vCloud Suite Architecture Overview and Use Cases

vCloud Suite 5.8

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-001564-03
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.
# Updated Information

This vCloud Suite Architecture Overview and Use Cases is updated with each release of the product or when necessary.

This table provides the update history of the vCloud Suite Architecture Overview and Use Cases.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN-001564-02</td>
<td>Added information on provisioning applications in a vCloud environment as part of a functional platform-as-a-service deployment. See “Application Provisioning,” on page 63.</td>
</tr>
<tr>
<td>EN-001564-01</td>
<td>Updated version numbers of some vCloud Suite components to reflect the most recent enhancements. To ensure interoperability, verify that the components of your vCloud Suite environment are the correct versions. See “List of vCloud Suite Components,” on page 9.</td>
</tr>
<tr>
<td>EN-001564-00</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Introduction to vCloud Suite

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

You download, install, and configure vCloud Suite components separately. When deployed and configured, the interoperable components enable the software-defined data center (SDDC), where resources are virtualized and available as a service. Control of the data center is fully automated by software, and hardware configuration is maintained through software systems. vCloud Suite makes it possible for workloads to run in private, public, or hybrid clouds.

Individual products in vCloud Suite are delivered as either installation packages for Windows or Linux-based virtual appliances that you can deploy on ESXi hosts.

You can extend your vCloud Suite by using VMware vCloud Air as a second site in your datacenter environment. Use vCloud Suite together with 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.

**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>
<thead>
<tr>
<th>Table 1-1. Components of vCloud Suite 5.8 and their versions</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Product name</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>5.5 Update 2</td>
<td>Provides bare-metal virtualization of servers so you can consolidate your applications on less hardware.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>5.5 Update 2</td>
<td>Provides a centralized platform for managing vSphere environments. <strong>IMPORTANT</strong> vCenter Server is required for building the core infrastructure of the Software-Defined Data Center and is licensed separately on a per instance basis. See vCenter Server product overview.</td>
</tr>
<tr>
<td>Product name</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vCenter Orchestrator</td>
<td>5.5.2.1</td>
<td>Provides the capability to create workflows that automate activities such as provisioning virtual machine, performing scheduled maintenance, initiating backups, and many others.</td>
</tr>
<tr>
<td>vCenter Update Manager</td>
<td>5.5 Update 2</td>
<td>Provides centralized, automated patch and version management for vSphere and offers support for ESXi hosts, virtual machines, and virtual appliances.</td>
</tr>
<tr>
<td>vCloud Networking and Security</td>
<td>5.5.3.1</td>
<td>Provides a security suite for vSphere. vCloud Networking and Security (formerly vShield) is a critical security component for protecting virtualized datacenters from attacks and misuse to help you achieve your compliance-mandated goals.</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>5.5.2</td>
<td>Provides the ability to build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual datacenters.</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>6.1</td>
<td>Provides functionality for deploying and provisioning of business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers. vCloud Automation Center Enterprise includes vCloud Automation Center Application Services.</td>
</tr>
<tr>
<td>vCloud Automation Center Application Services</td>
<td>6.1</td>
<td>Provides automated application provisioning in the cloud including deploying and configuring the application’s components and dependent middleware platform services on infrastructure clouds.</td>
</tr>
<tr>
<td>vCenter Operations Manager</td>
<td>5.8.3</td>
<td>Provides comprehensive visibility and insights into the performance, capacity and health of your infrastructure.</td>
</tr>
<tr>
<td>vCenter Configuration Manager</td>
<td>5.7.2</td>
<td>Provides automation of configuration and compliance management across your virtual, physical and cloud environments, assessing them for operational and security compliance.</td>
</tr>
<tr>
<td>vCenter Hyperic</td>
<td>5.8.3</td>
<td>Provides monitoring of operating systems, middleware and applications running in physical, virtual, and cloud environments.</td>
</tr>
<tr>
<td>vCenter Infrastructure Navigator</td>
<td>5.8.2</td>
<td>Provides automated discovery of application services, visualizes relationships, and maps dependencies of applications on virtualized compute, storage and network resources.</td>
</tr>
<tr>
<td>Product name</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>5.8.0.1</td>
<td>Provides replication, at the individual virtual machine disk level, between datastores hosted on any storage.</td>
</tr>
<tr>
<td>vCenter Site Recovery Manager</td>
<td>5.8</td>
<td>Provides disaster recovery capability that lets you perform automated orchestration and nondisruptive testing for virtualized applications.</td>
</tr>
<tr>
<td>vSphere Data Protection</td>
<td>5.8</td>
<td>Provides advanced data protection with backup and recovery to disk via VMware vSphere with Operations Management Data Protection features.</td>
</tr>
<tr>
<td>vSphere Big Data Extensions</td>
<td>2.0</td>
<td>Simplifies running Big Data workloads on the vSphere platform.</td>
</tr>
<tr>
<td>vSphere App HA</td>
<td>1.1.1</td>
<td>Provides high availability for the applications that are running on the virtual machines in your environment.</td>
</tr>
<tr>
<td>vCenter Support Assistant</td>
<td>5.5.1.1</td>
<td>Provides proactive support, by collecting support bundles on a regular basis.</td>
</tr>
</tbody>
</table>
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. Start by deploying the datacenter core infrastructure, because it 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

**Application Platform Service**
- Self-service application development
- Application blueprinting
- Application deployment standardization

**Infrastructure Service**
- Self-service user portal
- Catalogs and standard templates
- Low administration overhead

**Software-defined Data Center Core Infrastructure**
- Management
- Monitoring with performance and capacity
- Orchestration

**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 mainly by vCloud Automation Center, 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 53.
To start deploying vCloud Suite, you need a small number of physical hosts. 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.

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, and you expand it as needed.

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

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.

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

The hosts in the management cluster run all management components required to support the software-defined data center. A single management cluster is required within a 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 paired with VMware vCloud Networking and Security. Payload clusters that require access to external networks are managed by the same vCenter Server instance. As the platform scales, you should deploy additional Edge clusters to service specific groups of payload clusters.

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

Payload cluster

The payload cluster supports the delivery of all 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 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, and you expand it as needed.

Typically, you deploy more vCloud Suite components in the management cluster than you do in other types of clusters.

**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. vCenter Orchestrator is a vCloud Suite component that you should deploy at early stage, in order to prepare the environment for IaaS and PaaS capabilities.

### Extended set of components

As the complexity of the environment increases, you install and configure additional products. vCenter Operations Manager and related products provide advanced monitoring features. vCloud Automation Center 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 vCenter Operations Manager and vCenter 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 as an Element of vCloud Suite Infrastructure on page 18
  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 as an Element of vCloud Suite Core Infrastructure on page 21
  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 as an Element of vCloud Suite Core Infrastructure on page 23
  The software-defined data center requires orchestration capability. In vCloud Suite, you can use vCenter Orchestrator to orchestrate processes by using workflows.

Virtualization and Management as an Element 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 19
  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 19
  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 20
  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 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 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 in a 64-bit Windows 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 Microsoft licensing costs. When using an external Oracle database, the vCenter Server Virtual Appliance can support a maximum of 3,000 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 as an Element of 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 in vCenter Operations Manager Suite include the following products:

Table 2-1. Monitoring products in vCloud Suite

<table>
<thead>
<tr>
<th>Monitoring component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Operations Manager</td>
<td>Provides comprehensive visibility and insights into the performance, capacity and health of your infrastructure.</td>
</tr>
<tr>
<td>vCenter Infrastructure Navigator</td>
<td>Automatically discovers application services, visualizes relationships and maps dependencies of applications on virtualized compute, storage and network resources.</td>
</tr>
<tr>
<td>vCenter Hyperic</td>
<td>Monitors application health and is fundamental to the operation of VMware AppHA.</td>
</tr>
</tbody>
</table>

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

vCenter 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 vCenter Operations Manager and related products, see https://www.vmware.com/support/pubs/vmware-vcops-suite-pubs.html.
The vCenter Operations Manager vApp contains two virtual machines. One of the virtual machines runs the analytics engine, and the other runs the user interface component. Plug-ins enable you to add additional functionality, according to the needs of your environment. You can use and configure vCenter Operations Manager by using the Web-based interface.
Orchestration as an Element of vCloud Suite Core Infrastructure

The software-defined data center requires orchestration capability. In vCloud Suite, you can use vCenter Orchestrator to orchestrate processes by using 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. In the IaaS layer, vCloud Automation Center can trigger vCenter Orchestrator workflows, and you can publish workflows in your service catalog.

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 one vCenter Orchestrator instance for each vCenter Server system in your environment.

The main elements of the orchestration layer are:
- vCenter Orchestrator
- vCenter Orchestrator plug-ins

![Design of the orchestration layer](image)

Table 2-2. Components of vCloud Suite orchestration

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Orchestrator Appliance</td>
<td>You can deploy vCenter Orchestrator as a virtual appliance. The vCenter Orchestrator Appliance, running in stand-alone mode (not HA) is the recommended approach for deployment.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication can be provided by Active Directory or vCenter Single Sign-on.</td>
</tr>
</tbody>
</table>
Table 2-2. Components of vCloud Suite orchestration (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Orchestrator config.</td>
<td>The Web-based interface where you configure the appliance database, SSL cert., license, and so on.</td>
</tr>
<tr>
<td>designer interface</td>
<td>The Web-based interface where you create and customize workflows.</td>
</tr>
<tr>
<td>vCenter Server plug-in</td>
<td>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.</td>
</tr>
<tr>
<td>Multi Node plug-in</td>
<td>An Orchestrator plug-in that provides remote vCO management and remote workflow execution.</td>
</tr>
</tbody>
</table>

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.

The core of the IaaS layer is the vCloud Automation Center virtual appliance that you must deploy on an ESXi host and configure.

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

Table 2-3. Infrastructure service components

<table>
<thead>
<tr>
<th>Infrastructure service section</th>
<th>Design components</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center</td>
<td>vCloud Automation Center Portal Web/App server</td>
</tr>
<tr>
<td>virtual appliance</td>
<td>vCloud Automation Center vPostgreSQL database</td>
</tr>
<tr>
<td>vCloud Automation Center IaaS</td>
<td>vCloud Automation Center IaaS Web server</td>
</tr>
<tr>
<td></td>
<td>vCloud Automation Center IaaS Manager services</td>
</tr>
<tr>
<td>Distributed execution</td>
<td>vCloud Automation Center distributed execution managers:</td>
</tr>
<tr>
<td></td>
<td>■ Orchestrator</td>
</tr>
<tr>
<td></td>
<td>■ Workers</td>
</tr>
<tr>
<td>Integration</td>
<td>vCloud Automation Center Agent machines</td>
</tr>
<tr>
<td>Cost management</td>
<td>IT Business Management</td>
</tr>
</tbody>
</table>
Table 2-3. Infrastructure service components (Continued)

<table>
<thead>
<tr>
<th>Infrastructure service section</th>
<th>Design components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning infrastructure</td>
<td>• vSphere environment</td>
</tr>
<tr>
<td></td>
<td>• vCloud Director environment</td>
</tr>
<tr>
<td></td>
<td>• vCenter Orchestrator environment</td>
</tr>
<tr>
<td></td>
<td>• Other supported physical, virtual, or cloud environment</td>
</tr>
<tr>
<td>Supporting infrastructure</td>
<td>• Microsoft SQL database environment</td>
</tr>
<tr>
<td></td>
<td>• PostgreSQL database environment (if not embedded in the virtual appliance)</td>
</tr>
<tr>
<td></td>
<td>• LDAP or Active Directory environment</td>
</tr>
<tr>
<td></td>
<td>• SMTP and email environment</td>
</tr>
</tbody>
</table>

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

Figure 2-8. IaaS components

For an in-depth discussion of key IaaS concepts, see the vCloud Automation Center documentation.

