

vCloud Suite 6.0 Architecture Overview and Use Cases

vCloud Suite 6.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001713-00

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2014, 2015 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

| | | |
|----------|---|----|
| | <i>About vCloud Suite Architecture Overview and Use Cases</i> | 5 |
| 1 | Introduction to vCloud Suite | 7 |
| | List of vCloud Suite Components | 7 |
| 2 | Architecture Overview | 9 |
| | Conceptual Design of a vCloud Suite Environment | 11 |
| | vCloud Suite Components in the Management Cluster | 13 |
| | Software-Defined Data Center Core Infrastructure | 14 |
| | Delivering an Infrastructure Service | 19 |
| | Delivering Platform as a Service | 22 |
| 3 | Deploying vCloud Suite | 23 |
| | Install vCloud Suite Components | 23 |
| | Upgrade vCloud Suite Components | 24 |
| | External Dependencies for Deploying vCloud Suite | 26 |
| | System Requirements of vCloud Suite Components | 27 |
| | Security Considerations | 27 |
| | vCloud Suite Licensing | 34 |
| 4 | vCloud Suite Use Cases | 49 |
| | Disaster Recovery to Cloud | 49 |
| | Index | 55 |

About vCloud Suite Architecture Overview and Use Cases

The *vCloud Suite Architecture Overview and Use Cases* publication provides information about the design and capabilities of cloud environments based on VMware vCloud[®] Suite.

vCloud Suite is a collection of interoperable VMware products. *vCloud Suite Architecture Overview and Use Cases* provides a listing of components, high-level design guidelines for vCloud Suite deployment and operation, as well as example use cases.

The provided architecture overview is based on concepts from the practical approach used by the VMware Professional Services organization.

vCloud Suite Architecture Overview does not include detailed installation and configuration instructions for individual components. You can find that information in the dedicated documentation sets for individual VMware products.

Intended Audience

This information is intended for IT professionals and business decision makers with prior knowledge of virtualization and data center operations, who want to understand the capabilities of vCloud Suite and learn about recommended deployment models and example use cases.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

Introduction to vCloud Suite

VMware vCloud Suite lets you build and operate your software-defined data centers based on vSphere. vCloud Suite contains components that can be integrated to deliver IT as a service.

The vCloud Suite components are available to be downloaded, installed, and configured separately. When they are deployed and configured together these interoperable components enable the software-defined data center (SDDC) where virtual and non-virtual resources are made available as a service. Control of the data center is fully automated by software, and hardware configuration is maintained through software systems. vCloud Suite enables you to build and manage a vSphere-based private cloud on which to run workloads. You can extend your vCloud Suite deployment by adding public cloud capacity and services using VMware vCloud[®] Air[™] or vCloud Air Network Service Providers, and using vRealize Operations Manager to manage workloads based in vCloud Air or other public clouds. The result is a hybrid cloud using a common vRealize cloud management platform..

You can extend your vCloud Suite by using vCloud Air as a second site in your datacenter environment. Use vCloud Suite together with with the vCloud Air to satisfy business needs such as business continuity and burst capacity.

vCloud Suite can serve the needs of different organizations, from SMBs to large enterprises and organizations in the public sector.

List of vCloud Suite Components

A vCloud Suite edition contains individual products with different versions. To ensure interoperability, you should verify that the components of your vCloud Suite environment are the correct versions.

vCenter Server is required for building the core infrastructure of the Software-Defined Data Center (SDDC).

NOTE VMware makes available patches and releases to address critical security issues for several products. Verify that you are using the latest security patches and releases for a given component when deploying vCloud Suite.

Table 1-1. Components of vCloud Suite 6.0 and their versions

| Product name | Version | Description |
|-------------------------------|---------|---|
| ESXi | 6.0 | Provides bare-metal virtualization of servers so you can consolidate your applications on less hardware. |
| vCenter Server | 6.0 | Provides a centralized platform for managing vSphere environments. |
| vCenter Site Recovery Manager | 6.0 | Provides disaster recovery capability that lets you perform automated orchestration and nondisruptive testing for virtualized applications. |

Table 1-1. Components of vCloud Suite 6.0 and their versions (Continued)

| Product name | Version | Description |
|--|---------|--|
| vRealize Automation | 6.2.1 | Provides functionality for deploying and provisioning of business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers. |
| vRealize Automation Application Services | 6.2.0 | Provides automated application provisioning in the cloud including deploying and configuring the application's components and dependent middleware platform services on infrastructure clouds. |
| vRealize Business for vSphere | 6.1.0 | Provides transparency and control over the costs and quality of IT services that is critical for private or hybrid cloud success. |
| vRealize Configuration Manager | 5.7.3 | Provides automation of configuration and compliance management across your virtual, physical and cloud environments, assessing them for operational and security compliance. |
| vRealize Hyperic | 5.8.4 | Provides monitoring of operating systems, middleware and applications running in physical, virtual, and cloud environments. |
| vRealize Infrastructure Navigator | 5.8.4 | Provides automated discovery of application services, visualizes relationships, and maps dependencies of applications on virtualized compute, storage and network resources. |
| vRealize Operations Manager | 6.0.1 | Provides comprehensive visibility and insights into the performance, capacity and health of your infrastructure. |
| vRealize Orchestrator | 6.0.1 | Provides the capability to create workflows that automate activities such as provisioning virtual machine, performing scheduled maintenance, initiating backups, and many others. |
| vSphere Big Data Extensions | 2.1.0 | Simplifies running Big Data workloads on the vSphere platform. |
| vSphere Data Protection | 6.0 | Provides advanced data protection with backup and recovery to disk. |
| vSphere Replication | 6.0 | Provides replication, at the individual virtual machine disk level, between datastores hosted on any storage. |

Network Components for vCloud Suite

You can adopt NSX for vSphere for the networking and security needs of your SDDC. vCloud Suite customers have the option to purchase NSX for vSphere at a reduced, add-on price. NSX provides layer 2 to layer 7 network virtualization, with security policies that follow workloads across the data center for faster network provisioning and management.

To learn more about NSX for vSphere, visit the VMware NSX™ Web site:

<http://www.vmware.com/products/nsx>

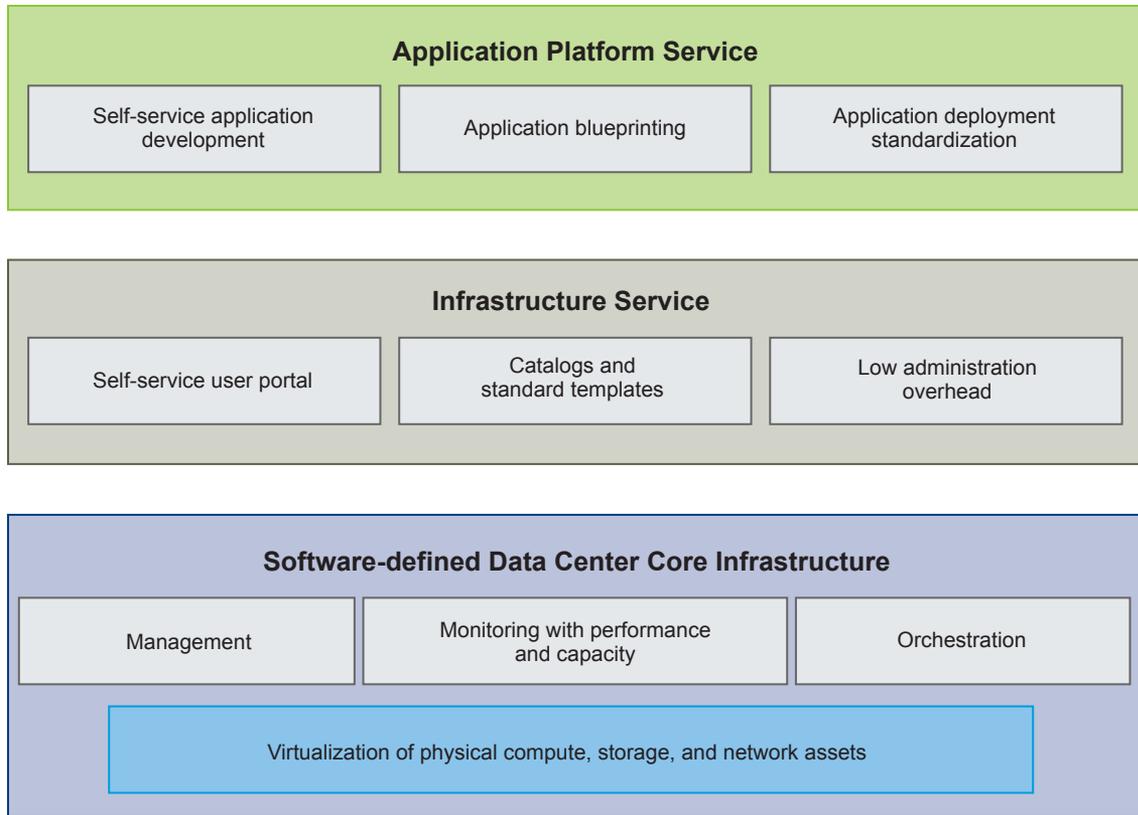
Architecture Overview

To enable the full set of vCloud Suite features, you must perform a series of installation and configuration operations. The software-defined data center provides different types of capabilities, with more complex features building on top of underlying infrastructure.

Delivering the full operational capabilities of vCloud Suite to your organization or clients is a structured process. In a large organization, it might involve cycles of assessment, design, deployment, knowledge transfer, and solution validation. Depending on your organization, you should plan for an extended process that involves different roles.

Not every environment needs the full scope of vCloud Suite capabilities at a given time. Begin by deploying the core datacenter infrastructure, which enables you to add capabilities as your organization requires them. Each of the software-defined data center layers might require you to plan and perform a separate deployment process.

Figure 2-1. Layers of the Software-Defined Data Center



SDDC Core Infrastructure

The basis of the vCloud Suite deployment is the resource abstraction layer. By using VMware software, you can virtualize compute, network, and storage resources in your data center and abstract them from the underlying hardware. ESXi and vCenter Server enable you to establish a robust virtualized environment into which all other solutions integrate. The resource abstraction layer provides the foundation for the integration of orchestration and monitoring solutions by VMware. Additional processes and technologies build on top of the infrastructure to enable infrastructure as a service and platform as a service.

Infrastructure Service

Infrastructure services introduce fast, self-service provisioning of virtual machines to physical, virtualized, or hybrid clouds. The IaaS layer is represented by vRealize Automation, which provides service provisioning, catalog management, policy based management, and authorization.

Application Platform Service

The application platform service enables end-to-end deployment and configuration of applications, along with their dependencies, to a target deployment infrastructure.

You can enhance your vCloud Suite environment by integrating additional products and services by VMware, in order to enable capabilities such as disaster recovery to cloud, software-defined storage, and software-defined networking. For information about implementing failover protection for virtual machines in vCloud Air, see *“Disaster Recovery to Cloud,”* on page 49.

■ [Conceptual Design of a vCloud Suite Environment](#) on page 11

To start deploying vCloud Suite, only a small number of physical hosts are needed. Distribute your hosts into three types of clusters, in order to establish the foundation of a deployment that can later scale to tens of thousands of VMs.

- [vCloud Suite Components in the Management Cluster](#) on page 13
The number of vCloud Suite components in the management cluster increases as you add capabilities. A management cluster can contain a minimal set of products that you expand as needed.
- [Software-Defined Data Center Core Infrastructure](#) on page 14
The core of vCloud Suite environments consists of vSphere and the associated monitoring and orchestration products, such as vRealize Operations Manager and vRealize Orchestrator.
- [Delivering an Infrastructure Service](#) on page 19
The ability to deliver infrastructure as a service represents the technological and organizational transformation from traditional data center operations to cloud. The infrastructure service lets you model and provision VMs and services across private, public, or hybrid cloud infrastructure.
- [Delivering Platform as a Service](#) on page 22
Platform-as-a-Service (PaaS) lets you model and provision applications across private, public, and hybrid cloud infrastructures.

Conceptual Design of a vCloud Suite Environment

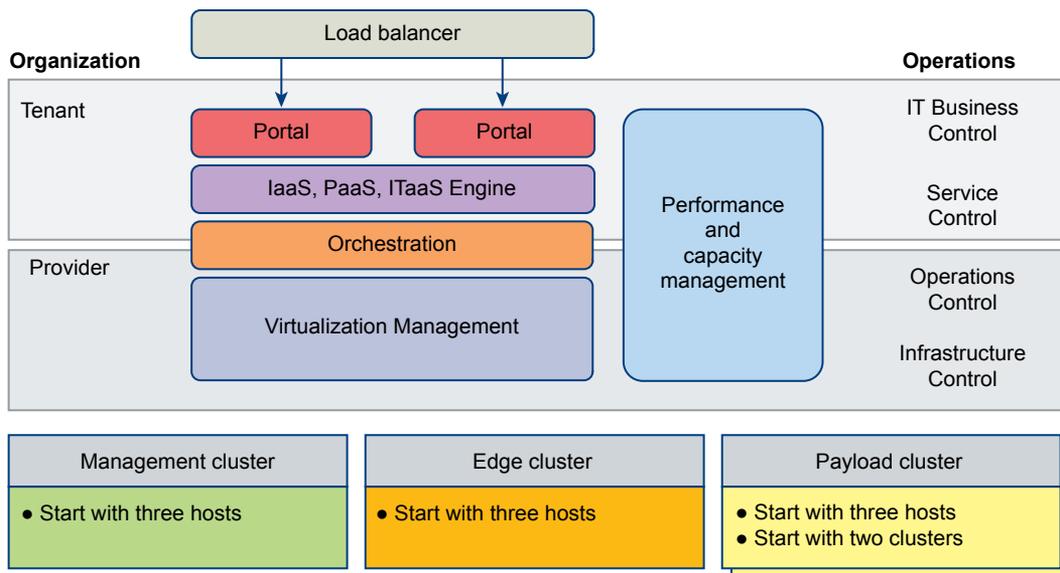
To start deploying vCloud Suite, only a small number of physical hosts are needed. Distribute your hosts into three types of clusters, in order to establish the foundation of a deployment that can later scale to tens of thousands of VMs.

