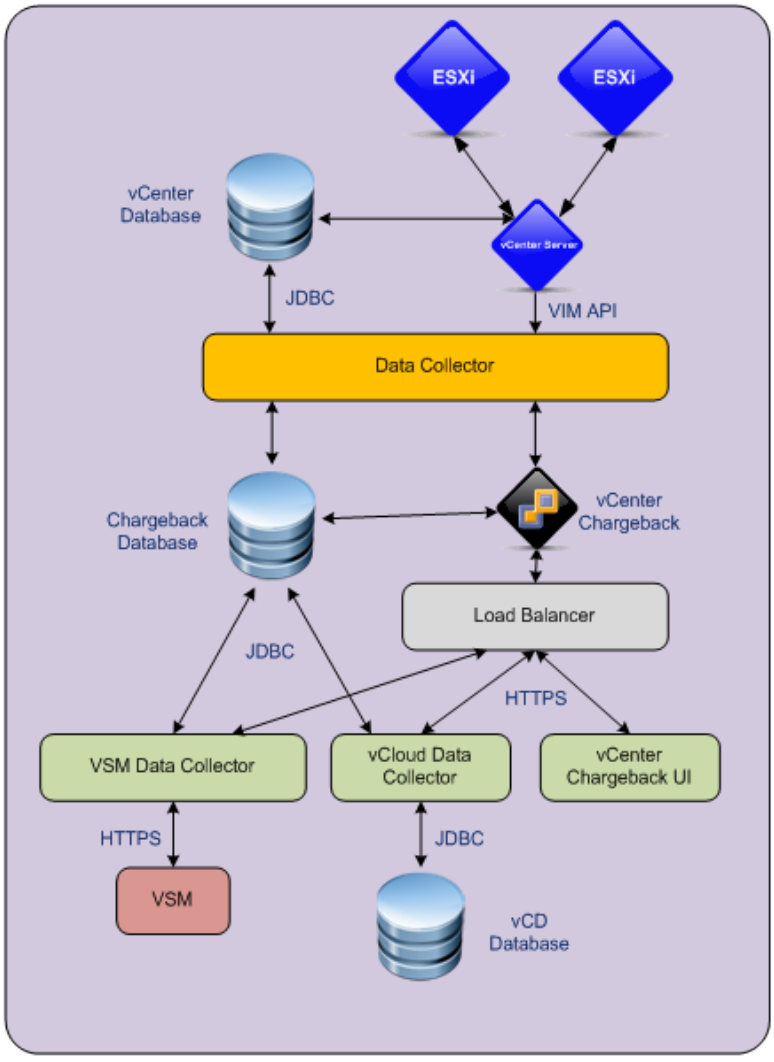
VMware Service Manager includes an easy- to-use GUI-based workflow engine to design and support service-oriented workflow, a federated CMDB that supports the ability to visualize the vCloud infrastructure, and an integration platform that includes connectors to VMware vCenter Configuration Manager™, and vCenter Orchestrator to enhance the self-service provisioning for the vCloud. Using the quick start package in VMware Professional Service, VSM CP can typically be implemented in about two weeks.

Figure 14. VMware Service Manager

8. Metering

vCenter Chargeback provides organization level visibility and cost configuration within the NewCo vCloud. Although NewCo is internally not ready to implement actual budget code chargeback at this time, vCenter Chargeback will be used to generate monthly reports with sample costs for cost visibility (*showback*) so that a process can be developed for actual business unit chargeback within a year. The following diagram depicts the chargeback logical architecture within the NewCo design.

Figure 15. vCenter Chargeback Logical Diagram



For the initial implementation, two cost models are configured to reflect the two different resource allocation policies being leveraged at NewCo. The resource allocation policies are configured at the organization virtual datacenters and there are two of these in each organization. vCenter Chargeback will synchronize the hierarchy from vCloud Director and place the organizational objects under the appropriate chargeback hierarchy based on the resource allocation policy for the organization virtual datacenter.

Table 37. NewCo Chargeback Billing Policies

Organization	Virtual Datacenter	Resource Allocation	Billing Policy
EIT	EIT Gold	Reservation	vCloud Director Reservation Pool
EIT	EIT Silver	Pay-As-You-Go	vCloud Director Pay-As-You-Go – Fixed
AES	AES Gold	Reservation	vCloud Director Reservation Pool
AES	AES Silver	Pay-As-You-Go	vCloud Director Pay-As-You-Go – Fixed

For the NewCo design, achieving these cost structures involved configuring two cost models and using the appropriate billing policies above to reflect the level of service being provided. Rate factors are configured to a value of 1 for CPU, memory, and disk.