**Self-service portal**

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

**Infrastructure Components**

vCloud Automation Center requires you to configure vSphere 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 vCloud Automation Center, such as VMware ITBM.
**Conceptual 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 2-9. Conceptual 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 by 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-a-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 vCloud Automation Center 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 vCloud Director and vCloud Automation Center, and across public clouds such as Amazon EC2.

Using vCloud Automation Center, 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, vCloud Application Director 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, you must install its components separately and ensure that the required prerequisites and configuration requirements are met.

This book 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 29
- “Update vCloud Suite Components,” on page 31
- “External Dependencies for Deploying vCloud Suite,” on page 32
- “System Requirements of vCloud Suite Components,” on page 33
- “Security Considerations,” on page 33
- “Licensing,” on page 43

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 vCenter Operations Manager to monitor applications, you must install vCenter Infrastructure Navigator first. If you want to use vSphere App HA, you must install vCenter Hyperic first.

You download and install vCloud Suite components separately. Depending on the type of cluster that you are building, you might need to omit some components from the installation 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 32.

Verify that you have a valid vCloud Suite license. See “Licensing,” on page 43.
**Procedure**

1. Install ESXi.
   
   If you install vCenter Server on a physical machine, you can install vCenter Server first.
   
   See [Installing ESXi](#).

2. Install vCenter Server.
   
   See [Installing vCenter Server](#).

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

4. Install the following suite components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Orchestrator</td>
<td>Installing Orchestrator</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>Installing vCloud Automation Center</td>
</tr>
<tr>
<td>vCenter Operations Manager</td>
<td>Deployment and Configuration Guide</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>Installation and Upgrade Guide</td>
</tr>
</tbody>
</table>

5. Install the following suite components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center Application Services</td>
<td>Installing vCloud Application Director</td>
</tr>
<tr>
<td>vCenter Hyperic</td>
<td>vCenter Hyperic Installation and Configuration</td>
</tr>
</tbody>
</table>

6. Install the following suite components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Site Recovery Manager</td>
<td>Installing Site Recovery Manager</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>Installing vSphere Replication</td>
</tr>
<tr>
<td>vCenter Infrastructure Navigator</td>
<td>Installation and Configuration Guide</td>
</tr>
<tr>
<td>vSphere Data Protection</td>
<td>Administration Guide</td>
</tr>
<tr>
<td>vSphere Big Data Extensions</td>
<td>Installing Big Data Extensions</td>
</tr>
<tr>
<td>vCenter Configuration Manager</td>
<td>Installation Guide</td>
</tr>
</tbody>
</table>

7. Install the following suite components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>vShield Edge</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
<tr>
<td>vShield App</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
<tr>
<td>vShield Endpoint</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
<tr>
<td>vCenter Update Manager</td>
<td>Installing Update Manager</td>
</tr>
</tbody>
</table>
Update vCloud Suite Components

Updating vCloud Suite components to newer versions requires you to perform separate update procedures. Follow the recommended update order to ensure that vCloud Suite updates complete without problems.

You should perform the update operations according to the recommended sequence. Some of the products in the sequence are bundled in groups. You can install the products that belong to a specific group in any order.

Prerequisites

- Verify that you have the required installation or upgrade packages.
- Verify that you have administrator privileges for all systems.

Procedure

1. Upgrade vCloud Automation Center.
   See Upgrading to vCloud Automation Center 6.1.
2. Update the following components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Update documentation</th>
</tr>
</thead>
</table>
| vCloud Automation Center Application Services | Upgrade Guide  
You can migrate data from Application Director to a  
fresh installation of  
vCloud Automation Center Application Services. |
| vCenter Configuration Manager          | Installation Guide                                                                   |
| vCloud Director                        | Upgrading vCloud Director                                                             |

   See vShield Installation and Upgrade Guide.
4. Update vCenter Server.
   See Upgrading vCenter Server.
5. Update vCenter Orchestrator.
   Installing and Upgrading Orchestrator.
6. Update the following components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Update documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Site Recovery Manager</td>
<td>Upgrading Site Recovery Manager</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>Upgrading vSphere Replication</td>
</tr>
<tr>
<td>vCenter Operations Manager</td>
<td>Deployment and Configuration Guide</td>
</tr>
<tr>
<td>vSphere Data Protection</td>
<td>Administration Guide</td>
</tr>
<tr>
<td>vCenter Infrastructure Navigator</td>
<td>Installation and Configuration Guide</td>
</tr>
<tr>
<td>vCenter Hyperic</td>
<td>vCenter Hyperic Installation and Configuration</td>
</tr>
<tr>
<td>vSphere Big Data Extensions</td>
<td>Upgrading Big Data Extensions</td>
</tr>
</tbody>
</table>
7 Update ESXi.
   See Upgrading Your Hosts.
   You should update VMware tools on your VMs after the ESXi update.

8 Update the following components:

<table>
<thead>
<tr>
<th>Product</th>
<th>Installation instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>vShield Edge</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
<tr>
<td>vShield App</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
<tr>
<td>vShield Endpoint</td>
<td>vShield Installation and Upgrade Guide</td>
</tr>
</tbody>
</table>

You have updated 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

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Active Directory is required to implement and operate the vCloud Suite infrastructure.</td>
</tr>
<tr>
<td>DNS</td>
<td>DNS must be configured for connectivity between vCenter Server, Active Directory, ESXi hosts, and virtual machines.</td>
</tr>
<tr>
<td>DHCP/TFP</td>
<td>PXE boot is required for vSphere Auto Deploy functionality.</td>
</tr>
<tr>
<td>64-bit Windows OS</td>
<td>Some vCloud Suite components can be installed on Windows Server 2008 and later. vCloud Director requires RHEL or CentOS Linux.</td>
</tr>
<tr>
<td>Microsoft SQL or Oracle database</td>
<td>vCloud Suite components can work with embedded or external databases, depending on the product and your environment.</td>
</tr>
<tr>
<td>Network infrastructure</td>
<td>Network infrastructure with 1Gbps or 10Gbps switches. Depending on the needs of your environment, higher throughput is recommended.</td>
</tr>
<tr>
<td>Storage Area Network</td>
<td>Stability and performance of the SAN affects the virtual machines.</td>
</tr>
<tr>
<td>Time synchronization</td>
<td>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.</td>
</tr>
<tr>
<td>Staff</td>
<td>Properly trained IT staff is critical for the correct implementation, operation, support, and enhancement of your environment.</td>
</tr>
<tr>
<td>Policies and procedures</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 5.8 components |
|---|---|
| Product | System requirements documentation |
| vSphere | System Requirements |
| vCenter Orchestrator | Orchestrator System Requirements |
| vCenter Update Manager | System Requirements |
| vCloud Networking and Security | vShield Installation and Upgrade Guide |
| vCloud Automation Center | Preparing for Installation |
| vCloud Automation Center Application Services | System Requirements |
| vCenter Operations Manager | Deployment and Configuration Guide |
| vCenter Configuration Manager | Installation Guide |
| vCenter Hyperic | Supported Configurations and System Requirements |
| vCenter Infrastructure Navigator | Installing vCenter Infrastructure Navigator |
| vCloud Director | Hardware and Software Requirements |
| vSphere Replication | Installing vSphere Replication |
| vCenter Site Recovery Manager | Site Recovery Manager 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 34
  Virtual machines are the 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 36
  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 Virtual Machines with VLANs on page 36
  The network can be one of the most vulnerable parts of any system. The virtual machine network requires as much protection as its physical counterpart. Virtual Machine network security can be enhanced in several ways, including through the use of virtual local area networks (VLANS).
Securing Standard Switch Ports on page 38
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 39
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 and the ESX Management Interfaces on page 40
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 firewall.

Securing vCenter Server Systems on page 41
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 41
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 41
vCenter Single Sign-On is a component of the management infrastructure that provides the capability to manage the environment with Active Directory credentials.

Security and Virtual Machines
Virtual machines are the 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 networks within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated from any physical 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 Virtual Machines with VLANs**

The network can be one of the most vulnerable parts of any system. The virtual machine network requires as much protection as its physical counterpart. Virtual Machine network security can be enhanced in several ways, including through the use of virtual local area networks (VLANS).

If the virtual machine network is connected to a physical network, it can be subject to breaches to the same degree that a network made up of physical machines is. Even if the virtual machine network is isolated from any physical network, virtual machines in the network can be subject to attacks from other virtual machines in the network. The requirements for securing virtual machines are often the same as those for physical machines.

Virtual machines are isolated from each other. One virtual machine cannot read or write another virtual machine’s memory, access its data, use its applications, and so forth. However, within the network, any virtual machine or group of virtual machines can still be the target of unauthorized access from other virtual machines and might require further protection by external means.

- Adding firewall protection to the virtual network by installing and configuring host-based firewalls on some or all of its virtual machines.
For efficiency, private virtual machine Ethernet networks or virtual networks can be configured. With virtual networks, a host-based firewall is installed on a virtual machine at the head of the virtual network. This serves as a protective buffer between the physical network adapter and the remaining virtual machines in the virtual network.

Installing a host-based firewall on virtual machines at the head of virtual networks is a good security practice. However, because host-based firewalls can slow performance, it’s important to balance security needs against performance before deciding to install host-based firewalls on virtual machines elsewhere in the virtual network.

Keeping different virtual machine zones within a host on different network segments. If virtual machine zones on their own network segments are isolated, the risks of data leakage from one virtual machine zone to the next is minimized. Segmentation prevents various threats, including Address Resolution Protocol (ARP) spoofing, in which an attacker manipulates the ARP table to remap MAC and IP addresses, thereby gaining access to network traffic to and from a host. Attackers use ARP spoofing to generate Man in the Middle attacks, DoS attacks, hijack the target system, and otherwise disrupt the virtual network.

Planning segmentation carefully lowers the chances of packet transmissions between virtual machine zones, which prevents sniffing attacks that require sending network traffic to the victim. Also, an attacker cannot use an insecure service in one virtual machine zone to access other virtual machine zones in the host. Segmentation can be implemented by using either of two approaches, each of which has different benefits.

- Use separate physical network adapters for virtual machine zones so that the zones are isolated. Maintaining separate physical network adapters for virtual machine zones is probably the most secure method and is less prone to misconfiguration after the initial segment creation.
- Set up virtual local area networks (VLANs) to help safeguard the network. Because VLANs provide almost all of the security benefits inherent in implementing physically separate networks without the hardware overhead, they offer a viable solution that can save the cost of deploying and maintaining additional devices, cabling, and so forth.

This level of security can be implemented in different ways.

VLANs are an IEEE standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN. When properly configured, VLANs provide a dependable means to protect a set of virtual machines from accidental or malicious intrusions.

VLANs let you segment a physical network so that two machines in the network are unable to transmit packets back and forth unless they are part of the same VLAN. For example, accounting records and transactions are among a company’s most sensitive internal information. In a company whose sales, shipping, and accounting employees all use virtual machines in the same physical network, you might protect the virtual machines for the accounting department by setting up VLANs.
Figure 3-3. Sample VLAN Layout

In this configuration, all employees in the accounting department use virtual machines in VLAN A and the employees in sales use virtual machines in VLAN B.

The router forwards packets containing accounting data to the switches. These packets are tagged for distribution to VLAN A only. Therefore, the data is confined to Broadcast Domain A and cannot be routed to Broadcast Domain B unless the router is configured to do so.