Management, Edge, and payload clusters run the entire vCloud Suite infrastructure, in addition to customer workloads.

Deploying and leveraging vCloud Suite is a process that involves both technological transformation and operational transformation. As new technologies are deployed in the data center, your organization must also implement appropriate processes and assign the necessary roles.

In the diagram below, technological capabilities in color appear over organizational constructs in grayscale.

Figure 2-2. Conceptual Design of a vCloud Suite environment



Management cluster

The hosts in the management cluster run the management components required to support the software-defined data center. A single management cluster is required for each physical location. ESXi hosts running in the management cluster can be manually installed and configured to boot using local hard drives.

A management cluster provides resource isolation. Production applications, test applications, and other types of applications cannot use the cluster resources reserved for management, monitoring, and infrastructure services. Resource isolation helps management and infrastructure services to operate at their best possible performance level. A separate cluster can satisfy an organization's policy to have physical isolation between management and production hardware.

Edge cluster

The Edge cluster supports network devices that provide interconnectivity between environments. It provides protected capacity by which internal data center networks connect via gateways to external networks. Networking edge services and network traffic management take place in the cluster. All external facing network connectivity terminates in this cluster.

The ESXi hosts in the edge cluster are managed by a dedicated vCenter Server instance that is paired either with a vCloud Networking and Security Manager or with a VMware NSX Manager. Payload clusters that require access to external networks are managed by the same vCenter Server instance.

This specialized cluster will likely be small and can be made up of less capable server systems when compared to the management and payload clusters.

Payload cluster

The payload cluster supports the delivery of all other (non-edge) consumer workloads. The cluster remains empty until a consumer of the environment begins to populate it with virtual machines. You can scale up by adding more payload clusters.

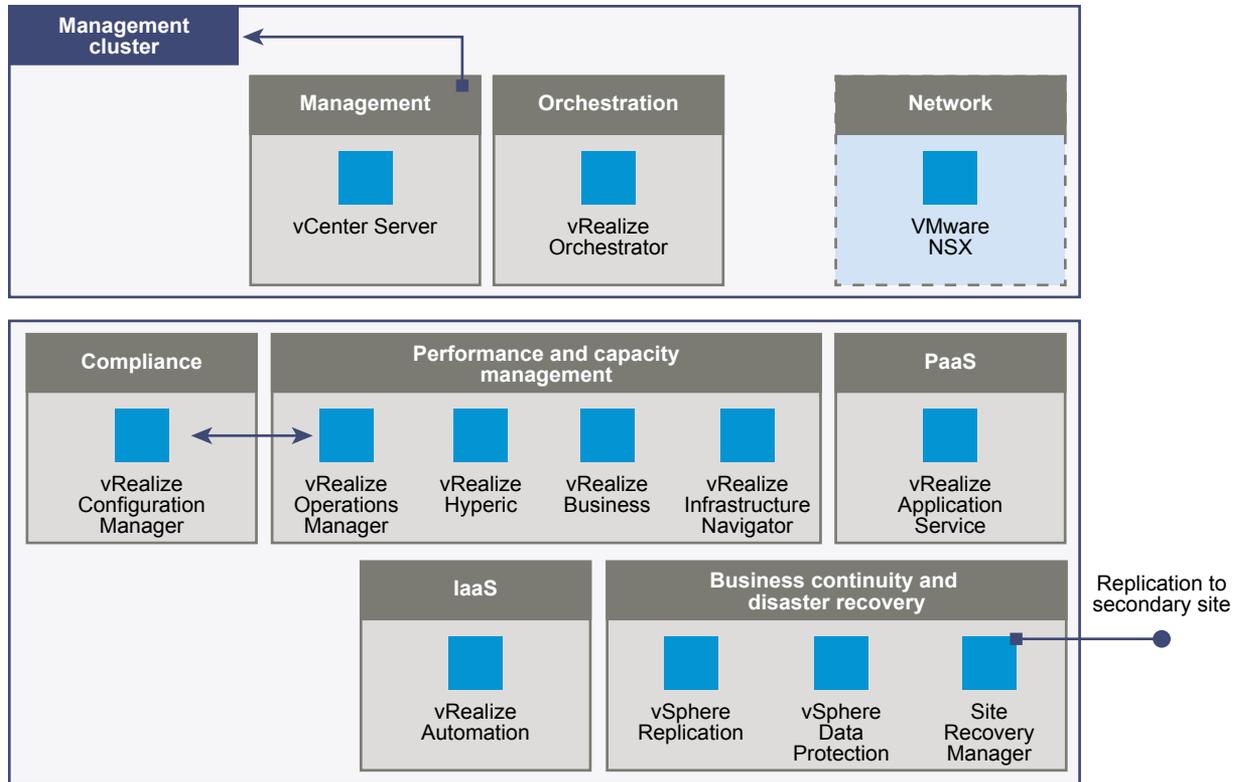
You can create new edge and payload clusters, scale up, or scale out, as the data center grows in size.

NOTE You can choose to combine the management and Edge clusters into a single entity. However, the model with three types of clusters provides the best and most secure basis for scaling your environment.

vCloud Suite Components in the Management Cluster

The number of vCloud Suite components in the management cluster increases as you add capabilities. A management cluster can contain a minimal set of products that you expand as needed.

Figure 2-3. VMware products in the management cluster



Minimal set of components

An example set of VMware products required for the management cluster always includes a vCenter Server instance. vRealize Orchestrator is a vCloud Suite component that you should deploy at early stage, in order to prepare the environment for IaaS and PaaS capabilities.

The above illustration shows NSX for vSphere fulfilling the networking functions of the vCloud Suite management cluster. vCloud Suite 6.0 does not include any VMware networking solutions, however, you can adopt NSX for vSphere for the networking and security needs of your Software Defined Data Center. vCloud Suite customers have the option to purchase NSX for vSphere at a reduced, add-on price. NSX provides layer 2 to layer 7 network virtualization, with security policies that follow workloads across the data center for faster network provisioning and management.

NOTE vCloud Networking and Security was included with the previous version of vCloud Suite, and performed the networking functions of the management cluster. While vCloud Networking and Security is no longer a part of vCloud Suite, it is available for customers upgrading from the previous release. See [“Upgrade vCloud Suite Components,”](#) on page 24.

Extended set of components

As the complexity of the environment increases, you install and configure additional products. vRealize Operations Manager and related products provide advanced monitoring features. vRealize Automation is the key element of your IaaS solution. A vCenter Site Recovery Manager instance provides replication to a secondary site.

Software-Defined Data Center Core Infrastructure

The core of vCloud Suite environments consists of vSphere and the associated monitoring and orchestration products, such as vRealize Operations Manager and vRealize Orchestrator.

The software-defined data center infrastructure layer includes the core virtualization, monitoring, and orchestration sub-layers. The infrastructure enables consolidation and pooling of physical resources, in addition to providing orchestration and monitoring capabilities, while reducing the costs associated with operating an on-premise data center.

Once the SDDC infrastructure is in place, you can extend it to provide Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings to consumers of IT resources inside or outside the organization. IaaS and PaaS complete the SDDC platform, and provide further opportunities for extending capabilities. With IaaS and PaaS, you increase the agility of IT and developer operations.

Figure 2-4. The stages of building the software-defined data center infrastructure



- [Virtualization and Management of vCloud Suite Infrastructure](#) on page 14
VMware products provide the virtualization and management capabilities required for the vCloud Suite foundation. You should consider the design choices that are available to you.
- [Monitoring vCloud Suite Core Infrastructure](#) on page 17
Monitoring is a required element of a software-defined data center. The monitoring element provides capabilities for performance and capacity management of related infrastructure components, including requirements, specifications, management, and their relationships.
- [Orchestration of vCloud Suite Core Infrastructure](#) on page 17
The software-defined data center requires orchestration capability. In vCloud Suite, you can use vRealize Orchestrator to orchestrate processes through workflows.

Virtualization and Management of vCloud Suite Infrastructure

VMware products provide the virtualization and management capabilities required for the vCloud Suite foundation. You should consider the design choices that are available to you.

Virtualization and management components are the core of the software-defined data center. For organizations of all sizes, they reduce costs and increase agility. Establishing a robust foundation for your datacenter requires you to install and configure vCenter Server and ESXi, as well as supporting components.

- [ESXi and vCenter Server Design Considerations](#) on page 15
Design decisions for the virtualization component of the software-defined data center must address the deployment and support specifics of ESXi and vCenter Server.

- [Network Design Considerations](#) on page 15
As virtualization and cloud computing become more popular in the data center, a shift in the traditional three-tier networking model is taking place. The traditional core-aggregate-access model is being replaced by the leaf and spine design.
- [Shared Storage Design Considerations](#) on page 16
A proper storage design provides the basis for a virtual data center that performs well.

ESXi and vCenter Server Design Considerations

Design decisions for the virtualization component of the software-defined data center must address the deployment and support specifics of ESXi and vCenter Server.

Consider the following design decisions when planning the deployment of ESXi hosts.

ESXi

- Use a tool such as VMware Capacity Planner to analyze the the performance and use of existing servers.
- Use supported server platforms that are listed in the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.
- Verify that your servers meet the minimum required system requirements for running ESXi.
- To eliminate variability and achieve a manageable and supportable infrastructure, standardize the physical configuration of the ESXi hosts.
- You can deploy ESXi hosts either manually, or by using an automated installation method such as VMware Auto Deploy. One valid approach is to deploy the management cluster manually, and implement Auto Deploy as your environment grows.

vCenter Server

- You can deploy vCenter Server as a Linux-based virtual appliance or on a 64-bit Windows physical or virtual machine.

NOTE vCenter Server on Windows scales up to support up to 10,000 powered-on virtual machines. The vCenter Server Virtual Appliance is an alternative choice that comes pre-configured and enables faster deployment method along with reduced operating system licensing costs. When using an external Oracle database, the vCenter Server Virtual Appliance can support a maximum of 10,000 virtual machines.

- Provide sufficient virtual system resources for vCenter Server.
- Deploy the vSphere Web Client and the vSphere Client for user interfaces to the environment. Deploy the VMware vSphere Command-Line Interface, VMware vSphere PowerCLI, or VMware vSphere Management Assistant for command-line and scripting management.

Network Design Considerations

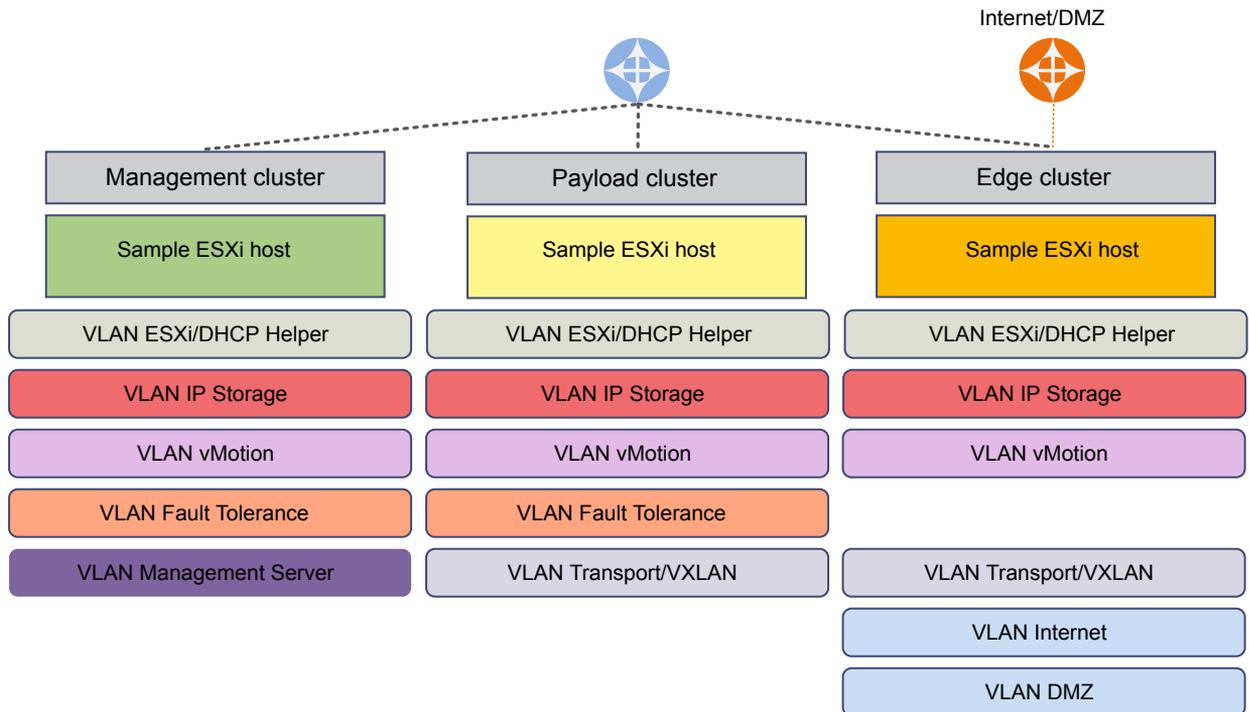
As virtualization and cloud computing become more popular in the data center, a shift in the traditional three-tier networking model is taking place. The traditional core-aggregate-access model is being replaced by the leaf and spine design.