8.1 Silver Level of Service – Cost Configuration

Both the EIT and AES Silver virtual datacenters charge based on a fixed slot pricing and chargeback model that is calculated monthly. This model uses the following fixed vCPU and memory matrix costs.

Table 38. NewCo Pay-As-You-Go Fixed Cost Model

	512MB	1GB	2GB	3GB	4GB	8GB
1 vCPU	$248.00	$272.00	$289.00	$315.00	$341.00	$461.00
2 vCPU	N/A	N/A	$308.00	$331.00	$354.00	$477.00
4 vCPU	N/A	N/A	N/A	N/A	$386.00	$509.00

8.2 Gold Level of Service – Cost Configuration

Both the EIT and AES Gold organization virtual datacenters charge based on resources allocated to their Reservation Pool with pricing calculated monthly. The cost model has monthly base rate values specified for CPU, memory and storage. The costs are prorated if the organization virtual datacenter has been deployed for less than a month.

Table 39. Reservation Cost Model

Resource	Base Rate
CPU	$20 per GHz/month
Memory	$10 per MB/month
Storage	$3 per GB/month

Monthly cost reports are scheduled to be automatically generated in PDF format and emailed to department stakeholders in both the EIT and AES departments.

Appendix A: Bill of Materials

The inventory and specifications of components comprising the vCloud are provided in Table 40.

Table 40. Management Cluster Inventory

Item	Quantity	Name/Description
ESXi Host	3	• Vendor X compute resource • Chassis: 1 • Blades per Chassis: 8 • Processors: 2 x Intel Xeon x5630 2.53 GHz (4 core) • Memory: 32GB • Version: vSphere 5.0 (ESXi)
vCenter Server	1	• Type: virtual machine • Guest OS: Windows Server 2008 x64 • 2 vCPUs • 4GB memory • 1 vNIC • Minimum free disk space: 10GB • Version: 5.0
VMware vCloud Director cell	1	• Minimum number of vCloud Director cells: 1 • Type: virtual machine • Guest OS: RHEL 5.6 x64 • 4 vCPUs • 4GB memory • 2 vNICs • Version: 1.5
SQL 2008 Database	2	• Type: Physical Server – Microsoft Failover Cluster • Guest OS: Windows Server 2008 Enterprise R2 • SQL Server 2008 Enterprise SP3 x64 • 4 vCPUs • 8GB memory • 1 NIC

Item	Quantity	Name/Description
vShield Manager	1	• Type: virtual machine appliance • Version: 5.0 • 1vCPU • 4GB memory • 1 vNIC
vCenter Chargeback Server	1	• Type: virtual machine • Guest OS: Windows Server 2008 x64 • Version: 1.6.2 • 2 vCPUs • 2GB memory • 1 vNIC
NFS Appliance	0	• N/A
vCenter CapacityIQ	1	• Type: virtual machine • Guest OS: Windows Server 2008 x64 • 2 vCPUs • 2GB memory • 1 vNIC
Domain Controllers (AD)	1	• Dedicated AD virtual machine built specifically for vCloud infrastructure with failback to alternate DCs. • Type: virtual machine • Windows Server 2008 • 1 vCPU • 4GB memory • 1 NIC
Storage	1	• FC SAN Array • VMFS • LUN Sizing: 750GB • RAID5

Table 41 provides a vCloud resources inventory.

Table 41. Cloud Resources Inventory

Item	Quantity	Name/Description
ESXi host	6	• Vendor X compute blade • Chassis: 2 • Blades per chassis: 8 • Blade Type: Vendor X Blade Type Y • Processors: 2 Socket Intel Xeon X5670 (6 core, 2.9 GHz Westmere) • Memory: 96GB • Version: vSphere 5.0
vCenter Server	1	• Same as management cluster
vShield Edge Appliances	Multiple	• Type: virtual machine • 1 vCPU • 256MB RAM • 1vNIC
Storage	1	• FC SAN array • VMFS • Cluster 1 LUN sizing: 900GB • RAID Level: 5 • Cluster 2 LUN sizing: 1,500GB • RAID Level: 5