This VLAN configuration prevents the sales force from intercepting packets destined for the accounting department. It also prevents the accounting department from receiving packets intended for the sales group. The virtual machines serviced by a single virtual switch can be in different VLANs.

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 and the ESX 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 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 though 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 Active Directory credentials.

In product versions earlier than vCenter Server 5.1, when users connect to vCenter Server, they were authenticated when vCenter Server validated their credentials against an Active Directory domain or the list of local operating system users. In vCenter Server 5.5, users authenticate through vCenter Single Sign On.
ESXi 5.5 is not integrated with vCenter Single Sign-On, and ESXi users cannot be created with the vSphere Web Client. ESXi users must be created and administered with the vSphere Client. vCenter Server is not aware of users that are local to ESXi. In addition, ESXi is not aware of vCenter Server users. However, Single Sign-On can be configured to use an Active Directory domain as an identity source and the ESXi host can be configured to point to the same Active Directory domain to obtain user and group information. This action allows the same set of users to be available to the host and to vCenter Server.

In vCenter Single Sign-On 5.5, the way that vCenter Single Sign-On is deployed and the type of user who installs vCenter Single Sign-On no longer affects which administrator user accounts have privileges on the Single Sign-On server and on vCenter Server. During the vCenter Server installation process, certain users are granted privileges to log in to vCenter Server and certain users are granted privileges to manage vCenter Single Sign-On. The vCenter Server administrator might not be the same user as the vCenter Single Sign-On administrator. This means that when a user logs in to the vSphere Web Client as the default Single Sign-On administrator (administrator@vsphere.local), they might not see any vCenter Server systems in the inventory. The inventory appears to be empty because the only see the systems upon which they have privileges in the vSphere Web Client.

This also means that when an operator logs in to the vSphere Web Client as the default vCenter Server administrator, they might not see the vCenter Single Sign-On configuration tool. The configuration tool is not present because only the default vCenter Single Sign-On Administrator (administrator@vsphere.local) is allowed to view and manage vCenter Single Sign-On after installation. The Single Sign-On administrator can create additional administrator users if necessary.

A conflict might occur if Local OS users cannot be seen or if there is a multiple site or node configuration issue. In that case, the identity source must be configured, or SSO must be used with vsphere.local domain authentication.

After SSO is installed (no matter the configuration), validate the identity sources which are configured so that they are both present and accurate to the way that authentication should proceed. Note that there is only one default domain in Single Sign-On 5.5, and as a result choose the most frequently logged into domain as the default domain.

Single Sign-On provides several different deployment methods to best suit your environment.

**Basic deployment**

A single standalone instance of vCenter Single Sign-On 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 vCenter Single Sign-On nodes are installed at a local site and configured for high availability. In vSphere 5.5, vCenter Single Sign-On has its own Directory Service that automatically replicates information to other vCenter Single Sign-On nodes in the environment.

**Multiple instances in different locations**

vCenter Single Sign-On nodes are installed at geographically separate sites. Each site has one or more vCenter Single Sign-On installations and data is replicated between sites. Multi-site deployment is required if configuring Linked Mode vCenter Server instances across sites.

The following vCloud Suite components support vCenter Single Sign-On:

- vCenter Server
- vCenter Orchestrator
- vCloud Automation Center
- vCloud Director
- vCloud Networking and Security
- vSphere Big Data Extensions
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 5.8 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 5.8 edition combines components such as vSphere Enterprise Plus, vCloud Director, vCloud Networking and Security, 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 5.8 Standard, you can use the same key to activate vSphere Enterprise Plus, vCloud Director, vCloud Networking and Security, 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 5.8 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 5.8 Enterprise edition.

Table 3-3. vCloud Suite 5.8 components that require a license

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td>Provides virtualization technology to serve as the platform for cloud infrastructure.</td>
</tr>
<tr>
<td>VMware vCloud® Director</td>
<td>Provides the ability to build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual datacenters.</td>
</tr>
<tr>
<td>VMware vCloud Networking and Security</td>
<td>Provides a security suite for VMware vSphere. vCloud Networking and Security (formerly vShield) is a critical security component for protecting virtualized datacenters from attacks and misuse to help you achieve your compliance-mandated goals.</td>
</tr>
<tr>
<td>VMware vCenter Operations Management Suite</td>
<td>Automates operations management and provides integrated performance, capacity, and configuration management for virtualized and cloud infrastructure.</td>
</tr>
</tbody>
</table>
Table 3-3. vCloud Suite 5.8 components that require a license (Continued)

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter Site Recovery Manager</td>
<td>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).</td>
</tr>
<tr>
<td>VMware vCloud Automation Center</td>
<td>Provides functionality for deploying and provisioning of business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers. vCloud Automation Center Enterprise includes vCloud Automation Center Application Services that automates application provisioning in the cloud including deploying and configuring the application's components and dependent middleware platform services on infrastructure clouds.</td>
</tr>
</tbody>
</table>

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 processor 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 5.x 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 44
- 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 5.8 license is compatible with vCenter Server 5.1 and 5.5.

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 45

**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 vCenter Operations Management Suite in the vSphere Client**

Assign the vCloud Suite license key to the components of vCenter Operations Management Suite to use them 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 45

**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 the components of vCenter Operations Management Suite that you want to run as part of vCloud Suite.

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.

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

**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 45

**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 45

**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, vCloud Automation Center, and vCloud Automation Center Application Services provide their own licensing interfaces for license assignments.

**NOTE** The vCloud Suite 5.8 license is compatible with vCenter Server 5.1 and 5.5.

**Assigning the vCloud Suite License to vCloud Automation Center Application Services**

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

If vCloud Automation Center Application Services is already installed and running and has another license key assigned, reinstall the product and assign it the vCloud Suite license key.

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

**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.

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 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 vCloud Automation Center 6.0**

To use vCloud Automation Center 6.0 as part of vCloud Suite, you must assign it the vCloud Suite license.

To enable the full functionality of vCloud Automation Center, 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 49
   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 49
   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 **vCAC 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 49.

**Procedure**

1. Log in to the vCloud Automation Center 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 vCloud Automation Center license keys in addition to vCloud Suite license keys.

   If you add both a vCloud Suite license key and a standalone vCloud Automation Center 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 vCloud Automation Center.

   - 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 vCloud Automation Center 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 vCloud Automation Center license, the new license must be of the same level or higher. For example, a license for vCloud Automation Center Advanced Edition can only be replaced by another license for vCloud Automation Center Advanced Edition or Enterprise Edition. A license for vCloud Automation Center Enterprise Edition can only be replaced by another license for vCloud Automation Center Enterprise Edition.

A vCloud Automation Center Desktop license can be used in combination with any vCloud Suite or standalone vCloud Automation Center license. After you add a license to IaaS, you cannot remove it.

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 45

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 45

**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.

This chapter includes the following topics:

- “Disaster Recovery to Cloud,” on page 53
- “Infrastructure Provisioning,” on page 59
- “Application Provisioning,” on page 63
- “Highly Available vCenter Single Sign-On Deployment,” on page 75

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, 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 the primary site, 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

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi 5.5 Update 2</td>
<td>The VMware hypervisor that lets you run a virtualized environment.</td>
</tr>
<tr>
<td>vCenter Server 5.5 Update 2</td>
<td>Provides management capabilities in a browser-based interface, as well as integration points for other vCloud Suite components.</td>
</tr>
<tr>
<td>vSphere Replication 5.8</td>
<td>vSphere Replication is an extension to vCenter Server that provides hypervisor-based virtual machine replication and recovery.</td>
</tr>
</tbody>
</table>
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 9.

**NOTE** You cannot use vSphere Replication to protect virtual machines that are protected by using Site Recovery Manager.

The following example objects are used in the scenario:

**Table 4.2. Sample Environment Details**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME Corp VM 1</td>
<td>A Linux virtual machine that runs one of your mission-critical applications.</td>
</tr>
<tr>
<td>ACME Corp VM 2</td>
<td>A Windows virtual machine that runs another of your mission-critical applications.</td>
</tr>
</tbody>
</table>
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.

By using vCloud Connector, you can copy virtual machines from vCloud Air to your on-premise data center.

**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 56

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 57

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 58

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 58

By using the Web interface of vCloud Air, you can recover the virtual machines that you replicated. Recovering a virtual machine shuts down the virtual machine at your source site (if possible) and recovers it in 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_OVF1.0.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 networks 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 credentials 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. Recovering a virtual machine shuts down the virtual machine at your source site (if possible) and recovers it in 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.

**Infrastructure Provisioning**

As a tenant administrator in ACME Corporation, you use the infrastructure service to deploy, configure, and manage workloads, so that you can quickly address the IT needs of your organization.

You can use the vCloud Automation Center portal to provision workloads to a vSphere environment.

**Figure 4-2. Workload Provisioning Workflow**
Table 4-3. Environment Details

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere endpoint</td>
<td>vCloud Automation Center can deploy workloads to a vSphere environment that administrators configured for use in ACME Corp. A fabric group and a network reservation are configured for the vSphere environment. You can configure other types of endpoints, for example vCloud Air or AWS.</td>
</tr>
<tr>
<td>vSphere blueprint</td>
<td>The Inventory Manager blueprint exists in your catalog. The virtual machine runs an application that is used in ACME Corp. The prefix that is configured for the workload is InventoryMgr-.</td>
</tr>
<tr>
<td>Configured service with a catalog</td>
<td>A service exists with the name Development Infrastructure.</td>
</tr>
</tbody>
</table>

A functional IaaS environment is based on several components.

Table 4-4. vCloud Suite Components Required for the Infrastructure Service

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>VMware bare-metal hypervisor that lets you run a virtualized environment.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Provides management capabilities in a browser-based interface, and integration points for other vCloud Suite components.</td>
</tr>
<tr>
<td>vCenter Orchestrator</td>
<td>Enables you to create workflows that automate activities in the data center.</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>Provides a secure portal where authorized administrators, developers, or business users can request new IT services.</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>vCloud Director lets you provision services as virtual data centers with virtualized compute, networking, storage, and security.</td>
</tr>
</tbody>
</table>

Prerequisites

Verify that the following conditions are met.

- You have the required components in your environment.
- You have a configured vSphere instance to serve as an vCloud Automation Center endpoint.
- You have set a reservation policy.
- You have created blueprints based on vSphere snapshots.

Procedure

1. Request a Virtual Machine Workload on page 61

   A new instance of a virtual machine that runs an inventory management application is required at ACME Corp. As an administrator for the tenant group that is responsible for inventory management, you can use the vCloud Suite Infrastructure as a Service capability to deploy and manage the workload.

2. Provision the Workload on page 62

   After you request the workload, you can provision the workload when you receive an approval.
3 **Customize the Virtual Machine** on page 62
   You requested and provisioned the virtual machine. You can customize the virtual machine to increase or decrease the amount of memory, the number of CPUs, and so on.

4 **Manage Workload Snapshots** on page 63
   You deployed and configured the workload. You can create snapshots of your running workloads from the self-service portal.

5 **Retire the Virtual Machine** on page 63
   The final stage in the lifecycle of a workload is the retirement operation. Alternatively, the tenant administrator can send a reclamation request to the owners of machines.

---

**Request a Virtual Machine Workload**

A new instance of a virtual machine that runs an inventory management application is required at ACME Corp. As an administrator for the tenant group that is responsible for inventory management, you can use the vCloud Suite Infrastructure as a Service capability to deploy and manage the workload.

In this scenario, the infrastructure service is preconfigured for your organization.