- The network must be designed to meet the diverse needs of many different entities in an organization. These entities include applications, services, storage, administrators, and users.
- The network design should improve availability. Availability is typically achieved by providing network redundancy
- The network design should provide an acceptable level of security. Security can be achieved through controlled access where required and isolation where necessary.

- Simplify the network architecture by using a leaf and spine design.
- Configure common port group names across hosts to support virtual machine migration and failover.
- Separate the network for key services from one another to achieve greater security and better performance.

Network isolation is often recommended as a best practice in the data center. In a vCloud Suite environment, you might have several key VLANs, spanning two or more physical clusters.

Figure 2-5. Network isolation in the software-defined data center



ESXi/DHCP Helper The helper network is used for PXE booting ESXi images by using Auto Deploy.

IP Storage Network storage traffic over Ethernet should be isolated for performance and security reasons.

vMotion vMotion traffic is not encrypted by default. Isolate the vMotion traffic to increase security while migrating the state of virtual machines and the contents of virtual disks between hosts.

Fault Tolerance FT logging traffic should use a dedicated VLAN.

Management Server Management traffic between vCenter Server and ESXi hosts.

Shared Storage Design Considerations

A proper storage design provides the basis for a virtual data center that performs well.

- The storage design must be optimized to meet the diverse needs of applications, services, administrators, and users.
- Tiers of storage have different performance, capacity, and availability characteristics.
- Designing different storage tiers is cost efficient, given that not every application requires expensive, high-performance, highly available storage.

- Fibre Channel, NFS, and iSCSI are mature and viable options to support virtual machine needs.

Monitoring vCloud Suite Core Infrastructure

Monitoring is a required element of a software-defined data center. The monitoring element provides capabilities for performance and capacity management of related infrastructure components, including requirements, specifications, management, and their relationships.

VMware monitoring components include the following products.

Table 2-1. Monitoring products in vCloud Suite

| Monitoring component | Description |
|-----------------------------------|---|
| vRealize Operations Manager | Provides comprehensive visibility and insights into the performance, capacity and health of your infrastructure. |
| vRealize Infrastructure Navigator | Automatically discovers application services, visualizes relationships and maps dependencies of applications on virtualized compute, storage and network resources. |
| vRealize Hyperic | Monitors application health. |

A subset of the products can be deployed without damaging the integrity of the solution.

vRealize Operations Manager is distributed as virtual appliance that you can deploy on ESXi hosts. You need to configure the virtual appliance and register it with a vCenter Server system. For an in-depth discussion of vRealize Operations Manager and related products, see the [VMware vRealize Operations documentation](#).

Orchestration of vCloud Suite Core Infrastructure

The software-defined data center requires orchestration capability. In vCloud Suite, you can use vRealize Orchestrator to orchestrate processes through workflows.

The orchestration layer of the software-defined data center provides the ability to build macro-like workflows that automate manual processes and is instrumental when delivering repeatable operations. Traditionally, orchestration is implemented when the Infrastructure Service and Platform Application Service layers of the SDDC solution are being considered. Within the IaaS layer, vRealize Automation can trigger vRealize Orchestrator workflows automatically. Additionally, you can also publish workflows in your service catalog to trigger manually.

Establishing the orchestration engine early in the process benefits all levels of customer maturity and provides a foundation that the rest of the solution builds on. You should deploy at least one vCenter Server instance for each vCenter Server system in your environment depending on your scale requirements.

The main elements of the orchestration layer are:

- vRealize Orchestrator
- vRealize Orchestrator plug-ins

Figure 2-6. Design of the orchestration layer

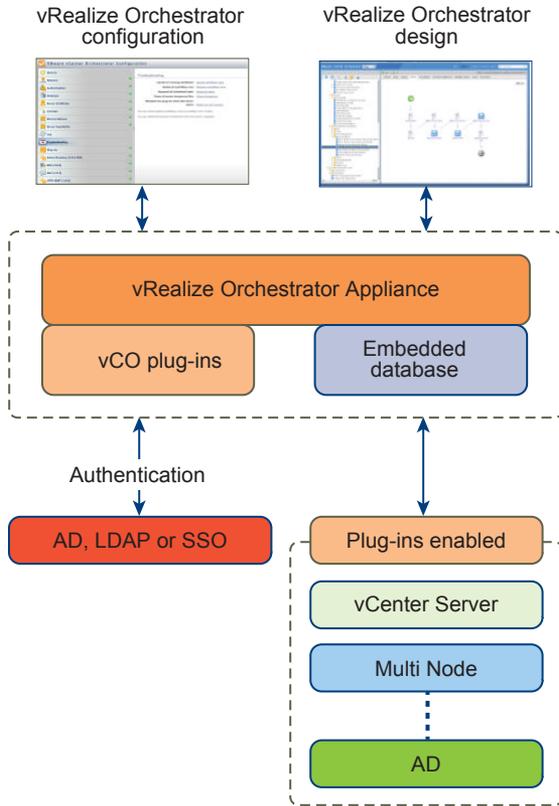


Table 2-2. Components of vCloud Suite orchestration

| Component | Description |
|---|--|
| vRealize Orchestrator Appliance | You can deploy vRealize Orchestrator as a virtual appliance. The vRealize Orchestrator Appliance, running in stand-alone mode (not HA) is the recommended approach for smaller deployments. |
| Authentication | Authentication can be provided by Active Directory or vCenter Single Sign-on. |
| vRealize Orchestrator configuration interface | The Web-based interface where you configure the appliance database, SSL certificate, license, and so on. |
| vRealize Orchestrator designer interface | The Web-based interface where your create and customize workflows. |
| vCenter Server plug-in | An Orchestrator plug-in that lets you manage multiple vCenter Server instances. The vCenter Server plug-in provides a library of standard workflows that automate vCenter Server operations. |
| Multi Node plug-in | An Orchestrator plug-in that provides remote vRealize Orchestrator management and remote workflow execution. |

Delivering an Infrastructure Service

The ability to deliver infrastructure as a service represents the technological and organizational transformation from traditional data center operations to cloud. The infrastructure service lets you model and provision VMs and services across private, public, or hybrid cloud infrastructure.

In the software-defined data center, provider groups or organizations can isolate and abstract resources in the form of infrastructure and application services, and make them available to tenant groups or organizations.

The Infrastructure Service layer delivers a self-service user portal that lowers administrative overhead through the use of policies to provision infrastructure services. Policies allow administrators to control the consumption of services in a granular and flexible fashion. The portal also provides robust approval capabilities.

You can build the infrastructure service core by using the following components:

Table 2-3. Infrastructure service components

| Infrastructure service section | Design components |
|---------------------------------------|---|
| vRealize Automation virtual appliance | <ul style="list-style-type: none"> ■ vCloud Automation Center Portal Web/App server ■ vCloud Automation Center vPostgreSQL database |
| vRealize Automation IaaS | <ul style="list-style-type: none"> ■ vRealize Automation IaaS Web server ■ vRealize Automation IaaS Manager services |
| Distributed execution | vRealize Automation distributed execution managers: <ul style="list-style-type: none"> ■ Orchestrator ■ Workers |
| Integration | vRealize Automation Agent machines |
| Cost management | vRealize Business for vSphere |
| Provisioning infrastructure | <ul style="list-style-type: none"> ■ vSphere environment ■ vRealize Orchestrator environment ■ Other supported physical, virtual, or cloud environment |
| Supporting infrastructure | <ul style="list-style-type: none"> ■ Microsoft SQL database environment ■ LDAP or Active Directory environment ■ SMTP and email environment |

The stages of deploying an infrastructure service are illustrated in the graphic below.

Figure 2-7. IaaS components



For an in-depth discussion of key IaaS concepts, see the [vCloud Automation Center documentation](#).

Self-service portal

vRealize Automation provides a secure portal where authorized administrators, developers or business users can request new IT services.

Infrastructure Components

vRealize Automation requires you to configure vSphere, vCloud Air, and physical machine endpoints, Fabric groups, and blueprints.

Services and Tenants

The service catalog provides a unified self-service portal for consuming IT services. Users can browse the catalog to request items they need, track their requests, and manage their provisioned items.

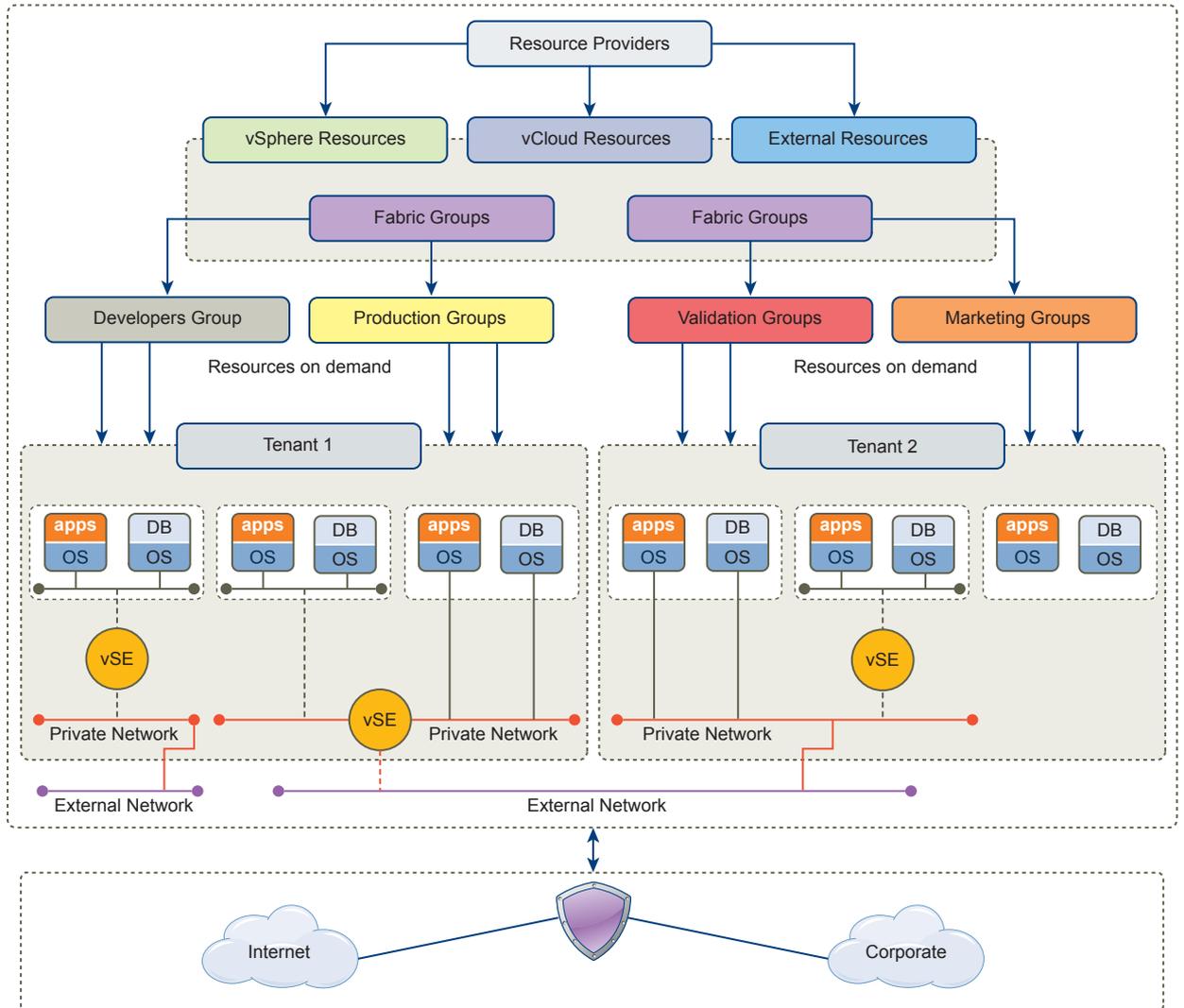
Cost Management

Understanding and controlling costs is an important SDDC feature. Cost management capability is solutions that integrate with vRealize Automation, such as vRealize Business for vSphere.

Design of an IaaS Environment

In a vCloud Suite environment that is configured to deliver infrastructure as a service, tenants have access to compute, network, and storage resources that have been preconfigured for them by the provider.

Figure 2-8. Diagram of an IaaS Environment



Resource providers

Providers are groups in the organization that configure and support the underlying virtual infrastructure.

Fabric Groups

Fabric groups organize virtualization compute resources and cloud endpoints by type and intent. An IaaS administrator also assigns one or more fabric administrators to manage the resources in the fabric group.

Business Groups

Create business groups to associate a set of services and resources to a set of users, often corresponding to a line of business, department, or other organizational unit. Users must belong to a business group to request machines.

Tenants Tenant can represent business units in a company that subscribe to cloud services from a service provider. Each tenant has its own dedicated configuration. Some system-level configuration is shared across tenants.

The networks in the example diagram are routed using vShield Edge instances, which in turn connect to internal and external networks.

Delivering Platform as a Service

Platform-as-a-Service (PaaS) lets you model and provision applications across private, public, and hybrid cloud infrastructures.

PaaS is a type of cloud computing service that provides a computing platform and a solution stack as a service. Along with Software-as-a-Service (SaaS) and Infrastructure-as-Service (IaaS), PaaS is a service model of cloud computing that lets you create an application (or service) using tools and libraries supplied by the provider. You control software deployment and configuration settings. The provider provides the networks, servers, storage, and other services required to host your application.

Automate Application Provisioning

A key aspect of PaaS is the ability to automate the provisioning of applications. VMware vRealize Automation is a model-based application provisioning solution that simplifies creating and standardizing application deployment topologies on cloud infrastructures. Application architects use the drag-and-drop interface to create application deployment topologies called application blueprints. These application blueprints define the structure of the application, enable the use of standardized application infrastructure components, and include installation dependencies and default configurations for custom and packaged enterprise applications. You can use the prepopulated and extensible catalog of standard logical templates, application infrastructure service, components, and scripts to model an application blueprint. These blueprints standardize the structure of the application, including software components, dependencies, and configurations, for repeated deployments. Application blueprints are logical deployment topologies that are portable across VMware-based IaaS clouds such as vRealize Automation, and across public clouds such as Amazon EC2.

Using vRealize Automation, you "declare" the application and service structure with the assumption that the underlying cloud infrastructure will deliver the necessary compute, network and storage requirements. Once built you can deploy the blueprints on any VMware vSphere-based private or public cloud, delivering on the cloud promise of choice. This application provisioning model frees developers and application administrators from dealing with infrastructure, OS, and middleware configuration issues, and allows you to focus on delivering business value with your applications.

Enterprise users can standardize, deploy, configure, update, and scale complex applications in dynamic cloud environments. These applications can range from simple Web applications to complex custom applications and packaged applications. With its catalog of standard components, or services, vRealize Automation Application Services automates and manages the update life cycle of deployments for multi-tier enterprise applications in hybrid cloud environments.

Monitor Application Performance

Monitoring provides capabilities for performance management related to applications.

Pre-built Application Components

VMware Cloud Management Marketplace provides blueprints, services, scripts and plugins that you can download and use to more rapidly develop your own application services. The pre-built components are provided by leading middleware, networking, security and application vendors using highly reusable and flexible configurations that you can insert into any multi-tier application-provisioning plan.

Deploying vCloud Suite

To leverage the capabilities of vCloud Suite, the components need to be installed separately with the required prerequisites and then configured to integrate with one another.

This document provides high-level design recommendations and deployment sequences. For installation instructions and in-depth discussions of individual vCloud Suite components, see the documentation for those products.

This chapter includes the following topics:

- [“Install vCloud Suite Components,”](#) on page 23
- [“Upgrade vCloud Suite Components,”](#) on page 24
- [“External Dependencies for Deploying vCloud Suite,”](#) on page 26
- [“System Requirements of vCloud Suite Components,”](#) on page 27
- [“Security Considerations,”](#) on page 27
- [“vCloud Suite Licensing,”](#) on page 34

Install vCloud Suite Components

Follow the recommended sequence of installation to build a stable and scalable vCloud Suite environment. The recommended installation sequence has been verified for a greenfield virtual environment.

NOTE If you want to use vRealize Operations Manager to monitor applications, you must install vRealize Infrastructure Navigator first.

You download and install vCloud Suite components separately. Depending on the type of environment that you are building, you might need to omit some components from the installation sequence.

Perform the operations according to the recommended sequence.

Prerequisites

Verify that you have system resources that are sufficient for the deployment of vCloud Suite components.

Verify that your environment meets the requirements for external dependencies. See [“External Dependencies for Deploying vCloud Suite,”](#) on page 26.

Verify that you have a valid vCloud Suite license. See [“vCloud Suite Licensing,”](#) on page 34.

Procedure

- 1 Install ESXi.
If you install vCenter Server on a physical machine, you can install vCenter Server first.
See [Installing ESXi](#).
- 2 Install Platform Services Controller and vCenter Server.
See [Installing vCenter Server](#).
- 3 Install vRealize Orchestrator.
See [Installing and Upgrading Orchestrator](#).
- 4 Install vRealize Configuration Manager.
See [Installing or Migrating vRealize Operations Manager](#).
- 5 Install vRealize Operations Manager.
See [Deployment and Configuration Guide](#).
- 6 Install vRealize Infrastructure Navigator.
See [Installation and Configuration Guide](#).
- 7 Install vRealize Hyperic.
See [vRealize Hyperic Installation and Configuration Guide](#).
- 8 Install vCenter Site Recovery Manager.
See [Installing SRM](#).
- 9 Install vSphere Replication.
See [Install vSphere Replication](#).
- 10 Install vSphere Data Protection.
See [Administration Guide](#).
- 11 Install vRealize Automation.
See [vRealize Automation Installation and Configuration](#).
- 12 Install vRealize Automation Application Services.
See [Install and Configure Application Services](#).
- 13 Install vSphere Big Data Extensions.
See [Installing Big Data Extensions](#).
- 14 Install vRealize Business for vSphere.
See [Installing vRealize Business](#).

Upgrade vCloud Suite Components

Upgrading vCloud Suite components to newer versions requires you to perform separate upgrade procedures. Follow the recommended upgrade order to ensure that vCloud Suite upgrades complete without problems.

You should perform the upgrade operations according to the recommended sequence.

Prerequisites

- Verify that you have the required installation or upgrade packages.

Before upgrading, review the VMware Product Interoperability Matrix for each product you plan to upgrade to ensure that you have supported, compatible product versions. See the [VMware Product Interoperability Matrix](#) Web site.

- Verify that you have administrator privileges for all systems.

Procedure

- 1 Uninstall the following components that are incompatible with the current version of vCloud Suite.

| Product | Uninstall documentation |
|---------------------------|--|
| vSphere Storage Appliance | Uninstall VSA Manager |
| vSphere App HA | Uninstalling vSphere App HA |
| vCenter Server Heartbeat | VMware vCenter Heartbeat Documentation |

- 2 If you use an external deployment of vCenter Single Sign-On, upgrade vCenter Single Sign-On to Platform Services Controller.

See [Upgrade vCenter Single Sign-On 5.5 for External Deployment](#)

If you use embedded vCenter Single Sign-On, it will be upgraded when you upgrade vCenter Server.

- 3 Upgrade vRealize Automation.

See [Upgrading to vRealize Automation 6.2](#).

- 4 Upgrade vRealize Automation Application Services.

See [Upgrading Application Services](#).

- 5 If you use IT Business Management in your environment as an additional product, upgrade IT Business Management to vRealize Business for vSphere.

See [Upgrading vRealize Business](#).

- 6 Upgrade vRealize Configuration Manager.

See [Installation Guide](#).

- 7 Upgrade vCloud Director.

See [Upgrading vCloud Director](#).

NOTE This product is no longer a part of vCloud Suite. It is only available for existing users who upgrade from an older version of vCloud Suite.

- 8 Upgrade vCloud Networking and Security.

See [vShield Installation and Upgrade Guide](#).

NOTE This product is no longer a part of vCloud Suite. It is only available for existing users who upgrade from an older version of vCloud Suite.

- 9 Upgrade vCenter Server.

See [Upgrading vCenter Server](#).

- 10 Upgrade vRealize Orchestrator.

[Installing and Upgrading Orchestrator](#).

- 11 Upgrade vSphere Replication.

See [Upgrading vSphere Replication](#).

- 12 Upgrade vCenter Site Recovery Manager.

See [Upgrading SRM](#).

- 13 Upgrade vSphere Data Protection.

See [Administration Guide](#).

- 14 Upgrade vRealize Operations Manager.

See [Migrating vRealize Operations Manager](#).

- 15 Upgrade vRealize Hyperic.

See [vCenter Hyperic Installation and Configuration](#).

- 16 Upgrade vRealize Infrastructure Navigator.

See [Installation and Configuration Guide](#).

- 17 Upgrade vSphere Big Data Extensions.

See [Upgrading Big Data Extensions](#).

- 18 Upgrade ESXi.

See [Upgrading Your Hosts](#).

You should upgrade VMware tools and virtual hardware version on your VMs after the ESXi upgrade.

You have upgraded vCloud Suite components.

External Dependencies for Deploying vCloud Suite

External dependencies address other systems or technologies that depend on or might be affected by the vCloud Suite infrastructure.

Table 3-1. External Dependencies in vCloud Suite

| Component | Description |
|--|--|
| Identity source (Active Directory, OpenLDAP or Local OS) | Identity sources (Active Directory, OpenLDAP or Local OS) or similar is required to implement and operate the vCloud Suite infrastructure. |
| DNS | DNS must be configured for connectivity between vCenter Server, Active Directory, ESXi hosts, and virtual machines. |
| DHCP/TFTP | PXE boot is required for vSphere Auto Deploy functionality. |
| 64-bit Windows OS | Some vCloud Suite components can be installed on Windows Server 2008 and later. |
| Microsoft SQL or Oracle database | vCloud Suite components can work with embedded or external databases, depending on the product and your environment. |
| Network infrastructure | Network infrastructure with 1Gbps or 10Gbps bandwidth. Depending on the needs of your environment, higher throughput is recommended. |
| Shared Storage Array | Stability and performance of the shared storage array affects the virtual machines. |

Table 3-1. External Dependencies in vCloud Suite (Continued)

| Component | Description |
|-------------------------|---|
| Time synchronization | Accurate time keeping and time synchronization is critical for a healthy vSphere infrastructure. All components, including ESXi hosts, vCenter Server, the SAN, physical network infrastructure, and virtual machine guest operating systems must have accurate time keeping. This is especially critical for virtual machines protected by FT. |
| Staff | Properly trained IT staff is critical for the correct implementation, operation, support, and enhancement of your environment. |
| Policies and procedures | The policies and procedures governing the use of information technology must be revised to properly incorporate the unique properties and capabilities of virtualization and cloud operations. |

System Requirements of vCloud Suite Components

The software and hardware requirement for vCloud Suite depend on the set of components that you have deployed. Information for each product or feature is available in the individual product documentation sets.

Documentation resources

Table 3-2. List of system requirements documentation for vCloud Suite 6.0 components

| Product | System requirements documentation |
|--|--|
| ESXi | ESXi Requirements |
| vCenter Server | System Requirements |
| vRealize Infrastructure Navigator | Installing vCenter Infrastructure Navigator |
| vCenter Site Recovery Manager | SRM System Requirements |
| vRealize Automation | Preparing for Installation |
| vRealize Automation Application Services | System Requirements |
| vRealize Business for vSphere | vRealize Business System Requirements |
| vRealize Configuration Manager | Installation Guide |
| vRealize Hyperic | Supported Configurations and System Requirements |
| vRealize Operations Manager | Preparing for Installation |
| vRealize Orchestrator | Orchestrator System Requirements |
| vSphere Big Data Extensions | System Requirements for Big Data Extensions |
| vSphere Data Protection | vSphere Data Protection Administration Guide |
| vSphere Replication | vSphere Replication System Requirements |

Security Considerations

The vSphere platform is an inherently secure environment from a technical standpoint, with a minimal hypervisor footprint, APIs for monitoring that eliminate the need for third-party software on the host, secure syslog activity, Active Directory integration, and more. There are however several guidelines for securing a vSphere implementation. See the vSphere hardening guide for detailed configurations.

For a detailed discussion of security considerations for the SDDC core layer, see *vSphere Security*.

- [Security and Virtual Machines](#) on page 28
Virtual machines are the logical containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and provides both their ability to access hardware and their uninterrupted performance.
- [Security and Virtual Networks](#) on page 30
If an ESXi host is accessed through vCenter Server, it is typical to protect vCenter Server using a firewall. This firewall provides basic protection for the network.
- [Securing Standard Switch Ports](#) on page 30
As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine or impersonate another machine so that it can receive network frames intended for that machine. Also, like physical network adapters, a virtual network adapter can be configured so that it receives frames targeted for other machines.
- [Securing iSCSI Storage](#) on page 31
The storage configured for a host might include one or more storage area networks (SANs) that use iSCSI. When iSCSI is configured on a host, several measures can be taken to minimize security risks.
- [Securing ESXi Management Interfaces](#) on page 32
Security of the ESXi management interface is critical to protect against unauthorized intrusion and misuse. If a host is compromised in certain ways, the virtual machines it interacts with might also be compromised. To minimize the risk of an attack through the management interface, ESXi is protected with a built-in firewall.
- [Securing vCenter Server Systems](#) on page 33
Securing vCenter Server includes ensuring security of the host where vCenter Server is running, following best practices for assigning privileges and roles, and verifying the integrity of the clients that connect to vCenter Server.
- [Encryption and Security Certificates](#) on page 33
ESXi and vCenter Server support standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components. If SSL is enabled, data is private, protected, and cannot be modified in transit without detection.
- [vCenter Single Sign-On](#) on page 33
vCenter Single Sign-On is a component of the management infrastructure that provides the capability to manage the environment with external identity sources, such as Active Directory or OpenLDAP.

Security and Virtual Machines

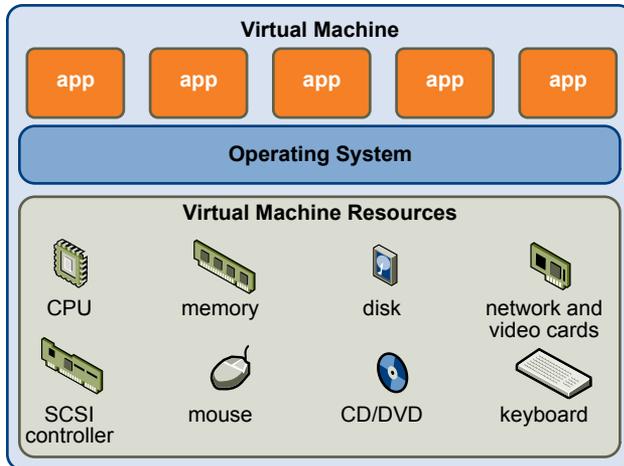
Virtual machines are the logical containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and provides both their ability to access hardware and their uninterrupted performance.

Even a user with system administrator privileges on a virtual machine's guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESXi system administrator. As a result of virtual machine isolation, if a guest operating system running in a virtual machine fails, other virtual machines on the same host continue to run. The guest operating system failure has no effect on:

- The ability of users to access the other virtual machines.
- The ability of the operational virtual machines to access the resources they need.
- The performance of the other virtual machines.

Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it.