**Procedure**

1. Open a Web browser and log in to the vCloud Automation Center portal.
2. Select **Infrastructure > Blueprints > Blueprints**.
3. Review the configuration of the **Warehouse Manager** blueprint.
   When deployed, the vSphere blueprint uses the reservation policy vSphere and the machine prefix is **WarehouseMgr-**.
4. In the vCloud Automation Center portal, click **Catalog**.
   All services are listed.
5. Select a service in the catalog.
   All catalog items appear that are linked to the Development Infrastructure service and that are available for the user.
   Select the Development Infrastructure service.
6. Click an item to view details.
   The Catalog Item Details page shows information regarding the item, including the type and available configurations.
   - #Machines
   - Lease duration
   - #CPUs
   - Memory (MB)
   - Storage (GB)
   - Description
   - Reason for request
   All modifications change the daily and lease costs.
   When you are finished reviewing the settings, click **Submit**, and click **OK**.
7. Click **Request**.
What to do next

Wait for an approval from the assigned role, and provision your workload.

Provision the Workload

After you request the workload, you can provision the workload when you receive an approval.

Procedure

1. In the vCloud Automation Center portal, click Request to monitor status.
   
The workload request changes status several times during deployment. When it is finished, the request shows the status Successful.
   
   Workloads in the portal can be associated with third-party CMDB systems so that other roles in the company can approve the request before the workloads deploy. The request is coming from vCloud Automation Center through vCenter Orchestrator. Administrators can customize the details that are sent from vCloud Automation Center.

2. Click Items and click InventoryMgr-000 to review workloads requests.
   
The virtual machine is now deployed.

What to do next

You received an approval and successfully provisioned the workload. You can customize the virtual machine to adjust the amount of memory or other characteristics, so that the virtual machine performs better.

Customize the Virtual Machine

You requested and provisioned the virtual machine. You can customize the virtual machine to increase or decrease the amount of memory, the number of CPUs, and so on.

You perform the customization in the vCloud Automation Center portal. You cannot add more to the system than the amount permitted by the reservation policy for your organization.

Procedure

1. Review the VM configuration in the VM console.
   
   a. Click Connect Using VMRC to launch a remote connection to this virtual machine.

   To log in, you need valid credentials for the virtual machine.

2. Click Close.

3. Reconfigure the workload.
   
   a. Next to InventoryMgr-000, click the right arrow and select Edit.
   
   b. Increase the assigned memory.

   On the Execution tab, the default action is to immediately run the request and to shut down the virtual machine before reconfiguration.

   c. Click Submit to begin the reconfiguration task, and click OK.

4. Verify that memory is increased.

   When the status changes to On, click the VM and note the increased amount of memory.

What to do next

After you have customized the virtual machines to meet your requirements, you can snapshot the virtual machine to preserve your changes.
Manage Workload Snapshots

You deployed and configured the workload. You can create snapshots of your running workloads from the self-service portal.

Procedure

1. In the vCloud Automation Center portal, click Items and click Machines.
2. Click InventoryMgr-000 and click Snapshots.
3. Click New Snapshot.
4. Click Snapshot the machine's memory and click OK.
5. Wait for the snapshot creation to complete, and click Close.

You can view and delete existing snapshots on the Snapshots tab of the virtual machine.

What to do next

When you have performed the required task by using the provisioned virtual machine, you can archive it.

Retire the Virtual Machine

The final stage in the lifecycle of a workload is the retirement operation. Alternatively, the tenant administrator can send a reclamation request to the owners of machines.

If a blueprint does not specify a lease period, machines are provisioned from that blueprint with no expiration date. If a blueprint specifies a single value for lease duration, machines are provisioned from that blueprint with an expiration date based on the blueprint lease duration.

Procedure

1. In the vCloud Automation Center portal, click Machines.
2. Click InventoryMgr-000.
3. Click Destroy and confirm the operation.

You requested, provisioned, customized, and retired a workload.

Application Provisioning

You can use vCloud Director, vCloud Automation Center and vCloud Automation Center Application Services to provision applications to a vCloud environment.

Using vCloud Automation Center Application Services (Application Services), you must register a cloud provider and template. When you register a cloud provider, you map a specific vCloud Automation Center blueprint in a provisioning or business group to a cloud template in Application Services. The registration process makes the vCloud Automation Center blueprint available in the Application Services catalog. To deploy an application using this cloud template, you must map a cloud template to a logical template. You then create a deployment environment that you map to an applicable vCloud Automation Center reservation policy.
Figure 4-3. Platform-as-a-Service workflow

A functional Platform-as-a-Service (PaaS) environment is based on several components.

Table 4-5. vCloud Suite Components Required for the Platform-as-a-Service

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>VMware bare-metal hypervisor that lets you run a virtualized environment.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Provides management capabilities in a browser-based interface, and integration points for other vCloud Suite components.</td>
</tr>
<tr>
<td>vCenter Orchestrator</td>
<td>Enables you to create workflows that automate activities in the data center.</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>Provides a secure portal through which authorized administrators, developers, or business users can request new IT services.</td>
</tr>
</tbody>
</table>
Table 4-5. vCloud Suite Components Required for the Platform-as-a-Service (Continued)

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Automation Center Application Services</td>
<td>A model-based application provisioning solution that simplifies creating and standardizing application deployment topologies on multiple infrastructure clouds. Application architects use a graphic-based canvas with a drag-and-drop interface to model application deployment topologies called application blueprints. Application Services was known formerly as VMware vCloud Application Director.</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>vCloud Director lets you provision services as virtual data centers with virtualized compute, networking, storage, and security.</td>
</tr>
</tbody>
</table>

The following example objects are used in the scenario:

Table 4-6. Sample Environment Details

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACME Corp. Development organization</td>
<td>The business group owning and deploying the application.</td>
</tr>
<tr>
<td>vCAC 6.1 Cloud provider for ACME Corp</td>
<td>A cloud provider in vCloud Director that is registered with Application Services.</td>
</tr>
<tr>
<td>ACME Corp Deployment Environment</td>
<td>The deployment environment to which you will map a vCloud Director virtual datacenter (vDC).</td>
</tr>
<tr>
<td>CentOS6 64bit</td>
<td>The name of the logical template used to map application blueprints to Application Services.</td>
</tr>
<tr>
<td>Acme-DB</td>
<td>The database component that serves as the back-end datastore for the ACME Corp application.</td>
</tr>
<tr>
<td>Acme-AppSrv</td>
<td>The application server that serves as the middle-tier application processing component for the ACME Corp application.</td>
</tr>
<tr>
<td>Acme-Web</td>
<td>The Web server that serves as the front-end component for the ACME Corp application, providing content to be rendered by a Web browser as the interface for the end user of the application.</td>
</tr>
</tbody>
</table>

Prerequisites

Verify that the following conditions are met.

- You have the required components in your environment.
- You have a configured vSphere instance to serve as an vCloud Automation Center endpoint.
- You have set a reservation policy within vCloud Automation Center.
- Create cloud templates in vCloud Director or vCloud Automation Center that meet the requirements for working properly in Application Service.
- Verify that at least one vCloud Director cloud provider is registered in Application Service.
- Verify that virtual machine templates that meet Application Service requirements have been created.
- When you map cloud templates for a cloud provider in Application Service, verify that the vCloud Director template that you are mapping to is a single virtual machine. Templates with multiple virtual machines cannot be registered to a Application Service cloud provider.
Verify that the vCloud organization that you plan to use with Application Service is created and configured with organization administrator privileges.

**Procedure**

1. **Register the Cloud Provider** on page 66
   Application Services registers a cloud provider by connecting to a vCloud Director instance and organization. As the cloud administrator for ACME Corp, you will register a cloud provider for the ACME Corp Development organization.

2. **Create a vCloud Director Deployment Environment** on page 67
   You must map a deployment environment to a vCloud Director organization provider virtual datacenter (vDC) before you can deploy your application.

3. **Add a Logical Template to the Catalog** on page 68
   As a cloud administrator for ACME Corp, you create logical templates that map application blueprints in vCloud Automation Center Application Services and vCloud Automation Center. Logical templates allow an application blueprint to remain cloud agnostic.

4. **Create an Application** on page 69
   With vCloud Automation Center Application Services, you can model your application deployment, create dependencies, and edit the application configurations.

5. **Create an Application Blueprint** on page 70
   The application blueprint provides detailed control over installation dependencies, configuration changes, and editable scripts. Application Services generates execution plans from the blueprint that you use to deploy applications to your vCloud environment.

6. **Deploy the Application** on page 74
   Deploy the ACME Corp application from the Application Services user interface.

---

**Register the Cloud Provider**

Application Services registers a cloud provider by connecting to a vCloud Director instance and organization. As the cloud administrator for ACME Corp, you will register a cloud provider for the ACME Corp Development organization.

A vCloud Automation Center business group associates users with a set of services and resources, often corresponding to a business, department, or other organizational unit. Each business group can have access to one or more vCloud Automation Center blueprints used to request machines. These blueprints can belong to one or more business groups.

In this task, you will register a cloud provider and associate it with the ACME Corp Development organization.

**Prerequisites**

- Verify that the user account has the **ROLE_CLOUD_ADMIN** cloud administrator role assigned to it.

**Procedure**

1. Open a Web browser and log into vCloud Director as the cloud administrator for ACME Corp.
2. Click **Applications > Clouds > Cloud Providers**.
3. Click **New** to create a new cloud provider.
4 Complete the cloud provider information.
   a Type vCAC 6.1 Provider for ACME Development in the Description field.
      Include the vCloud Director organization name in either of these fields. The text from these fields
      appears in the Deployment Profile wizard under the Cloud Provider column.
   b Select vCAC 6.1 for the Cloud Provider type.
   c Type https://paas.acme.corp.com for the cloud hostname.
      The cloud IP or host name must match the IP address or host name of the vCloud Director instance.
   d Select ACME Corp Development from the Business Group drop-down menu.
   e Type credentials for an organization user with organization administrator privileges for that
      organization.
      This user must not be the vCloud Director system administrator.
5 Click Save to register the cloud provider.

The cloud provider vCAC 6.1 Provider for ACME Development is registered and available for use in
Application Services.

What to do next
Create a deployment environment to deploy an application to the vCloud Director environment. See
“Create a vCloud Director Deployment Environment,” on page 67.

Create a vCloud Director Deployment Environment

You must map a deployment environment to a vCloud Director organization provider virtual datacenter
(vDC) before you can deploy your application.

A vDC combines the compute and memory resources of a single vCenter Server resource pool with the
storage resources of one or more datastores connected to that resource pool. vCloud Director vDCs provide
an environment where virtual systems can be stored, deployed, and operated. For example, you might have
separate deployment environments for development, testing, staging, and production. For vCloud Director,
a deployment environment is mapped to an organization virtual datacenter (organization vDC).

The organization vDC is a deployment environment for virtual systems owned by the containing
organization (in this scenario the containing organization is the ACME Corp. Development organization),
and an allocation mechanism for resources such as networks, storage, CPU, and memory. In an organization
vDC, computing resources are fully virtualized, and can be allocated based on demand, service level
requirements, or a combination of the two.

Prerequisites
- Verify that your user account has the ROLE_CLOUD_ADMIN cloud administrator role assigned to it.
- Verify that an organization vDC is created and configured in the vCloud Director organization. The
  Application Services deployment environment is equivalent to the organization vDC in
  vCloud Director.
- For information on integrating vCloud Director in an existing
  vCloud Automation Center Application Services deployment, see IaaS Configuration for vCloud Director.

Procedure
1 Open a Web browser and log into Application Services as an application cloud administrator for
   ACME Corp.
2 Click Applications > Clouds > Deployment Environment.
3 Click **New** to create a new deployment environment.