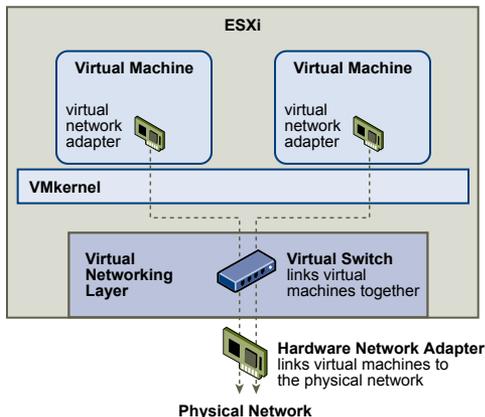
Figure 3-1. Virtual Machine Isolation



Because the VMkernel mediates the physical resources and all physical hardware access takes place through the VMkernel, virtual machines cannot circumvent this level of isolation.

Just as a physical machine communicates with other machines in a network through a network card, a virtual machine communicates with other virtual machines running in the same host through a virtual switch. Further, a virtual machine communicates with the physical network, including virtual machines on other ESXi hosts, through a physical network adapter.

Figure 3-2. Virtual Networking Through Virtual Switches



These characteristics apply to virtual machine isolation in a network context:

- If a virtual machine does not share a virtual switch with any other virtual machine, it is completely isolated from virtual machines within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated. This includes isolation from any physical or virtual networks.
- If the same safeguards are used (firewalls, antivirus software, and so forth) to protect a virtual machine from the network as if it were a physical machine, the virtual machine is as secure as the physical machine.

Virtual machines can be further protected by setting up resource reservations and limits on the host. For example, through the detailed resource controls available in ESXi, a virtual machine can be configured so that it always receives at least 10 percent of the host's CPU resources, but never more than 20 percent.

Resource reservations and limits protect virtual machines from performance degradation that would result if another virtual machine consumed excessive shared hardware resources. For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack, a resource limit on that machine prevents the attack from taking up so much of the hardware resources that the other virtual machines are also affected. Similarly, a resource reservation on each of the virtual machines provides that, in the event of high resource demands by the virtual machine targeted by the DoS attack, all the other virtual machines still have enough resources to operate.

By default, ESXi imposes a form of resource reservation by applying a distribution algorithm that divides the available host resources equally among the virtual machines while keeping a certain percentage of resources for use by other system components. This default behavior provides a degree of natural protection from DoS and distributed denial-of-service (DDoS) attacks. Specific resource reservations and limits are set on an individual basis to customize the default behavior so that the distribution is not equal across the virtual machine configuration.

Security and Virtual Networks

If an ESXi host is accessed through vCenter Server, it is typical to protect vCenter Server using a firewall. This firewall provides basic protection for the network.

A firewall might lie between the clients and vCenter Server. Alternatively, vCenter Server and the clients can be behind the firewall, depending on deployment. The main point is to provide a firewall at what is considered to be an entry point for the system.

Networks configured with vCenter Server can receive communications through the vSphere Client or third-party network management clients that use the SDK to interface with the host. During normal operation, vCenter Server listens for data from its managed hosts and clients on designated ports. vCenter Server also assumes that its managed hosts listen for data from vCenter Server on designated ports. If a firewall is present between any of these elements, it needs to be confirmed that the firewall has open ports to support data transfer.

Firewalls might also be included at a variety of other access points in the network, depending on how the network is planned to be used and the level of security various devices require. Select the locations for firewalls based on the security risks that have been identified for network configuration. The following is a list of firewall locations common to ESXi implementations.

Securing Standard Switch Ports

As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine or impersonate another machine so that it can receive network frames intended for that machine. Also, like physical network adapters, a virtual network adapter can be configured so that it receives frames targeted for other machines.

When a standard switch is created, port groups are added to impose a policy configuration for the virtual machines and storage systems attached to the switch. Virtual ports are created through the vSphere Web Client or the vSphere Client.

As part of adding a port or standard port group to a standard switch, the vSphere Client configures a security profile for the port. This security profile can be used so that the host prevents the guest operating systems for its virtual machines from impersonating other machines on the network. This security feature is implemented so that the guest operating system responsible for the impersonation does not detect that the impersonation was prevented.

The security profile determines how strongly the protection is enforced against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profile, one must understand the basics of how virtual network adapters control transmissions and how attacks are staged at this level.

Each virtual network adapter has its own MAC address assigned when the adapter is created. This address is called the initial MAC address. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system. In addition, each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. The guest operating system is responsible for setting the effective MAC address and typically matches the effective MAC address to the initial MAC address.

When sending packets, an operating system typically places its own network adapter's effective MAC address in the source MAC address field of the Ethernet frame. It also places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only when the destination MAC address in the packet matches its own effective MAC address.

Upon creation, a network adapter's effective MAC address and initial MAC address are the same. The virtual machine's operating system can alter the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter receives network traffic destined for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. This means an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter that the receiving network authorizes.

Standard switch security profiles can be used on hosts to protect against this type of attack by setting three options. If any default settings for a port are changed, the security profile must be modified by editing standard switch settings in the vSphere Client.

Securing iSCSI Storage

The storage configured for a host might include one or more storage area networks (SANs) that use iSCSI. When iSCSI is configured on a host, several measures can be taken to minimize security risks.

The storage configured for a host might include one or more storage area networks (SANs) that use iSCSI. When iSCSI is configured on a host, several measures can be taken to minimize security risks.

iSCSI is a means of accessing SCSI devices and exchanging data records by using TCP/IP over a network port rather than through a direct connection to a SCSI device. In iSCSI transactions, blocks of raw SCSI data are encapsulated in iSCSI records and transmitted to the requesting device or user.

One means of securing iSCSI devices from unwanted intrusion is to require that the host, or initiator, be authenticated by the iSCSI device, or target, whenever the host attempts to access data on the target LUN. The goal of authentication is to prove that the initiator has the right to access a target, a right granted when authentication is configured. ESXi does not support Kerberos, Secure Remote Protocol (SRP), or public-key authentication methods for iSCSI. Additionally, it does not support IPsec authentication and encryption. Use the vSphere Client or the vSphere Web Client to determine whether authentication is being performed and to configure the authentication method.

iSCSI SANs enable the efficient use of existing Ethernet infrastructures to provide hosts access to storage resources that they can dynamically share. iSCSI SANs provide an economical storage solution for environments that rely on a common storage pool to serve numerous users. As with any networked system, iSCSI SANs can be subject to security breaches.

Securing ESXi Management Interfaces

Security of the ESXi management interface is critical to protect against unauthorized intrusion and misuse. If a host is compromised in certain ways, the virtual machines it interacts with might also be compromised. To minimize the risk of an attack through the management interface, ESXi is protected with a built-in firewall.

To protect the host against unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities. Constraints can be relaxed to meet configuration needs, but if done so, measures have to be taken to protect the network as a whole and the devices connected to the host.

Consider the following recommendations when evaluating host security and administration.

- To improve security, restrict user access to the management interface and enforce access security policies like setting up password restrictions.
- The ESXi Shell has privileged access to certain parts of the host. Therefore, provide only trusted users with ESXi Shell login access.
- When possible, run only the essential processes, services, and agents such as virus checkers, and virtual machine backups.
- When possible, use the vSphere Web Client or a third-party network management tool to administer ESXi Server hosts instead of working through the command-line interface as the root user. The usage of the vSphere Client enables limitations to the accounts with access to the ESXi Shell and one can safely delegate responsibilities and set up roles that prevent administrators and users from using capabilities they do not need.

The host runs a variety of third-party packages to support management interfaces or tasks that an operator must perform. VMware does not support upgrading these packages from anything other than a VMware source. If a download or patch is used from another source, management interface security or functions might be compromised. Regularly check third-party vendor sites and the VMware knowledge base for security alerts.

In addition to implementing the firewall, risks to the hosts are mitigated using other methods.

- By default, all ports not specifically required for management access to the host are closed. Ports must be specifically opened if additional services are required.
- By default, weak ciphers are disabled and all communications from clients are secured by SSL. The exact algorithms used for securing the channel depend on the SSL handshake. Default certificates created on ESXi use SHA-1 with RSA encryption as the signature algorithm.
- VMware monitors all security alerts that could affect ESXi security and, if needed, issues a security patch.
- Insecure services such as FTP and Telnet are not installed, and the ports for these services are closed by default. Because more secure services such as SSH and SFTP are easily available, always avoid using these insecure services in favor of their safer alternatives. If insecure services must be used sufficient protection for the host must be implemented, specific ports must be opened to support these services.

To increase the security of the ESXi Server hosts, they can be put in lockdown mode. When lockdown mode is enabled, no users other than vpxuser have authentication permissions, nor can they perform operations against the host directly. Lockdown mode forces all operations to be performed through vCenter Server. When a host is in lockdown mode, vSphere CLI commands cannot be executed from an administration server, from a script, or from VMware vSphere Management Assistant against the host. External software or management tools might not be able to retrieve or modify information from the ESXi host.

Securing vCenter Server Systems

Securing vCenter Server includes ensuring security of the host where vCenter Server is running, following best practices for assigning privileges and roles, and verifying the integrity of the clients that connect to vCenter Server.

Strictly control vCenter Server administrator privileges to increase security for the system, as follows:

- Full administrative rights to vCenter Server should be removed from the local Windows administrator account and granted to a special-purpose local vCenter Server administrator account. Grant full vSphere administrative rights only to those administrators who are required to have it. Do not grant this privilege to any group whose membership is not strictly controlled.
- Avoid allowing users to log in directly to the vCenter Server system. Allow only those users who have legitimate tasks to perform to log into the system and confirm that these events are audited.
- Install vCenter Server using a service account instead of a Windows account. A service account or a Windows account can be used to run vCenter Server. Using a service account allows to enable Windows authentication for SQL Server, which provides more security. The service account must be an administrator on the local machine.
- Check for privilege reassignment when restarting vCenter Server. If the user or user group that is assigned the Administrator role on the root folder of the server cannot be verified as a valid user or group, the Administrator privileges are removed and assigned to the local Windows Administrators group.

Grant minimal privileges to the vCenter Server database user. The database user requires only certain privileges specific to database access. In addition, some privileges are required only for installation and upgrade. These can be removed after the product is installed or upgraded.

Encryption and Security Certificates

ESXi and vCenter Server support standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components. If SSL is enabled, data is private, protected, and cannot be modified in transit without detection.

Certificate checking is enabled by default and SSL certificates are used to encrypt network traffic. However, ESXi and vCenter Server use automatically generated certificates that are created as part of the installation process and stored on the server system. These certificates are unique and make it possible to begin using the server, but they are not verifiable and are not signed by a trusted, well-known certificate authority (CA). These default certificates are vulnerable to possible man-in-the-middle attacks. To receive the full benefit of certificate checking, particularly if encrypted remote connections are to be used externally, install new certificates that are signed by a valid internal certificate authority or acquire a certificate from a trusted security authority.

The SSL Certificate Automation Tool is a command-line utility that automates the Self- or CA-signed certificate renewal process for vSphere 5.5. See VMware KB 2057340.

vCenter Single Sign-On

vCenter Single Sign-On is a component of the management infrastructure that provides the capability to manage the environment with external identity sources, such as Active Directory or OpenLDAP.

Starting with vSphere 6.0, vCenter Single Sign-On is part of the Platform Services Controller. The Platform Services Controller contains the shared services that support vCenter Server and vCenter Server components. These services include vCenter Single Sign-On, VMware Certificate Authority, License Service, and Lookup Service. See [vSphere Installation and Setup](#) for details on the vCenter Server.

vCenter Single Sign-On is an authentication broker and security token exchange infrastructure. When a user or a solution user authenticates to vCenter Single Sign-On, that user receives SAML token. Going forward, the user can use the SAML token to authenticate to vCenter Server services. The user can then perform the actions that user has privileges for.

vCenter Single Sign-On authentication service provides secure authentication services to the vSphere software components. By using vCenter Single Sign-On, the vSphere components communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. vCenter Single Sign-On constructs an internal security domain (for example, vsphere.local) where the vSphere solutions and components are registered during the installation or upgrade process, providing an infrastructure resource. vCenter Single Sign-On can authenticate users from its own internal users and groups, or it can connect to trusted external directory services such as Microsoft Active Directory. Authenticated users can then be assigned registered solution-based permissions or roles within a vSphere environment.

Platform Services Controller provides several different deployment methods that include vCenter Single Sign-On to best suit your environment.

| | |
|--|--|
| Basic deployment | A single standalone instance of Platform Services Controller supports the connectivity of identity sources and is installed on the same host as vCenter Server. This type of deployment meets the requirements of most users. |
| Multiple instances in the same location | Multiple Platform Services Controller nodes are installed at a local site and configured for high availability. In vSphere 6.0, Platform Services Controller has its own Directory Service that automatically replicates information to other Platform Services Controller nodes in the environment. |
| Multiple instances in different locations | Platform Services Controller nodes are installed at geographically separate sites. Each site has one or more Platform Services Controller installations and data is replicated between sites. Multi-site deployment is required if configuring Linked Mode vCenter Server instances across sites. |

vCloud Suite Licensing

The components of a vCloud Suite edition are activated by using a single licence. You can perform the activation of all components by using the vSphere Web Client or the licensing interfaces of individual products.

vCloud Suite Licensing Model

VMware vCloud Suite 6.0 combines multiple components into a single product to cover the complete set of cloud infrastructure capabilities. When used together, the vCloud Suite components provide virtualization, software-defined data center services, policy-based provisioning, disaster recovery, application management, and operations management.

A vCloud Suite 6.0 edition combines components such as vSphere Enterprise Plus, vRealize Automation, vRealize Orchestrator, and others, under a single license. vCloud Suite editions are licensed on a per-processor basis. Many of the vCloud Suite components are also available as standalone products licensed on a per-virtual machine basis. However, when these components are obtained through the vCloud Suite, they are licensed on a per-processor basis.

The components from a vCloud Suite edition are activated with a single license key. For example, if you have a license key for vCloud Suite 6.0 Standard, you can use the same key to activate vSphere Enterprise Plus, vRealize Automation, vRealize Orchestrator, and so on.

All virtual machines running on a processor licensed with a vCloud Suite edition can use all components included in that vCloud Suite edition. To run virtual machines on processors that are not licensed for vCloud Suite, you need individual licenses for the products that you want to use.

vCloud Suite Licenseable Components

The different vCloud Suite 6.0 editions include different sets of components. You must assign the vCloud Suite license to all components in your vCloud Suite edition.

The following vCloud Suite components correspond to vCloud Suite 6.0 Enterprise edition.

Table 3-3. vCloud Suite 6.0 components that require a license

| Components | Description |
|--|--|
| vSphere | Provides virtualization technology to serve as the platform for cloud infrastructure. |
| vCenter Site Recovery Manager | Provides business continuity and disaster recovery capabilities that help you plan, test, and perform recovery of virtual machines between one site (the protected site) and another site (the recovery site). |
| vRealize Automation | Provides functionality for deploying and provisioning of business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers. |
| vRealize Automation Application Services | Automates application provisioning in the cloud including deploying and configuring the application's components and dependent middleware platform services on infrastructure clouds. |
| vRealize Business for vSphere | Provides transparency and control over the costs and quality of IT services that is critical for private or hybrid cloud success. |
| vRealize Configuration Manager | Provides automation of configuration and compliance management across your virtual, physical and cloud environments, assessing them for operational and security compliance. |
| vRealize Hyperic | Provides monitoring of operating systems, middleware and applications running in physical, virtual, and cloud environments. |
| vRealize Infrastructure Navigator | Automates operations management and provides integrated performance, capacity, and configuration management for virtualized and cloud infrastructure. |
| vRealize Operations Manager | Provides comprehensive visibility and insights into the performance, capacity and health of your infrastructure. |

Licenses for vCloud Suite 5.8 Components

vCloud Suite 5.8 included vCloud Director and vCloud Networking and Security. These components have been removed from vCloud Suite 6.0. However, customers with an existing vCloud Suite 5.8 license are entitled to upgrade to these components.

Distributing the Processor Capacity of a vCloud Suite License

Each vCloud Suite license has a certain processor capacity that you can use to license multiple physical processors on ESXi hosts where you run the vCloud Suite components. When you assign a vCloud Suite license key to a host, the amount of processor capacity that is consumed is equal to the number of physical processors on the host.

To license physical processors that run vCloud Suite components, you need to assign the ESXi hosts a vCloud Suite license key with processor capacity that is sufficient to license all physical processors on the host.

For example, to run vCloud Suite on two ESXi 6.0 hosts that have four processors each, you need to assign the hosts a vCloud Suite license key with a minimum capacity of eight processors.

You can assign and reassign the processor capacity of a vCloud Suite license key to any combination of ESXi hosts. For example, suppose that you purchase a vCloud Suite license key for 10 processors. You can assign the license key to any of the following combinations of hosts.

- Five 2-processor hosts.
- Three 2-processor hosts and one 4-processor host.
- Two 4-processor hosts and one 2-processor host.
- One 8-processor host and one 2-processor host.

Dual-core and quad-core processors, such as Intel processors that combine two or four independent processors on a single chip, count as one processor.

Activating vCloud Suite Components in the vSphere Web Client

You must assign the vCloud Suite license key to all suite components. For components that integrate with the vSphere Web Client, you can use the license management option in the client.

Add the vCloud Suite License in the vSphere Web Client

To assign the vCloud Suite license key to the suite components, you must add the key to the license inventory of vCenter Server.

Prerequisites

Required privilege: **Global.Licenses**

Procedure

- 1 From the vSphere Web Client navigator home, select **Administration**, and under **Licensing** select **Licenses**.
- 2 On the **License Keys** tab, click **Add License Keys**.
- 3 Type the vCloud Suite license key and click **Next**.

You can copy and paste the license key from My VMware.

- 4 Click **Finish**.

What to do next

Assign the vCloud Suite license key to the suite components that integrate with the vSphere Web Client.

Assign the vCloud Suite License to vSphere in the vSphere Web Client

You must assign the vCloud Suite license key to the ESXi hosts that run the vCloud Suite components. You can assign the license key by using the license management option in the vSphere Web Client.

Prerequisites

- Verify that the vCloud Suite license key is added in the inventory of vCenter Server. See [“Add the vCloud Suite License in the vSphere Web Client,”](#) on page 36
- Required privilege: **Global.Licenses**

Procedure

- 1 From the vSphere Web Client navigator home, select **Administration**, and under **Licensing** select **Licenses**.
- 2 On the **Hosts** tab, select the ESXi hosts that run the vCloud Suite components and click **Assign License Key**.
To select multiple hosts, use Shift+click.
- 3 Select the vCloud Suite license key and click **OK**.

The ESXi hosts are licensed for vCloud Suite.

Activating vCloud Suite Components in the vSphere Client

You must assign the vCloud Suite license to all suite components to unlock the vCloud Suite capabilities. For components that integrate with the vSphere Client, you can use the license management option in the client.

NOTE The vCloud Suite 6.0 license is compatible with vCenter Server 5.1, 5.5, and 6.0.

Add the vCloud Suite License by Using the vSphere Client

To assign the vCloud Suite license key to the suite components, you must add the key to the license inventory of vCenter Server.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.

Procedure

- 1 In the vSphere Client, select **Home > Administration > Licensing**.
- 2 Select **Manage vSphere Licenses**.
- 3 In the Add License Keys page, type or paste the vCloud Suite license key, and type an optional label for the key.
- 4 Click **Add License Keys**.
- 5 Review the details for the license key, click **Next** on the remaining pages of the wizard, and click **Finish**.

The vCloud Suite license key is added to the license inventory of vCenter Server.

What to do next

Assign the vCloud Suite license key to vSphere, vCenter Operations Management Suite, vCenter Site Recovery Manager, and vCloud Networking and Security.

Assign the vCloud Suite License to vSphere in the vSphere Client

You must assign the vCloud Suite license key to the ESXi hosts that run the components of vCloud Suite.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.
- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, select **Home > Administration > Licensing**.
- 2 Select **Manage vSphere Licenses**.
- 3 Click **Next**.
- 4 On the Assign Licenses page, select **ESX**.
- 5 Select the ESXi hosts that run the vCloud Suite components.
- 6 From the Product pane, select the vCloud Suite license key.
- 7 On the Remove License Keys page, click **Next**.
- 8 Click **Finish** to save your changes.

Assign the vCloud Suite License to vRealize Infrastructure Navigator in the vSphere Client

Assign the vCloud Suite license key to vRealize Infrastructure Navigator to use it as part of vCloud Suite.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.
- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, select **Home > Administration > Licensing**.
- 2 Select **Manage vSphere Licenses**.
- 3 Click **Next**.
- 4 On the Assign Licenses page, select **Solutions**.
- 5 Select vRealize Infrastructure Navigator.
- 6 From the Product pane, select the vCloud Suite license key.
- 7 On the Remove License Keys page, click **Next**.
- 8 Click **Finish** to save your changes.

Assign the vCloud Suite License to vCloud Networking and Security in the vSphere Client

Assign the vCloud Suite license key to vCloud Networking and Security to use it as part of the suite.

vCloud Suite 5.8 included vCloud Networking and Security, which has been removed from vCloud Suite 6.0. However, customers with an existing vCloud Suite 5.8 license who are upgrading to vCloud Suite 6.0 are entitled to use vCloud Networking and Security.

NOTE New licenses for vCloud Suite 6.0 are not entitled to enable vCloud Networking and Security functionality using your license key.

NOTE vCloud Networking and Security components appear under vShield in the vSphere Client.

Prerequisites

- You must be a vCloud Suite 5.8 license in order to enable vCloud Networking and Security functionality using your vCloud Suite 6.0 license key.
- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.
- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, select **Home > Administration > Licensing**.
- 2 Select **Manage vSphere Licenses**.
- 3 Click **Next**.
- 4 On the Assign Licenses page, select **Solutions**.
- 5 Select vCloud Networking and Security (vShield) .
- 6 From the Product pane, select the vCloud Suite license key.
- 7 On the Remove License Keys page, click **Next**.
- 8 Click **Finish** to save your changes.

Assign the vCloud Suite License Key to vCenter Site Recovery Manager

Assign the vCloud Suite license key to vCenter Site Recovery Manager to use it as part of the suite.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.
- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, select **Home > Administration > Licensing**.
- 2 Select **Manage vSphere Licenses**.
- 3 Click **Next**.

- 4 On the Assign Licenses page, select **Solutions**.
- 5 Select vCenter Site Recovery Manager.
- 6 From the Product pane, select the vCloud Suite license key.
- 7 On the Remove License Keys page, click **Next**.
- 8 Click **Finish** to save your changes.

Activating vCloud Suite Components by Using Their Own Licensing Interfaces

You must assign the vCloud Suite license to all suite components. vCloud Director, vRealize Automation, and vRealize Automation Application Services provide their own licensing interfaces for license assignments.

NOTE The vCloud Suite 6.0 license is compatible with vCenter Server 5.1, 5.5, and 6.0.

Assigning the vCloud Suite License to vRealize Automation Application Services

You can assign the vCloud Suite license key to vRealize Automation Application Services to enable full functionality.

If vRealize Automation Application Services is already installed using another license key (such as an individual product license), reinstall the product and assign it the vCloud Suite license key.

The license key unlocks the vRealize Automation Application Services for Release Automation edition, which includes the basic features, updating a deployed application, and deploying applications to the Amazon EC2 environment capabilities.

To learn more about installing vRealize Automation Application Services and assigning license keys, see [Install and Configure Application Services](#).

Assign the vCloud Suite License to vCloud Director

To use vCloud Director as part of the vCloud Suite, you must assign vCloud Director the vCloud Suite license key.

vCloud Suite 5.8 included vCloud Director, which has been removed from vCloud Suite 6.0. Customers with an existing vCloud Suite 5.8 license who are upgrading to vCloud Suite 6.0 are entitled to use vCloud Director with your license key.

NOTE New licenses for vCloud Suite 6.0 are not entitled to enable vCloud Director functionality using your license key.

You can assign the vCloud Suite license key to vCloud Director while installing the component, or you can assign the license key to an already running instance of vCloud Director.

Prerequisites

- You must be avCloud Suite 5.8 license in order to enable vCloud Director functionality using your vCloud Suite 6.0 license key.
- You must be logged in to vCloud Director as an administrator.

Procedure

- 1 On the home page of the vCloud Director Web console, select **Administration**.
- 2 Under System Settings, select **License**.
- 3 In the **Serial number** text box, type or copy and paste the vCloud Suite license key.
- 4 Click **Apply**.

vCloud Director is licensed for vCloud Suite. The Licensed VM count field does not display any number of virtual machines, as vCloud Suite license is per-processor.

Assign the vCloud Suite License to vRealize Automation

To use vRealize Automation 6.2.1 as part of vCloud Suite, you must assign it the vCloud Suite license.

To enable the full functionality of vRealize Automation, you must assign the license in both the vCloud Automation Center Appliance and in Infrastructure as a Service.

Procedure

- 1 [Assign the License Key in the vCloud Automation Center Appliance](#) on page 41
You must assign the license key in the vCloud Automation Center Appliance to activate the product.
- 2 [Assign the License Key for Infrastructure as a Service](#) on page 41
You must assign the license key for Infrastructure as a Service to enable IaaS capabilities. Without a license, you cannot configure infrastructure endpoints or other features.

Assign the License Key in the vCloud Automation Center Appliance

You must assign the license key in the vCloud Automation Center Appliance to activate the product.

Procedure

- 1 Navigate to the vCloud Automation Center Appliance management console by using its fully qualified domain name (<https://vcac-va-hostname.domain.name:5480/>).
- 2 Log in with user name **root** and the password you specified when deploying the vCloud Automation Center Appliance.
- 3 Select **vRA Settings > Licensing**.
- 4 In the **New License Key** text box, type or copy and paste the vCloud Suite license key.
- 5 Click **Submit Key**.

Assign the License Key for Infrastructure as a Service

You must assign the license key for Infrastructure as a Service to enable IaaS capabilities. Without a license, you cannot configure infrastructure endpoints or other features.

Prerequisites

You must assign the license key in the vCloud Automation Center Appliance before you can access the Infrastructure-as-a-Service administration console. See [“Assign the License Key in the vCloud Automation Center Appliance,”](#) on page 41.

Procedure

- 1 Log in to the vRealize Automation console as an IaaS administrator.
- 2 Select **Infrastructure > Administration > Licensing**.
- 3 Click **Add License**.
The Add License dialog box appears.
- 4 In the **License key** text box, type or copy and paste the vCloud Suite license key.
- 5 Click **OK**.

- 6 (Optional) Repeat this procedure to enter additional license keys, for example, if you have standalone vRealize Automation license keys in addition to vCloud Suite license keys.

If you add both a vCloud Suite license key and a standalone vRealize Automation license key in IaaS, a message appears that you have overlapping licenses, but it is not an error. You can proceed with adding the license.

The following restrictions apply when assigning multiple licenses to vRealize Automation.

- Only one vCloud Suite license can be active. If you have an existing license and enter a new license key, it replaces the previous license.
- Only one vRealize Automation Advanced Edition or Enterprise Edition license can be active. If you have an existing license and enter a new license key, it replaces the previous license.
- When replacing a vCloud Suite or standalone vRealize Automation license, the new license must be of the same level or higher and of the same type. For example, a license for vRealize Automation Advanced Edition can only be replaced by another license for vRealize Automation Advanced Edition or Enterprise Edition. A license for vRealize Automation Enterprise Edition can only be replaced by another license for vRealize Automation Enterprise Edition. You cannot replace it with a vCloud Suite license.
- A vRealize Automation Desktop license can be used in combination with any vCloud Suite or standalone vRealize Automation license.