4 Complete the deployment environment information.
   a Type **ACME Corp Deployment Environment** in the Name and Description fields.
      The text from these fields appears in the Deployment Profile wizard under the Deployment Environment column.
   b Select vCAC 6.1 from the **Cloud Provider** drop-down menu.
      This is the cloud provider to associate with this deployment environment.
   c Click **Select**, and click the radio button **Select from the list of reservation policies** in the pop-up window that displays. Select **vSphere** from the list of available reservation policies. This corresponds to the reservation policy set in vCloud Automation Center.

5 Select an organization vDC and click **OK**.
   A vCloud Director organization vDC is mapped to the ACME Corp Deployment Environment deployment environment within Application Services.

6 Click **Save**.

The ACME Corp Deployment Environment is added to the list of deployment environments that you can select from when you create a deployment profile.

What to do next

You can add a Add a Logical Template to the Catalog. See “Add a Logical Template to the Catalog,” on page 68.

### Add a Logical Template to the Catalog

As a cloud administrator for ACME Corp, you create logical templates that map application blueprints in vCloud Automation Center Application Services and vCloud Automation Center. Logical templates allow an application blueprint to remain cloud agnostic.

Templates let you keep cloud resources and Application Services artifacts decoupled. For example, as a cloud administrator, you can update a template in the catalog, and if you want to use the updated template, you simply change the mapping between application blueprints in Application Services and vCloud Automation Center. By re-mapping your blueprints, you avoid having to update your organization's blueprints, services, and deployment environment.

### Prerequisites
- Log in to vCloud Automation Center Application Services as an **application cloud administrator** and an **application publisher and deployer**.
- Create cloud templates in vCloud Director or vCloud Automation Center that meet the requirements for working properly in Application Services.
- Verify that the vCAC 6.1 Provider for ACME Corp cloud provider is registered and available for use vCloud Automation Center Application Services. See “Register the Cloud Provider,” on page 66.

### Procedure
1 Open a Web browser and log into Application Services as an **application cloud administrator** for ACME Corp.
2 On the Application Service title bar, click the drop-down menu and select **Library > Logical Templates**.
3 Click **New**.
4 Type CentOS 64bit as the name of the logical template, ACME Corp Deployment Environment as the description, and click Save.

To keep track of which cloud template or operating system you are using, include the name of the cloud template or operating system.

5 Click Create LT Version to create a logical template version.

You can create multiple versions of a logical template.

A page opens for creating a logical template version.

6 Complete the template version information.

   a The logical template version name remains CentOS 64bit.

   b Add the following tags to the ACME Corp logical template: Application Servers, Database Servers, Messaging Servers, OS Templates, and Web Servers.

You categorize logical templates based on the functions that they provide. Application Service organizes templates based on tags you see when you create a deployment blueprint for an application.

   c Select CentOS 6.3.0 from the Supported OS drop-down list.

Specifies the operating system installed in the logical template. This OS information is used in the application blueprint to limit which services you can add to this template. Not all services run on all operating systems. For example, if you specify a CentOS operating system, when you use this template in a blueprint and try to add a service that is not compatible with CentOS, Application Service prevents you from adding that service.

7 Map the cloud template to the CentOS6 64bit logical template.

   a In the Cloud Provider Name column, click the down arrow and select vCAC 6.1 Provider for ACME Corp from the list of cloud providers that appears. This is the cloud provider you registered earlier in this use case.

   b In the Cloud Template column, click the down arrow and select the CentOS_6.3_x64 cloud template.

Cloud templates that belong to the same group as the application cloud administrator for ACME Corp. appear in the drop-down menu. If the list of cloud templates is empty, the existing cloud templates do not belong to your group or a cloud template was not registered.

8 When you finish creating the template, click Save.

The logical template CentOS 6.3.0 is added to the Logical Templates page. The template also appears in the list of logical templates that you can include when you create a deployment blueprint for your application.

What to do next

Create an application to deploy. See “Create an Application,” on page 69.

Create an Application

With vCloud Automation Center Application Services, you can model your application deployment, create dependencies, and edit the application configurations.

The tasks you have completed so far in this use case must be performed so that anyone in your organization using Application Services has a cloud target to which they can deploy an application. The applications you create using Application Services typically consist of multiple tiers. For example, a three-tier application consisting of a Web server front-end, an application server in the middle-tier, and a database in the back-end. Each application tier can use a different operating system, as well as have different services installed.
In practice you would develop each tier within an application and map it to a guest operating system. For the purpose of this use case scenario, we assume that the application components have been created by the application architect, and are available for you to add to the application blueprint created in the following task. The following procedure outlines the high level steps necessary to create an application component.

Prerequisites

- Log in to Application Service with a user account that has the application architect role ROLE_APP_ARCHITECT assigned to it.

Procedure

1. Open a Web browser and log into Application Services as a user with the application architect role for ACME Corp.
2. Click Applications > Create New Application.
3. Type ACME-Application in the Name text box.
4. (Optional) Enter a description of the application in the Description text box.
5. Select ACME Corp Development in the Business Group drop-down menu. This is the business group that has ownership of the application.
6. Select Private in the Sharing drop-down menu to specify the sharing status of the application. This restricts access of the ACME-Application to members of the ACME Corp Development organization.
7. Click Save.

What to do next

Create an application blueprint from which to deploy your application. See “Create an Application Blueprint,” on page 70.

Create an Application Blueprint

The application blueprint provides detailed control over installation dependencies, configuration changes, and editable scripts. Application Services generates execution plans from the blueprint that you use to deploy applications to your vCloud environment.

Blueprints allow an end user to deploy an application without knowing the underlying datacenter infrastructure. The end user selects the type of cloud into which they want to deploy the application, such as a vCloud Automation Center or vCloud Director cloud. Similarly, system administrators can set up cloud deployment targets without a detailed understanding of the application architecture. For these reasons the role of the application architect is critical, as those in this role are most familiar with the end user requirements, and the cloud infrastructure needed to meet those requirements.

You model and create applications in the blueprint canvas. On the left side of the blueprint canvas are the logical templates from the Application Services library. On the right is a list of the services available from the library and application components. You select a logical template and drag it to center of the blueprint canvas to model your application.

Prerequisites

- Verify that your application architect user account has the ROLE_APP_ARCHITECT role assigned to it.
- Verify that at least one application version is created in Application Services. See “Create an Application,” on page 69.
Procedure

1. Add a Database Back-End to the Application Blueprint on page 71
   Add a database to the application blueprint to serve as the ACME Corp application’s back-end datastore.

2. Add a Middle-Tier Application Server to the Application Blueprint on page 72
   Add an application server to the ACME Corp. application blueprint.

3. Add a Front-End Web Server to the Application Blueprint on page 73
   Add a Web server to the ACME Corp. application blueprint to serve as the front-end of the application.

Add a Database Back-End to the Application Blueprint

Add a database to the application blueprint to serve as the ACME Corp application’s back-end datastore.

Procedure

1. Log into Application Services as an application architect.

2. On the Application Services title bar, click the drop-down menu and select Applications.

3. Locate and select the ACME-Development application and open the application version.
   To locate applications, type the name of the application in the Search field, and press Enter.

4. Click Create Blueprint to create an application blueprint.
   The canvas for modeling the application blueprint appears.

5. Select and drag the logical template labeled CentOS6 64bit v1.0.0 listed in the Logical Templates > Database Servers pane to the canvas.
   For example, to create a three-tiered application, you might drag one template from the OS Templates list, one item from the Database Servers list, and one from the Application Servers list. The names of the lists correspond to the tags associated with a template.

6. Select the CentOS6 64bit v1.0.0 node on the canvas and modify the properties of the node on the Details tab below the blueprint using the following values.
   a. Change the name of the node on the Details tab below the blueprint to Acme-DB.
      If the node name contains a character other than a letter, digit, underscore, or hyphen, that character is replaced with a hyphen.
   b. Type Acme-DB in the Host Name text box.
      This host name serves as an identifier for the virtual machine computer name in its network. If the host name text box is left blank, Application Services generates a host name using random characters.
   c. Change the default number of CPUs to 2.
   d. Specify 2048 MB of memory.
      It is important to allocate enough memory, as insufficient compute resources can cause the deployment to fail.
   e. Type Compute resources for Acme-DB. in the Description text box.
7 Select and drag the MySQL service from the Services panel onto the Acme-DB node.

If a service or application component is not compatible with a particular node, you cannot drop it on the node. For example, you can drag the application component called SQL SCRIPT onto a MySQL database service, but you cannot drag the SQL SCRIPT component onto a JBoss application server service.

Compatibility restrictions are created when the application catalog administrator sets the supported operating systems and components for a library service. The application catalog administrator can also add to the list of operating systems and tags that are already available in the library. For example, the MySQL service in the library has the supported components listed as SQL SCRIPT. Only the SQL SCRIPT application component type can be added to the MySQL service.

**NOTE** If any preinstalled services are added to a logical template after you create a blueprint, the new preinstalled services are not added to the node. In this case, you must recreate the node and add the preinstalled services.

8 Click **Save**.

You have added a database for use as a datastore with the ACME Corp Development organization's application.

**What to do next**

Add an application server to the application blueprint. See “Add a Middle-Tier Application Server to the Application Blueprint,” on page 72.

**Add a Middle-Tier Application Server to the Application Blueprint**

Add an application server to the ACME Corp. application blueprint.

**Prerequisites**

Verify that you are logged into Application Services as an application architect.

**Procedure**

1 On the Application Services title bar, click the drop-down menu and select **Applications**.

2 Select and drag the logical template labeled CentOS6 64bit v1.0.0 listed in Logical Templates > Application Servers to the canvas.

3 Select the CentOS6 64bit v1.0.0 node on the canvas and modify the properties of the node on the Details tab below the blueprint using the following values.

   a Change the name of the node on the Details tab below the blueprint to **Acme-AppSrv**.

      If the node name contains a character other than a letter, digit, underscore, or hyphen, that character is replaced with a hyphen.

   b Type **Acme-AppSrv** in the Host Name text box.

   c Change the default number of CPUs to 1.

   d Specify 1024 MB of memory.

   e Type **Compute resources for Acme Corp. development application server**. in the Description text box.

4 Click the **Convert to Node Array** icon to create a cluster.

For scaling deployments, you might need to deploy multiple virtual machines or a cluster for a particular node and use a load balancer to manage them.
5 Type 2 in the Cluster Size text box.
   By specifying a cluster size of 2, the application blueprint will deploy two middle-tier application servers.

6 Select and drag the JBoss service from the Services panel onto the Acme-AppSrv node.

7 Specify the IP address properties for the application server.
   a Select the Properties tab, and click the pencil icon next to the tcs_nodes_ip property name.
      The Edit Property dialog box displays.
   b Select the third radio button beneath the Blueprint Value label.
   c Select all(acme-appsrv:ip) from the drop-down menu.
      The application server has two nodes, and requires a corresponding number of IP addresses.
      Specifying the all(appserver:ip) property makes all application server nodes aware of sibling nodes.
   d Click Save.

8 Specify the node_index properties for the application server.
   a Select the Properties tab, and click the pencil icon next to the node_index property name.
      The Edit Property dialog box displays.
   b Select the third radio button beneath the Blueprint Value label.
   c Select self:node_array_index from the drop-down menu.
      If the node index is zero (0), you must create and initialize your database using sample data, and run the initialization on the first middle tier application server (the server whose index is zero).
      Failing to do this will cause all of the middle tier servers to initialize against the database simultaneously, which might cause performance degradation.
   d Click Save.

9 Create a relation between the application server and database in the blueprint.
   a Click the Add Relation button.
   b Select the Acme-AppSrv node, and then select the Acme-DB node.
      Some of the properties you specified as part of the database configuration, such as the db_ip property, auto-populate their complementary properties in the application server component.

10 Click Save.

You have added an application server to the application blueprint, and created a relationship between it and the database.

**What to do next**

Add a Web server front-end to the application blueprint. See “Add a Front-End Web Server to the Application Blueprint,” on page 73.

**Add a Front-End Web Server to the Application Blueprint**

Add a Web server to the ACME Corp. application blueprint to serve as the front-end of the application.

**Prerequisites**

Verify that you are logged into Application Services as an application architect.

**Procedure**

1 On the Application Services title bar, click the drop-down menu and select Applications.
2 Select and drag the logical template labeled CentOS6 64bit v1.0.0 listed in Logical Templates > Web Servers to the canvas.

3 Select the CentOS6 64bit v1.0.0 Web server node on the canvas and change the following properties of the node on the Details tab below the blueprint using the following values.
   a Change the name of the node on the Details tab below the blueprint to Acme-Web.
   b Type Acme-Web in the Host Name text box.
   c Change the default number of CPUs to 1.
   d Specify 512 MB of memory.

4 Select and drag the Frontend service from the Services panel onto the Acme-Web node.

5 Create a relation between the web server and application server in the blueprint.
   a Click the Add Relation button.
   b Select the Acme-Web node, and then select the Acme-AppSrv node.

6 Click Save.

You have added a Web server to the application blueprint, and created a relationship between it and the JBoss application server. You have successfully created a blueprint from which you can deploy the ACME Corp application.

What to do next
You can now deploy the application. See “Deploy the Application,” on page 74.

Deploy the Application

Deploy the ACME Corp application from the Application Services user interface.

Application Services simplifies and automates deployments of multi-tier enterprise applications in hybrid cloud environments.

Prerequisites
- Log in to Application Services as an application publisher and deployer.
- Verify that at least one deployment profile is available in Application Services.

Procedure
1 On the Application Services title bar, click the drop-down menu and select Applications.
2 Locate the ACME Corp application.
3 Select the appropriate application version and click the Add icon (the plus sign).
   A selection menu appears.
4 Select Create Deployment Profile from the menu.
   Follow the prompts in the Deployment Profile wizard and make any necessary changes.
5 Type ACME-Dev-App as a name for the deployment profile
   When naming a profile, you might consider a name that indicates which type of environment is used, specific override properties, or clustered node configuration. For example, if the ACME Corp application were for QA, you might name the profile ACME-App-QA to indicate that this profile is for the QA environment rather than for the development or production environment.
6 Review the deployment profile settings.
7 Click **Deploy**.

The Deployment Profile wizard appears, with the Deployment Environment page highlighted.

8 Select the ACME Corp Deployment Environment from the list and click **Map Details**.

Notice that the application uses the CentOS6 64bit logical template you created earlier in this use case example.

9 Click **Next** to navigate to the Application Properties page.

Review the properties you specified for each node in the application blueprint, and confirm that the values you entered for hostname, memory, and CPU are correct.

10 Click **Next** to navigate to the Execution Plan page.

Review the provisioning tasks, components, and dependencies in the execution plan.

11 Click **Next** to review the deployment profile settings.

12 Click **Save**.

13 Click **OK**.

The deployment profile is listed for the application version.

14 Click **Deploy**.

A deployment summary page appears and refreshes approximately every 30 seconds to display the deployment status.

It can take a considerable amount of time for an application to deploy depending upon its complexity, and the number of components included in the application. The deployment process must create virtual machines and provision software in those virtual machines.

**What to do next**

To understand the deployment process so that you can easily identify and troubleshoot any deployment failures, see “Understanding the Deployment and Update Process” in the VMware vCloud Automation Center Application Services documentation center.

**Highly Available vCenter Single Sign-On Deployment**

As a system administrator in ACME Corporation, who deploys a wide range of vCloud Suite components you must deploy vCenter Single Sign-On to achieve simple and secure authentication.

In this scenario, you are going to deploy the VMware recommended highly available option consisting of two vCenter Single Sign-On instances placed behind an industry standard network load balancer. This deployment gives you a validated enterprise-ready design to reduce the authentication load of multiple vCloud Suite products.
In your data center, you can use the vCenter Single Sign-On solution as an SSO site pair for placement behind an industry standard network load balancer. You can use a fully qualified domain name with a virtual IP to front all registrations to vCenter Single Sign-On to provide an authentication endpoint. The network load balancers, in this scenario, are also available as virtual appliances that let you virtualize the whole deployment.

A centralized Single Sign-On solution has multiple benefits.

- A shared and standardized authentication service for multiple products.
- An authentication process with fewer components to reduce resource requirement and footprint.
- Reduced dependency on other Single Sign-On solutions.

Placing your SSO servers behind a network load balancer provides several additional benefits.

- Distribution of authentication requests and workload.
- Authentication availability if a vCenter Single Sign-On server becomes unavailable.
- The ability to increase authentication compute by adding additional Single Sign-On servers into the load-balanced pool.

### Table 4-7. Required vCloud Suite Components for This Scenario

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>5.5 Update 2</td>
<td>The VMware bare-metal hypervisor that lets you run a virtualized environment.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>5.5 Update 2</td>
<td>The installation of vCenter Single Sign-On is a component of vCenter Server installer.</td>
</tr>
</tbody>
</table>
### Table 4-8. Optional vCloud Suite Components for This Scenario

<table>
<thead>
<tr>
<th>vCloud Suite component</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Data Protection</td>
<td>5.8</td>
<td>Provides advanced data protection with backup and recovery to disk via VMware vSphere with Operations Management Data Protection features.</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>6.1</td>
<td>Provides functionality for deploying and provisioning of business-relevant cloud services across private and public clouds, physical infrastructure, hypervisors, and public cloud providers.</td>
</tr>
<tr>
<td>vCenter Orchestrator</td>
<td>5.5.2.1</td>
<td>Provides the capability to create workflows that automate activities such as provisioning virtual machine, performing scheduled maintenance, initiating backups, and many others.</td>
</tr>
</tbody>
</table>

### Table 4-9. Required Scenario Environment Details

<table>
<thead>
<tr>
<th>Object</th>
<th>Host Name</th>
<th>FQDN</th>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer SSO</td>
<td>SSO</td>
<td>sso.acme.local</td>
<td>192.168.110.40</td>
<td>Industry standard load balancer.</td>
</tr>
<tr>
<td>vCenter Server VC</td>
<td>VC</td>
<td>vc.acme.local</td>
<td>192.168.110.45</td>
<td>Microsoft Server 2012 R2 virtual machine for vCenter Server installation. You also register your load balancer with the vCenter Server instance.</td>
</tr>
<tr>
<td>Active Directory CONTROL CENTER</td>
<td>controlcenter.a acme.local</td>
<td>192.168.110.10</td>
<td>Microsoft Server 2012 R2 with Active Directory Domain Services and installed certificate authority role service. You use the service to generate signed certificates that are needed for the trusted connection between the load balancer and the SSO servers.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4-10. Optional Scenario Environment Details

<table>
<thead>
<tr>
<th>Object</th>
<th>Host Name</th>
<th>FQDN</th>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Data Protection VM</td>
<td>VDP</td>
<td>vdp.acme.local</td>
<td>192.168.110.46</td>
<td>vSphere Data Protection appliance VM.</td>
</tr>
<tr>
<td>vCloud Automation Center instance</td>
<td>VCAC</td>
<td>vcac.acme.local</td>
<td>192.168.110.47</td>
<td>vCloud Automation Center appliance VM.</td>
</tr>
<tr>
<td>vCenter Orchestrator instance</td>
<td>VCO</td>
<td>vco.acme.local</td>
<td>192.168.110.48</td>
<td>vCenter Orchestrator instance. You can select between a standalone Windows deployment and a VM appliance deployment.</td>
</tr>
</tbody>
</table>
### Table 4.11. Load Balancers in This Scenario

<table>
<thead>
<tr>
<th>Load Balancer</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware NSX™ with VMware NSX Edge™</td>
<td>6.1.1</td>
<td>VMware NSX is a software networking and security virtualization platform that delivers the operational model of a virtual machine for the network. NSX Edge provides network edge security and gateway services to isolate a virtualized network.</td>
</tr>
<tr>
<td>F5 BIG-IP with Local Traffic Manager</td>
<td>11.6.0</td>
<td>F5 BIG-IP provides intelligent traffic management.</td>
</tr>
<tr>
<td>VMware vCloud® Networking and Security Edge™</td>
<td>5.5.3.1</td>
<td>VMware vCloud Networking and Security Edge provides firewall protection, traffic analysis, and network perimeter services to protect your vCenter Server virtual infrastructure.</td>
</tr>
</tbody>
</table>

### Table 4.12. Additional Required Software for Download

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win32 OpenSSL Software version 0.9.8zc</td>
<td>Win32 OpenSSL is used to generate certificate requests. Software version 0.9.8zc is required to successfully complete this scenario.</td>
</tr>
<tr>
<td>Microsoft Visual C++ 2008 Redistributable Package 32bit</td>
<td>OpenSSL has a dependency on this software package.</td>
</tr>
<tr>
<td>JXplorer</td>
<td>JXplorer is used to connect to LDAP on the second vCenter Single Sign-On server and to remove attributes that are not needed when a load balancer is used.</td>
</tr>
<tr>
<td>Java Runtime Environment</td>
<td>JXplorer has a dependency on this software package.</td>
</tr>
</tbody>
</table>
Figure 4-5. Single Sign-On Deployment Workflow

- Start
- Prepare Virtual Machines for vCenter Single Sign-On Installation
- Install the First vCenter Single Sign-On Instance
- Install the Second vCenter Single Sign-On Instance
- Generate SSL Certificates with OpenSSL to Reflect Load Balancer Entry Point
- Configure the First SSO Server to use the Signed Certificates
- Configure the Second SSO Server to use the Signed Certificates
- Install and configure vCenter Server to work with External SSO
- Configure the Load Balancer
- Test Your Environment
- Configure vCloud Suite Products to use the Virtual IP of the Load Balancer as SSO
- End
Procedure

1. **Prepare Virtual Machines for vCenter Single Sign-On Installation** on page 80
   Before you proceed to vCenter Single Sign-On installation, you must install required software on SSO Server A and SSO Server B virtual machines.

2. **Install the First vCenter Single Sign-On Instance** on page 82
   You have installed all the software that vCenter Single Sign-On needs, and can proceed with the installation of the first vCenter Single Sign-On instance on SSO Server A.

3. **Install the Second vCenter Single Sign-On Instance** on page 82
   You have installed your first vCenter Single Sign-On instance. Proceed with the installation of the second SSO server and pair it to the first to work in high availability mode.

4. **Generate SSL Certificates by Using OpenSSL** on page 83
   After you have successfully installed vCenter Single Sign-On servers, you must update their certificates to reflect the load balancer entry point. You use OpenSSL to prepare a request and Microsoft certificate authority (CA) as a trusted root authority to generate a signed certificate.

5. **Configure the First vCenter Single Sign-On Server to Use the Signed Certificates** on page 85
   After you have generated signed certificates, configure your first vCenter Single Sign-On server to use the certificates.

6. **Configure the Second vCenter Single Sign-On Server to Use the Signed Certificates** on page 88
   After you have configured your first vCenter Single Sign-On server, you must copy the certificates to the second vCenter Single Sign-On server and reconfigure the server to use these certificates.

7. **Install vCenter Server and Configure It to Use External vCenter Single Sign-On** on page 90
   After both vCenter Single Sign-On servers are installed and configured, you must install a vCenter Server that will later be paired with your load balancer.