After you add a license to IaaS, you cannot remove it.

If your license expires, you must replace it with a license of the same type

Assign the vCloud Suite License to vRealize Operations Manager

To use vRealize Operations Manager as part of the vCloud Suite, you must assign the vCloud Suite license key to vRealize Operations Manager.

To activate vRealize Operations Manager monitoring, you add licenses at installation or later. You track licenses so that you know what vRealize Operations Manager may monitor and when your licenses expire.

To learn more about vRealize Operations Manager licensing and license keys, see [Add a vRealize Operations Manager License Key](#) in *Maintaining and Expanding vRealize Operations Manager*.

Prerequisites

You must install vRealize Operations Manager before assigning it the vCloud Suite license key. See [“Install vCloud Suite Components,”](#) on page 23.

Procedure

- 1 In the left pane, click **Administration**.
- 2 Select **Licensing**.
- 3 Click the **License Keys** tab.
- 4 From the toolbar, click the button to add a license key.
- 5 From the drop-down menu, select the appropriate solution license for vCloud Suite (instead of the individual product license).
- 6 Enter the license key and click **Validate**.
- 7 Click **OK**, and click **Save**.

Assign the vCloud Suite License to vRealize Operations Manager vApp

To complete a new vRealize Operations Manager installation, you log in and complete a one-time process to license the product and add solutions for the kinds of resources to monitor and manage.

Prerequisites

- Create and configure the new cluster of vRealize Operations Manager nodes.
- Click the **Start vRealize Operations Manager** button to start the cluster.

Procedure

- 1 In a Web browser, navigate to the name or IP address of the master node.
If you configured nodes and started the cluster, the product takes you to the login page.
- 2 Enter the username **admin** and the password that you defined when you configured the master node, and click **Login**.
Because this is the first time logging in, a one-time wizard appears.
- 3 Click **New Environment** and click **Next**.
- 4 Read and accept the End User License Agreement, and click **Next**.
- 5 Enter your product key, or select the option to run vRealize Operations Manager in evaluation mode.
Your level of product license determines what solutions you may install to monitor and manage resources.
 - Standard. vCenter only
 - Advanced. vCenter plus other infrastructure solutions
 - Enterprise. All solutions
 vRealize Operations Manager does not license managed objects in the same way that vSphere does, so there is no object count when you license the product.
- 6 If you entered a product key, click **Validate License Key**.
- 7 Click **Next**, and click **Finish**.
The one-time wizard finishes, and the vRealize Operations Manager interface appears.

What to do next

- Use the vRealize Operations Manager interface to configure the solutions that are included with the product.
- Use the vRealize Operations Manager interface to add more solutions.
- Use the vRealize Operations Manager interface to add monitoring policies.

Assign the vCloud Suite License to vRealize Hyperic

You configure the vRealize Hyperic license in vCloud Suite by editing the `hq-server.conf` file.

vRealize Hyperic is part of several VMware products, including vCenter Operations Management Suite, vCloud Suite, and vRealize Hyperic, each with its own licensing mechanism. vRealize Hyperic is also available as a standalone product. You configure the license according to the requirements of the product of which it is a part. To learn more about vRealize Hyperic licensing options, see [vRealize Hyperic Installation and Configuration Guide](#).

Prerequisites

Stop the vRealize Hyperic server.

Procedure

- 1 Open the `ServerHome/conf/hq-server.conf` file for editing.
- 2 Add the line `vccloud.license.key=LicenseKey`, where *LicenseKey* is the vCloud Suite license key.

What to do next

Restart the vRealize Hyperic server.

Assign the vCloud Suite License to vRealize Configuration Manager

Assign a vCloud Suite license key to vRealize Configuration Manager.

Prerequisites

Supply a vCloud Suite license key before clicking the button to start the installation. To learn more about vRealize Configuration Manager, see [Configuration Manager Installation Guide](#)

Procedure

- 1 On the left, click **Basic Information**.
- 2 Under **License Keys** Installing or Migrating vRealize Operations Manager, type a key to activate vRealize Configuration Manager, and click **Add**.
- 3 To obtain a different key or otherwise manage your license keys, click the link to open the MyVMware.com Web site.
- 4 To remove a key that you added, select the key and click **Remove**.

Assign the vCloud Suite License to vRealize Business for vSphere

To use vRealize Business for vSphere as part of the vCloud Suite, you must assign the vCloud Suite license key to vRealize Business for vSphere.

You can access the vRealize Business Standard user interface after logging in to the vRealize Automation user interface. The vRealize Business Standard user interface appears as a tab in the vRealize Automation user interface.

Prerequisites

- Verify that you have deployed and configured the vRealize Automation virtual appliance in your cloud environment.
- Verify that you have created a vRealize Business Standard tenant. For more information, see *vRealize Business Standard Installation and Administration Guide*.

Procedure

- 1 Log in to the vRealize Automation interface at `https://vRealize_Automation_host_name/vcac/org/tenant_URL` using credentials of a tenant administrator.
- 2 Click the **Administration** tab.
- 3 Click **Users & Groups** and select **Identify Store Users & Groups**.
- 4 Search and select the user to which you want to add a role.

- 5 From the Add Roles to this User box, assign the following privileges based on the requirement.
 - If the user has to perform all administration tasks such as managing connections, managing public cloud account, updating reference database, assign the **Business Management Administrator** role to a user who has the **Tenant Administration** role.

NOTE To assign the **Tenant Administration** role to the user, you have to log in as a default tenant administrator in vRealize Automation.

- If the user has to view and update the cost information only, assign **Business Management Administrator** role.
 - If the user has to view the details but not update the information, assign **Business Management Read only** role.
 - If the user has to view the assigned tenant details, but not perform other administration cost, assign the **Business Management Controller** role.
- 6 Click **Update**.
 - 7 Refresh the browser.
The **Business Management** tab is available in the vRealize Automation user interface.
 - 8 Click the **Business Management** tab.
A dialog prompts you to enter the license key.
 - 9 Enter a valid license key and click **Save**.

Monitoring License Usage for vCloud Suite

You can monitor the license usage and the available license capacity for all assigned vCloud Suite licenses by using the license reporting function in vCenter Server.

You can use the license reporting function in vCenter Server to perform the following tasks:

- View statistics for the license usage and capacity of vCloud Suite filtered by a vCenter Server system and time period.
- Export license usage reports in CSV files for further analysis and processing.

View the License Usage for vCloud Suite in the vSphere Client

To make sure that the license usage for vCloud Suite meets the compliance criteria for the product, you can regularly track the CPU usage for the assigned vCloud Suite licenses.

vCenter Server takes snapshots of the license usage every hour. A license usage snapshot contains data about the current license assignments and usage. The usage information in the license reporting interface contains aggregated statistics from snapshots that are taken in the period that you select.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.
- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, navigate to **Home > Administration > Licensing** and select the **Reporting** tab.

- 2 From the **vCenter Server** drop-down list, select a vCenter Server system.
Leave the default **All vCenter Server instances** selection.
- 3 From the **Time period** drop-down menu, select a preconfigured or a custom time period for which you want to aggregate license usage data.
For a custom time period, you must specify the start and end dates, and click **Recalculate** .
- 4 From the Products Chart pane, select a vCloud Suite product.

Details about the license usage for vCloud Suite for the selected time period appear in the Product Details pane. The license usage is calculated as the average daily high water mark for the selected period.

View the License Usage for vCloud Suite in the vSphere Web Client

You can use the license reporting function in the vSphere Web Client to track the license usage for vCloud Suite.

vCenter Server takes snapshots of the license usage every hour. A license usage snapshot contains data about the current license assignments and usage. The usage information in the license reporting interface contains aggregated statistics from snapshots that are taken in the period that you select.

Prerequisites

Required privilege: **Global.Licenses**

Procedure

- 1 From the vSphere Web Client navigator home, select **Administration**, and under **Licensing** select **License Reports**.
- 2 From the **vCenter Server** drop-down list, select a vCenter Server system.
- 3 (Optional) To aggregate license usage data for a vCenter Server system that is part of a Linked Mode group, select **Show data only for the selected vCenter Server**.
- 4 From the **Time period** drop-down menu, select a preconfigured or a custom time period for which you want to aggregate license usage data.
For a custom time period, you must specify the start and end dates, and click **Recalculate** .
- 5 From the Products Chart pane, select a vCloud Suite product.

Details about the license usage for vCloud Suite for the selected time period appear in the Product Details pane. The license usage is calculated as the average daily high water mark for the selected period.

Export a License Usage Report for vCloud Suite

You can export a report of the license usage for vCloud Suite for a time period and vCenter Server system. The report is exported in a CSV file that you can later open with third-party applications.

The license usage data in an exported report contains the license usage snapshots that vCenter Server collects every hour.

NOTE A tamper-detection feature in vCenter Server protects the license usage information. If the licensing data in the vCenter Server database has been edited, you cannot export a license usage report.

Prerequisites

- Required privilege: **Global.Licenses**
- Verify that the vSphere Client is connected to the vCenter Server system.

- Verify that the vCloud Suite license key is added in the repository of vCenter Server. See [“Add the vCloud Suite License by Using the vSphere Client,”](#) on page 37

Procedure

- 1 In the vSphere Client, navigate to **Home > Administration > Licensing** and select the **Reporting** tab.
- 2 Click **Export**.
- 3 From the **vCenter Server** drop-down list, select the vCenter Server system for which you want to export a license usage report.
Leave the default **All vCenter Server instances** selection.
- 4 From the **Time period** drop-down menu, select a preconfigured or a custom time period.
- 5 Click **Export**.
- 6 Save the report on your local system.

Export a License Usage Report for vCloud Suite in the vSphere Web Client

In the vSphere Web Client, you can export a report of the license usage for vCloud Suite for a time period and vCenter Server system. The report is exported in a CSV file that you can later open with third-party applications.

The license usage data in an exported report contains the license usage snapshots that vCenter Server collects every hour.

NOTE A tamper-detection feature in vCenter Server protects the license usage information. If the licensing data in the vCenter Server database has been edited, you cannot export a license usage report.

Prerequisites

Required privilege: **Global.Licenses**

Procedure

- 1 From the vSphere Web Client navigator home, select **Administration**, and under **Licensing** select **License Reports**.
- 2 Click **Export**.
- 3 From the **vCenter Server** drop-down list, select the vCenter Server system for which you want to export a license usage report.
If you select a vCenter Server system that is part of a Linked Mode group, the report contains license use data for the entire group.
- 4 (Optional) To export data for a vCenter Server system that is part of a Linked Mode group, select **Export license data only for the selected vCenter Server instance**.
- 5 From the **Time period** drop-down menu, select a preconfigured or a custom time period.
- 6 Click **Export**.
- 7 Save the report on your local system.

vCloud Suite Use Cases

Scenarios in this chapter instruct you how to achieve realistic user goals by using vCloud Suite.

Disaster Recovery to Cloud

As a system administrator, you can configure cloud failover for virtual machines, so that you can guarantee that important workloads keep running even when your on-site data center experiences problems. You can combine the VM replication functionality provided by the vSphere Replication virtual appliance with the VMware vCloud Air service to achieve business continuity goals without the need for a second data center or additional equipment .

In your on-premise data center (also known as the primary site), the vSphere Replication virtual appliance lets you select the virtual machines that you want to replicate to a remote site over the Internet. The vCloud Air service can serve as a remote site for your virtual machines, ensuring that failover happens in a predictable and verifiable manner. When the protected virtual machines go offline at your on-premise data center, you can power on their copies in the cloud.

Disaster Recovery to Cloud subscriptions do not include service integration with shared and dedicated provisioning in vCloud Air.

The following VMware products are used in the scenario:

Table 4-1. vCloud Suite Components Required for Disaster Recovery to Cloud

| vCloud Suite component | Description |
|-------------------------|---|
| ESXi 6.0 | The VMware hypervisor that lets you run a virtualized environment. |
| vCenter Server 6.0 | Provides management capabilities in a browser-based interface, as well as integration points for other vCloud Suite components. |
| vSphere Replication 6.0 | vSphere Replication is an extension to vCenter Server that provides hypervisor-based virtual machine replication and recovery. |

vCloud Suite components that enable you to perform recovery to cloud can coexist with other solutions of compatible version. See [“List of vCloud Suite Components,”](#) on page 7.