8. **Configure the Load Balancer** on page 92
   After you have configured both your SSO servers, you must configure your load balancer to manage the load to the SSO servers.

   After you have deployed and configured all nodes, you must test your highly available vCenter Single Sign-On deployment.

10. **Configure vCloud Suite Products to Use the Virtual IP as vCenter Single Sign-On** on page 100
    When the load balancer is fully configured as an entry point for all requests to the vCenter Single Sign-On, you can configure other vCloud Suite products to use the virtual IP of the load balancer as their SSO.

Prepare Virtual Machines for vCenter Single Sign-On Installation

Before you proceed to vCenter Single Sign-On installation, you must install required software on SSO Server A and SSO Server B virtual machines.

Prerequisites

Verify that both VMs are running Microsoft Server 2012 R2 and meet the minimum hardware requirements.

<table>
<thead>
<tr>
<th>vCenter Single Sign-On Hardware</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel or AMD x64 processor with two or more logical cores, each with a speed of 2 GHz.</td>
</tr>
<tr>
<td>Memory</td>
<td>3 GB</td>
</tr>
<tr>
<td>vCenter Single Sign-On Hardware</td>
<td>Minimum Requirement</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Disk storage</td>
<td>2 GB</td>
</tr>
<tr>
<td>Network speed</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Procedure**

   
   The component is needed for correct operation of Open SSL.

2. On both virtual machines, install Win32OpenSSL version 0.9.8zc, leaving the default values.

   
   a. Create the folders `C:\certs\sso`.
   
   b. Create a text file `C:\certs\sso\sso.cfg` with the following content:

   ```
   [ req ]
   default_bits = 2048
   default_keyfile = rui.key
   distinguished_name = req_distinguished_name
   encrypt_key = no
   prompt = no
   string_mask = nombstr
   req_extensions = v3_req
   
   [ v3_req ]
   basicConstraints = CA:FALSE
   keyUsage = digitalSignature, keyEncipherment, dataEncipherment
   extendedKeyUsage = serverAuth, clientAuth
   subjectAltName = DNS:sso1, DNS:sso1.acme.local, DNS:sso2, DNS:sso2.acme.local, DNS:sso.acme.local, IP:192.168.110.40
   
   [ req_distinguished_name ]
   countryName = US
   stateOrProvinceName = California
   localityName = Palo Alto
   0.organizationName = ACME
   organizationalUnitName = vCenterSSO
   commonName = sso.acme.local
   ```

   Highlighted text is specific for the environment of the current scenario.

4. On SSO Server B, install the Java Runtime Environment with the default values.

5. On SSO Server B, install JXplorer with the default values.

**What to do next**

Install the first vCenter Single Sign-On instance and apply load balancer entry point in the configuration files.
Install the First vCenter Single Sign-On Instance

You have installed all the software that vCenter Single Sign-On needs, and can proceed with the installation of the first vCenter Single Sign-On instance on SSO Server A.

Procedure

1. Connect the vCenter Server ISO image to the sso1.acme.local virtual machine.
2. Log in to sso1.acme.local as an administrator.
3. Open the CD-ROM drive and double-click the autorun.exe file to start the vCenter Server installation wizard.
4. Select the vCenter Single Sign-On option under Custom Install, and click Install.
5. Follow the prompts of the installation wizard until vCenter Single Sign-On Information page appears, and select Standalone vCenter Single Sign-On.
6. Enter and confirm a password for the administrator@vsphere.local account.
   By default, the password must have at least eight characters, at least one lowercase character, one uppercase character, one number, and one special character. The password must not contain non-ASCII characters or exclamation mark (!).
7. On the vCenter Single Sign-On Configure Site page, enter Palo Alto as site and follow the prompts until the installation process is complete.
8. Edit the vCenter Single Sign-On configuration files to apply the load balancer entry point.
   a. Edit the C:\ProgramData\VMware\CIS\cfg\vmware-sso\hostname.txt file.
   b. Replace the hostname value with sso.acme.local.
      You must use the FQDN of the load balancer for the hostname value.
   c. Edit the C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\server.xml file.
   d. Locate the <Connector SSLEnabled="true"> element.
   e. Add two new attributes:
      proxyName="sso.acme.local"
      proxyPort="7444"

What to do next

Install the second vCenter Single Sign-On instance and apply load balancer entry point in the configuration files.

Install the Second vCenter Single Sign-On Instance

You have installed your first vCenter Single Sign-On instance. Proceed with the installation of the second SSO server and pair it to the first to work in high availability mode.

Procedure

1. Connect the vCenter Server ISO image to the sso2.acme.local virtual machine.
2. Log in to sso2.acme.local as an administrator.
3. Open the CD-ROM drive and double-click the autorun.exe file to start the vCenter Server installation wizard.
4. Select the vCenter Single Sign-On option under Custom Install, and click Install.
Follow the prompts of the installation wizard until vCenter Single Sign-On Information page appears, and select **High Availability**, and click **Next**.

Pairing of both servers must be over a local network a WAN connection should not be used.

6 Enter `sso1.acme.local` as the partner host to replicate from, enter the password set for the administrator@vsphere.local account and click **Next**.

7 Accept the host certificate and click **Next**.

8 On the vCenter Single Sign-On Configure Site page, select **Palo Alto** as site and follow the prompts until the installation process is complete.

9 Edit the vCenter Single Sign-On configuration files to apply the load balancer entry point.
   a Edit the `C:\ProgramData\VMware\CIS\cfg\vmware-sso\hostname.txt` file.
   b Replace the hostname value with `sso.acme.local`.
      You must use the FQDN of the load balancer for the hostname value.
   c Edit the `C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\server.xml` file.
   d Locate the `<Connector SSLEnabled="true">` element.
   e Add two new attributes:
      
      ```
      proxyName="sso.acme.local"
      proxyPort="7444"
      ```

You have successfully deployed two linked vCenter Single Sign-On servers that are part of the same vsphere.local security domain.

**What to do next**

Generate SSL certificates and use Certificate Authority to sign them.

**Generate SSL Certificates by Using OpenSSL**

After you have successfully installed vCenter Single Sign-On servers, you must update their certificates to reflect the load balancer entry point. You use OpenSSL to prepare a request and Microsoft certificate authority (CA) as a trusted root authority to generate a signed certificate.

**Prerequisites**

You must configure a new Certificate Authority (CA) template based on the Web Server template that has **Data Encipherment** enabled. By default, the Web Server template in Microsoft Windows Server does not include **Data Encipherment**, which is a requirement of vCenter Single Sign-On for generated certificates. For information about configuring the required template, see the VMware knowledge base article [http://kb.vmware.com/kb/2062108](http://kb.vmware.com/kb/2062108).

**Procedure**

1 Log in to sso1.acme.local as an administrator.

2 In a command prompt, navigate to the `bin` directory of OpenSSL.
   ```
   cd \OpenSSL\bin
   ```

3 Create a certificate request and export the private key.
   ```
   openssl req -new -nodes -out c:\certs\sso\rui.csr -keyout c:\certs\sso\rui-orig.key -config c:\certs\sso\sso.cfg
   ```

4 Convert the private key in RSA format.
   ```
   openssl rsa -in c:\certs\sso\rui-orig.key -out c:\certs\sso\rui.key
   ```
5. Save a local copy of the root certificate of your CA.
   a. Open a browser window and log in as domain administrator in the CA.
   b. Download your CA root certificate with Base64 encoding.
   c. Save it as C:\certs\Root64.cer file.

6. Submit a request for a new certificate.
   a. Open the private key C:\certs\sso\rui.csr with Notepad and copy the contents to your clipboard.
   b. Return to the browser window where you are logged to the CA.
   c. Go to the home page and click **Request a certificate**.
   d. Click **advanced certificate request**.
   e. Paste the copied content in the **Saved Request** text box.
   f. Select the previously configured **VMware Certificate** template and click **Submit**.
   g. Select **Base 64 encoded** and click **Download certificate**.
   h. Save the file as C:\certs\sso\rui.crt.

7. In a command prompt, create a PKCS #12 archive file containing all certificates and keys.
   ```
   openssl pkcs12 -export -in c:\certs\sso\rui.crt -inkey c:\certs\sso\rui.key -certfile c:\certs\Root64.cer -name "ssoserver" -passout pass:changeme -out c:\certs\sso\ssoserver.p12
   ```

8. Navigate to the folder containing the Java configuration for the vCenter Single Sign-On.
   ```
   cd C:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components\bin\ 
   ```

9. Create a Java keystore file containing your certificates, and confirm the overwrite operation when prompted.
   ```
   keytool -v -importkeystore -srckeystore C:\certs\sso\ssoserver.p12 -srcstoretype pkcs12 -srcstorepass changeme -srckallas ssoserver -destkeystore C:\certs\sso\root-trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword
   ```

10. Add the root certificate to the Java keystore.
    ```
        keytool -v -importcert -keystore C:\certs\sso\root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -file C:\certs\Root64.cer -alias root-ca
    ```

11. Change the name of the Java keystore according to the vCenter Single Sign-On requirements.
    ```
        copy C:\certs\sso\root-trust.jks C:\certs\sso\server-identity.jks
    ```

**What to do next**

Configure your vCenter Single Sign-On servers to use the CA-signed certificates.
Configure the First vCenter Single Sign-On Server to Use the Signed Certificates

After you have generated signed certificates, configure your first vCenter Single Sign-On server to use the certificates.

Procedure

1. Log in to sso1.acme.local as an administrator, and in a command prompt, set the JAVA_HOME and PATH variables.
   ```shell
   set JAVA_HOME=C:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components
   set PATH=%PATH%;C:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso;%JAVA_HOME%\bin
   ```
2. Go to the OpenSSL directory and register the new root certificate in the VMware trust store.
   ```shell
   cd \OpenSSL\bin
   openssl x509 -noout -subject_hash -in C:\certs\Root64.cer
   ```
   From the output, copy the eight-digit hexadecimal value to the clipboard.
3. Create an SSL directory and copy the Root64.cer certificate to the SSL folder.
   ```shell
   mkdir c:\ProgramData\VMware\SSL
   copy C:\certs\Root64.cer C:\ProgramData\VMware\SSL\eight_digit_hexadecimal_value.0
   ```
4. Copy the Root64.cer file to the SSL folder and rename it.
   ```shell
   more C:\certs\Root64.cer >> C:\ProgramData\VMware\SSL\ca_certificates.crt
   ```
5 Open Notepad and create three text files in C:\certs to update the Security Token Service, Administrative Service, and Group Check Service of vCenter Single Sign-On so that they use the network load balancer virtual IP.

a Create C:\certs\admin.properties with the following content:

```
[service]
friendlyName=The administrative interface of the SSO server
version=1.5
ownerId=
productId=product:sso
type=urn:sso:admin
description=The administrative interface of the SSO server

[endpoint0]
uri=https://sso.acme.local:7444/sso-adminserver/sdk/vsphere.local
ssl=c:\certs\Root64.cer
protocol=vmomi
```

b Create C:\certs\gc.properties with the following content:

```
[service]
friendlyName=The group check interface of the SSO server
version=1.5
ownerId=
productId=product:sso
type=urn:sso:groupcheck
description=The group check interface of the SSO server

[endpoint0]
uri=https://sso.acme.local:7444/sso-adminserver/sdk/vsphere.local
ssl=c:\certs\Root64.cer
protocol=vmomi
```

c Create C:\certs\sts.properties with the following content:

```
[service]
friendlyName=STS for Single Sign On
version=1.5
ownerId=
productId=product:sso
type=urn:sso:sts

[endpoint0]
uri=https://sso.acme.local:7444/sts/STSService/vsphere.local
ssl=c:\certs\Root64.cer
protocol=wsTrust
```

6 List the vCenter Single Sign-On services.

```
ssolscli listServices https://sso1.acme.local:7444/lookupservice/sdk
```

The result displays services with additional information including their service name, service ID and value.
Save the value of the serviceId for each of the three services, beginning with the localityName, to a separate file.

```
echo Palo Alto:32_digit_hexadecimal_value_of_group_check_interface >> C:\certs\gc_id
echo Palo Alto:32_digit_hexadecimal_value_of_security_token_service_interface >> C:\certs\sts_id
echo Palo Alto:32_digit_hexadecimal_value_of_administrative_interface >> C:\certs\admin_id
```

Back up the ssoserver.crt, ssoserver.key, and ssoserver.p12 files.