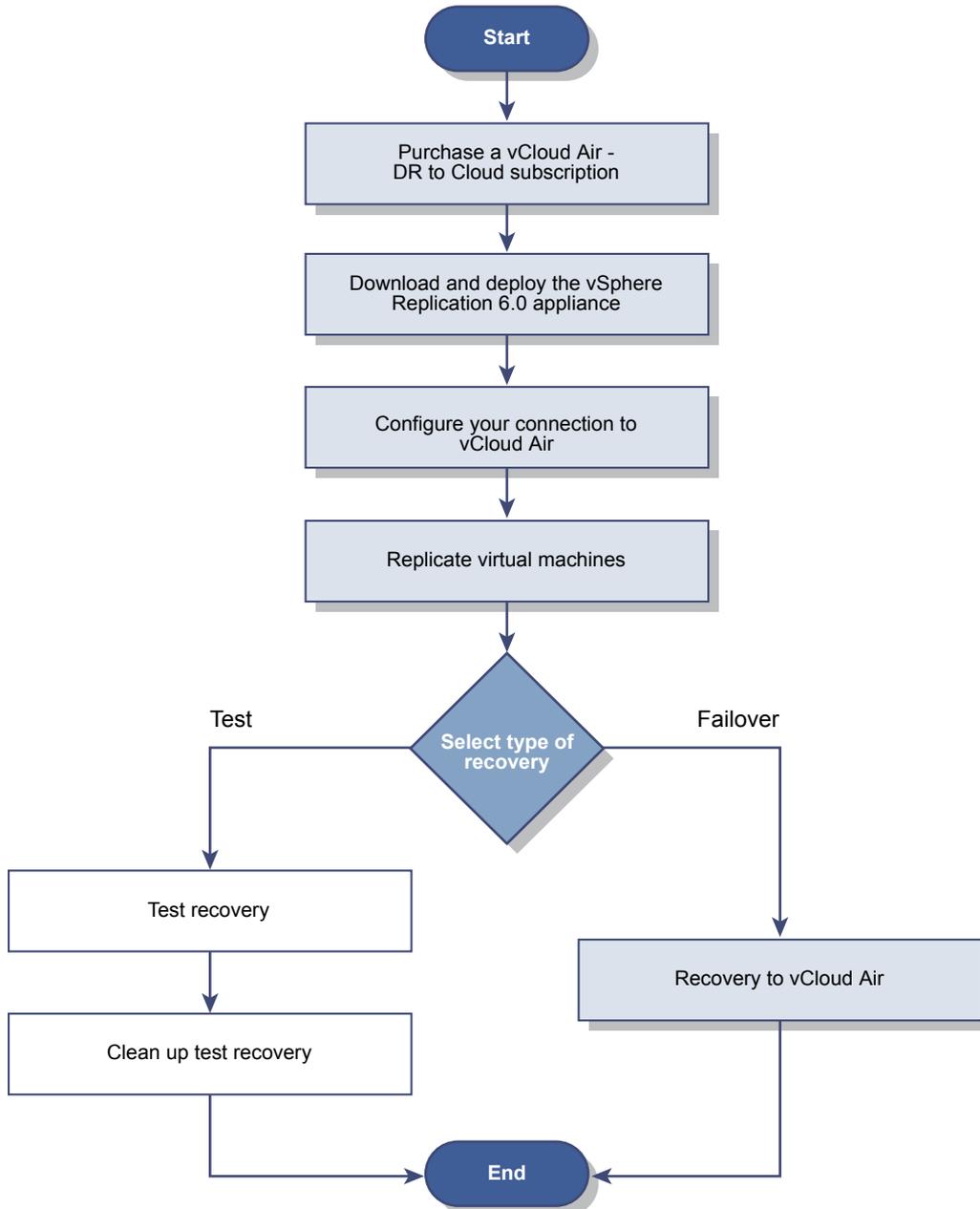
NOTE You cannot use Site Recovery Manager to protect virtual machines that are replicated to the vCloud Air.

The following example objects are used in the scenario:

Table 4-2. Sample Environment Details

| Object | Description |
|----------------|--|
| ACME Corp VM 1 | A Linux virtual machine that runs one of your mission critical applications . |
| ACME Corp VM 2 | A Windows virtual machine that runs another of your mission-critical applications. |

Figure 4-1. Disaster recovery to cloud workflow



To verify your setup, you can perform test recoveries before an actual recovery is required. Test recoveries are not enabled by default. You need to file a service request to make the test functionality available.

If you have purchased VMware vCloud® Air™ Disaster Recovery, and have access to failback capabilities (using vSphere Replication), please refer to the [vCloud Air Documents Library](#) for information on reverse replication from a vCloud Air data center to a customer's on premises environment. You can also copy virtual machines from vCloud Air to your on premises data center using vCloud Connector.

Prerequisites

- Verify that your virtual machines are running in a vSphere environment.
- Verify that you have sufficient privileges to perform administrative operations in the vSphere Web Client.
- Verify that you have valid licenses for all products in your environment.
- Verify that you have vCloud Air credentials for the Disaster Recovery to Cloud service.

Procedure

- 1 [Download and Deploy the vSphere Replication Virtual Appliance](#) on page 51
To start preparing your vCloud Suite environment for DR2C, you must install and configure vSphere Replication. vSphere Replication is distributed as an OVF virtual appliance.
- 2 [Configure Network Connection to vCloud Air](#) on page 52
You have deployed the vSphere Replication appliance in your on-premise environment. The next step of preparing your environment for DR2C is to set up a connection to vCloud Air.
- 3 [Replicate Virtual Machines to the Cloud](#) on page 53
In the vSphere Web Client, you can select your mission-critical virtual machines for replication to vCloud Air.
- 4 [Recover a Virtual Machine in the Cloud](#) on page 54
By using the Web interface of vCloud Air, you can recover the virtual machines that you replicated to the cloud. During recovery, all replication activity is stopped.

Download and Deploy the vSphere Replication Virtual Appliance

To start preparing your vCloud Suite environment for DR2C, you must install and configure vSphere Replication. vSphere Replication is distributed as an OVF virtual appliance.

You can use vSphere Replication with the vCenter Server Appliance or with a vCenter Server installation on Windows.

Prerequisites

- Verify that you have a valid vSphere Replication license.
- Verify that you have valid credentials for accessing the vCloud Air service.
- Verify that you have the vSphere Client Integration Plug-in installed.

Procedure

- 1 Visit the VMware corporate Web site or MyVMware to download the vSphere Replication virtual appliance.
You should save the template file to the local machine on which you use the vSphere Web Client.
- 2 Log in to the vSphere Web Client.
- 3 Select **vCenter > Hosts and Clusters**.
- 4 Right-click the host on which you want to deploy the appliance, and select **Deploy OVF template**.

- 5 Select **Local File** and browse to the vSphere Replication template file on your local machine.
The default name of the file is vSphere_Replication_OVF10.ovf.
- 6 Complete the template deployment wizard.
- 7 Log out of the vSphere Web Client, close the browser, and then log back in.
vSphere Replication is present on the **Home** tab of the vSphere Web Client.

What to do next

Configure the connection to vCloud Air.

Configure Network Connection to vCloud Air

You have deployed the vSphere Replication appliance in your on-premise environment. The next step of preparing your environment for DR2C is to set up a connection to vCloud Air.

vSphere Replication replicates the virtual machines from your on-premise data center to vCloud Air by using a secure connection over the Internet.

When you subscribe to the DR2C service, VMware creates two default networks for the service, an isolated network and an external routed network. The gateway for the routed network has a public IP address on its outside interface so that the routed network on the inside interface is accessible through the Intranet. You can use these networks for your virtual machines protected by the DR2C service.

When you configure VMs for disaster recovery in vSphere Replication by using the Connect to a cloud provider wizard, you specify which networks to use for the Test network and the Recovery network. The network choices that appear in the wizard are the networks configured for vCloud Air.

Procedure

- 1 In the vSphere Web Client, on the **vSphere Replication** tab under **Manage**, click the cloud connection icon .

The Connect to a Cloud Provider wizard opens.

- 2 On the Connection settings page, type the cloud provider address, the organization name, and credentials to authenticate with the cloud.

By default, vSphere Replication uses these credentials to establish a user session to the cloud and for system monitoring purposes. The login credential are in the message that you received with your vCloud Air account. The cloud provider address for vCloud Air has the format **https://unique_identifier.vchs.vmware.com**.

- 3 Click **Next**.

The Connect to a Cloud Provider wizard displays a list of virtual data centers to which you can connect. A virtual data center that is configured for disaster recovery is created for you in vCloud Air.

- 4 Select a virtual data center as a target for the connection and click **Next**.

- 5 Review your settings and click **Finish**.

When you add a new connection to the cloud, at first its status appears as **Missing network settings** status.

- 6 On the **vSphere Replication** tab under **Manage**, click the target network settings icon .

- 7 From the drop-down menus, select a recovery network and a test network, and click **Next**.

The drop-down menus display only the networks that are configured for vCloud Air.

- 8 On the Ready to complete page, review your settings and click **Finish**.

When you test a replication or perform a recovery operation, vCloud Air attaches the virtual machine to the test or recovery network respectively.

What to do next

Select the virtual machines to be replicated to vCloud Air.

Replicate Virtual Machines to the Cloud

In the vSphere Web Client, you can select your mission-critical virtual machines for replication to vCloud Air.

When you configure replication, you set a recovery point objective (RPO) to determine the period of time between replication operations. For example, an RPO of 1 hour aims to ensure that a virtual machine loses no more than 1 hour of data during the recovery.

Procedure

- 1 On the vSphere Web Client Home page, click **vSphere Replication**.
- 2 Select the vCenter Server instance that manages your virtual machines, and in the left pane, double-click **Virtual Machines**.
- 3 Select the virtual machines *ACME Corp VM 1* and *ACME Corp VM 2* to replicate.
You can select multiple inventory objects by using the Ctrl or Shift keys.
- 4 Right-click the virtual machines and select **All vSphere Replication Actions > Configure replication**.
The Configure Replication wizard opens, and Disaster Recovery to Cloud validates the virtual machines that can be configured for replication.
- 5 Verify the validation results and click **Next**.
- 6 Select **Replicate to a cloud provider** and click **Next**.
- 7 Select a target virtual data center in the vCloud Air site that you configured in the previous task, and click **Next**.
- 8 On the Target location page, select where to store replication data.
- 9 (Optional) On the Replication options page, select the quiescing method for the guest operating system of the source virtual machine and click **Next**.
- 10 On the Recovery settings page, use the RPO slider or the time spinners to set the longest period for which data loss is acceptable in the case of a site failure, and click **Next**.
The available RPO range is from 15 minutes to 24 hours.
- 11 Click **Finish**.

For each source virtual machine that is configured successfully, a replication task appears on the **vSphere Replication** tab under **Monitor**. When you configure replication by using vSphere Replication at your source site, the disaster recovery service creates placeholder virtual machines in vCloud Air that represent the virtual machines at your source site.

What to do next

Log in to the vCloud Air Web console and recover the virtual machines.

Recover a Virtual Machine in the Cloud

By using the Web interface of vCloud Air, you can recover the virtual machines that you replicated to the cloud. During recovery, all replication activity is stopped.

You can recover a virtual machine by using vCloud Air when your source site is no longer accessible. You might be able to begin a recovery from your source site by using your local vSphere Web Client; for example, if you have sufficient warning of an outage and still have access to your local vSphere Web Client so that you can run a planned migration.

In a production environment, you should verify that you tested the recovery before recovering the virtual machine to the cloud.

Procedure

- 1 Log in to the vCloud Air Web console.
- 2 On the **Dashboard** tab, click the virtual data center that is enabled for disaster recovery.
- 3 Click the **Virtual Machine** tab.
The table of virtual machines appears.
- 4 Select the virtual machines *ACME Corp VM 1* and *ACME Corp VM 2* to recover.
- 5 From the menu, click **Recovery**.
The confirmation dialog box appears.
- 6 Click **Continue**.

Recovering the virtual machine has the following result:

- In the **Virtual Machine** tab, the Recovery Status changes from Placeholder or Test to Recovered.
- Connects the virtual machine to the production network.
- Powers on the virtual machine in the cloud.

After you recover a virtual machine to the cloud, it has the same capabilities that the virtual machine had at the source site. You can access and operate your virtual machine recovered to the cloud for the time periods listed in the vCloud Air documentation.

Index

A

- activate vCloud Suite components **38**
- add the vCloud Suite license **36**
- assign license **40**
- assign license key **38**
- assign licenses **36**
- assign vCloud Suite license
 - vCenter Operations Management Suite **38**
 - vCenter Site Recovery Manager **39**
- assign vCloud Suite License, vCloud Networking and Security **39**

B

- business continuity **49, 53, 54**

C

- common services **33**
- conceptual design **11**
- configure license for vCloud Suite **42–44**

D

- Deployment **23**
- design considerations **15**
- disaster recovery to cloud
 - configure network connection **52**
 - deploy vSphere Replication **51**
- DR2C **49, 53, 54**

E

- encryption and security certificates **33**
- ESXi and the ESX Management Interfaces **32**
- external dependencies **26**

G

- glossary **5**

I

- IaaS **19**
- IaaS diagram **21**
- intended audience **5**
- introduction **7**
- iSCSI storage **31**
- iSCSI storage security **31**
- isolation, virtual machines **28**

L

- license
 - configure for vCloud Suite **42–44**
 - usage **46**
- license assignment **40**
- license capacity, processor **36**
- license key
 - add **37**
 - assign **37, 40**
- license usage
 - CPU usage **45**
 - export report **46, 47**
 - monitor **45**
- licensing, vCloud Suite **36**
- logical design **13**

M

- Monitoring **17**

N

- network **15**

O

- Orchestration layer **17**

P

- PaaS **22**
- platform-as-a-service **22**

R

- recover VMs **54**
- replicate VMs to cloud **53**
- resource limits and guarantees, security **28**

S

- scenarios **49**
- SDDC Infrastructure **14**
- SDDC model **9**
- security
 - resource guarantees and limits **28**
 - virtual machines **28**
- security considerations **27**
- shared storage **16**
- standard switch ports **30**
- system requirements **27**

V

- vCenter Server and security **33**
- vCenter Server systems **33**
- vCenter Single Sign-On **33**
- vCloud Suite
 - components **34, 35**
 - licensing **34, 36**
 - vSphere Web Client **36**
- vCloud Suite components
 - activate **37, 38, 40, 41**
 - add license key **37**
 - assign license **37, 38, 40**
 - custom licensing interface **40**
 - license management function **37, 38**
 - license vCloud Director **40**
 - vCloud Automation Center **41**
- vCloud Suite installation **23**
- vCloud Suite license, adding **36**
- vCloud Suite upgrade **24**
- virtual machines
 - resource reservations and limits **28**
 - security **28**
- virtual networks **30**
- virtualization and management in SDDC **14**
- vRealize Hyperic **43**
- vRealize Business for vSphere **44**
- vRealize Operations Manager **42, 43**