- Open a Windows Explorer window and navigate to `C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf`.
- Create a backup folder and copy ssoserver.crt, ssoserver.key, and ssoserver.p12 files there.

In the command prompt, copy the three certificates to the vCenter Single Sign-On configuration directories, and confirm overwriting when prompted.

```
copy C:\certs\sso\ssoserver.p12 C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.p12
copy C:\certs\Root64.cer C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.crt
copy C:\certs\sso\rui.key C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.key
```

Update the vCenter Single Sign-On services by using the service files created with the network load balancer configuration.

- Edit the local hosts file, and add the following entry:

  ```
  192.168.110.41       sso.acme.local
  ```

  The entry contains the IP address of the SSO node and the FQDN of the load balancer. This is required to provide the necessary FQDN response to successfully upgrade vCenter Single Sign-On services.

- In a command prompt, run the commands to update the services, and confirm overwriting when prompted:

  ```
  ssolscli updateService -d https://sso1.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si C:\certs\gc_id -ip C:\certs\gc.properties
  ssolscli updateService -d https://sso1.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si C:\certs\admin_id -ip C:\certs\admin.properties
  ssolscli updateService -d https://sso1.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si C:\certs\sts_id -ip C:\certs\sts.properties
  ```

Verify that the updates to the vCenter Single Sign-On services have been applied.

- In a command prompt, run the commands to restart the VMware Security Token service.

  ```
  net stop VMwareSTS
  net start VMwareSTS
  ```

- List the vCenter Single Sign-On services to confirm that the updates have been applied.

  ```
  ssolscli listServices https://sso1.acme.local:7444/lookupservice/sdk
  ```

  The endpoints entry on line 4 shows the load balancer URL sso.acme.local for each of the three services.
12 Verify the vCenter Single Sign-On configuration on sso1.acme.local.
   a Open a browser window and go to https://sso1.acme.local:
      7444/websso/SAML2/Metadata/vsphere.local.
   b Download and open the file that prompts for download.
   c Verify that each location attribute of the <ds:x509Certificate> element refers to the host name of
      the load balancer and not to the host name of the vCenter Single Sign-On server.

What to do next
Configure the second server to use the signed certificates and delete false entries in the
vCenter Single Sign-On configuration.

Configure the Second vCenter Single Sign-On Server to Use the Signed
Certificates
After you have configured your first vCenter Single Sign-On server, you must copy the certificates to the
second vCenter Single Sign-On server and reconfigure the server to use these certificates.

Procedure
1 Log in to sso2.acme.local as an administrator.
2 Copy configuration files from sso1.acme.local to sso2.acme.local.
   a Open Windows Explorer and copy the \sso1.acme.local\c$\certs directory to C: \.
   b Copy the \sso1.acme.local\c$\ProgramData\VMware\SSL directory to C:\ProgramData\VMware\.
3 In a command prompt, set the JAVA_HOME and PATH variables.
   set JAVA_HOME=C:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components
   set PATH=%PATH%;C:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso;%JAVA_HOME%\bin
4 Back up the ssoserver.crt, ssoserver.key, and ssoserver.p12 files.
   a Open a Windows Explorer window and navigate to
      C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf.
   b Create backup folder and copy ssoserver.crt, ssoserver.key, and ssoserver.p12 files there.
5 Update the vCenter Single Sign-On services with the service files that contain the network load balancer
   configuration.
   a Edit the local hosts file, and add the following entry:
      192.168.110.42       sso.acme.local
      The entry contains the IP address of the SSO node and the FQDN of the load balancer. This is
      required to provide the necessary FQDN response to successfully upgrade vCenter Single Sign-On
      services.
   b In a command prompt, run the commands to copy the three certificates to the
      vCenter Single Sign-On configuration directories, and confirm overwriting when prompted.
      copy c:\certs\sso\ssoserver.p12
      c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.p12
      copy c:\certs\Root64.cer c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.crt
      copy c:\certs\sso\rui.key c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\ssoserver.key
   c Restart the VMware Security Token service:
      net stop VMwareSTS
      net start VMwareSTS
d  Update the vCenter Single Sign-On services.

ssolscli updateService -d https://sso2.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si c:\certs\gc_id -ip C:\certs\gc.properties
ssolscli updateService -d https://sso2.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si c:\certs\admin_id -ip C:\certs\admin.properties
ssolscli updateService -d https://sso2.acme.local:7444/lookupservice/sdk -u administrator@vsphere.local -p password -si c:\certs\sts_id -ip C:\certs\sts.properties

e  Restart the VMware Security Token service for the new configurations to take effect:

net stop VMwareSTS
net start VMwareSTS

6  List the vCenter Single Sign-On services to confirm that the updates have been applied.

ssolscli listServices https://sso2.acme.local:7444/lookupservice/sdk

The endpoints entry on line 4 must now show the load balancer URL sso.acme.local for each service.

7  Back up the vCenter Single Sign-On configuration files and replace them with the ones from SSO Server A.

a  Open a Windows Explorer window and navigate to C:\ProgramData\VMware\CIS\cfg\vmware-sso.

b  Create a backup folder.

c  Copy the contents of C:\ProgramData\VMware\CIS\cfg\vmware-sso to C:\ProgramData\VMware\CIS\cfg\vmware-sso\backup.

d  Navigate to \sso1.acme.local\c$\ProgramData\VMware\CIS\cfg\vmware-sso.

e  Copy the files ssoserverRoot.crt, ssoserverSign.crt, ssoserverSign.pub, and ssoserverSign.key to C:\ProgramData\VMware\CIS\cfg\vmware-sso.

8  In a command prompt, run the following commands to stop Security Token Service and Identity Management Service:

net stop VMwareSTS
net stop VMwareIdentityMgmtService

9  Connect to LDAP to delete entries that are no longer needed in the vCenter Single Sign-On server configuration.

a  Open JXplorer window and establish a connection with the following values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>sso2.acme.local</td>
</tr>
<tr>
<td>Port</td>
<td>11711</td>
</tr>
<tr>
<td>Protocol</td>
<td>LDAP v3</td>
</tr>
<tr>
<td>Base DN</td>
<td>DC=acme,DC=local</td>
</tr>
<tr>
<td>Level</td>
<td>User + Password</td>
</tr>
<tr>
<td>User DN</td>
<td>CN=administrator,CN=users,DC=acme,DC=local</td>
</tr>
<tr>
<td>Password</td>
<td>administrator_user_password</td>
</tr>
</tbody>
</table>

b  In the left navigation, expand local > acme > ComponentManager > Ldus, and expand all sub-nodes.

c  For each TenantCredential-1 object, on the Table Editor tab, click Properties.
d Find and delete the TenantCredential-1 object that contains sso2 in the value of the modifiersName attribute.

e For each TrustedCertChain-1 object, on the Table Editor tab, click Properties.

f Find and delete the TrustedCertChain-1 object that contains sso2 in the value of the modifiersName attribute.

10 Start the Identity Management Service and reinstall the Security Token Service components.

a In a command prompt, run the command to start the Identity Management Service:

```
net start VMwareIdentityMgmtService
```

b Navigate to the location of the Security Token Service.

cd C:\ProgramData\VMware\CIS\cfg\vmware-sso

c Reinstall the Security Token Service.

The following command is a long, single command and should be executed at once. There are breaks in the command for better visibility. Verify that the command returns a success message.

```
"c:\Program Files\Common Files\VMware\VMware vCenter Server – Java Components\bin\java.exe" -cp"c:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso\*;c:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso\lib\*;.*" com.vmware.identity.installer.STSInstaller --install --root-cert-path ssoserverRoot.crt --cert-path ssoserverSign.crt --private-key-path ssoserverSign.key --retry-count 2 --retry-interval 30
```

d Start the Security Token Service.

```
net start VMwareSTS
```

11 Verify the vCenter Single Sign-On configuration on sso2.acme.local.

a Open a browser window and navigate to https://sso2.acme.local:7444/websso/SAML2/Metadata/vsphere.local.

b Download and open the file that prompts for download.

c Verify that each location attribute of the <ds:x509Certificate> element refers to the host name of the load balancer and not to the host name of the vCenter Single Sign-On server.

What to do next

Install and configure vCenter Server.

Install vCenter Server and Configure It to Use External vCenter Single Sign-On

After both vCenter Single Sign-On servers are installed and configured, you must install a vCenter Server that will later be paired with your load balancer.

Prerequisites

Verify that the VM, prepared for the installation of vCenter Server, is running Microsoft Server 2012 R2 and meets the minimum hardware requirements.

Procedure

1 Connect the vCenter Server ISO image to the vc.acme.local virtual machine.

2 Log in to vc.acme.local as a vCenter Server administrator.
3 Add the following entry to the local hosts file.

192.168.110.41    sso.acme.local

4 Open the CD-ROM drive and double-click the autorun.exe file to start the vCenter Server installation wizard.

5 Install the vSphere Web Client.
   a In the VMware vCenter Installer, select the **vSphere Web Client** option under Custom Install, and click **Install**.
   b Follow the prompts of the installation wizard until the vCenter Single Sign-On Information page appears, and enter the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO administrator user name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>SSO administrator password</td>
<td>administrator_user_password</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sso.acme.local:7444/lookupservice/sdk">https://sso.acme.local:7444/lookupservice/sdk</a></td>
</tr>
</tbody>
</table>

   c Click **Yes** to accept the vCenter Single Sign-On certificate.
   d Click **Install Certificates** and complete the installation process.

6 Install the vSphere Inventory Service.
   a In the VMware vCenter Installer, select the **vCenter Inventory service** option and click **Install**.
   b Follow the prompts of the installation wizard until Local System Information page appears, enter vc.acme.local, and click **Next**.
   c On the Configure Ports page, click **Next**.
   d Leave the Small Inventory Size option selected, and click **Next**.
   e On the vCenter Single Sign-On Information page, enter the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO administrator user name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>SSO administrator password</td>
<td>administrator_user_password</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sso.acme.local:7444/lookupservice/sdk">https://sso.acme.local:7444/lookupservice/sdk</a></td>
</tr>
</tbody>
</table>

   f Click **Yes** to accept the certificate of the vCenter Single Sign-On.
   g Complete the installation process.

7 Install vCenter Server.
   a In the VMware vCenter Installer, select the **vCenter Server** option under Custom Install, and click **Install**.
   b Follow the prompts of the installation wizard until the License Key page appears, enter your license key, and click **Next**.
   c Select the database option that best suits your needs, and click **Next**.
   d On the vCenter Server Service page, enter the password for the administrative service account, enter vc.acme.local as the fully qualified domain name, and click **Next**
   e Select **Create a standalone VMware vCenter Server instance** and click **Next**.
   f On the Configure ports page, leave the default port settings and click **Next**.
On the JVM Memory page, select the option that best suites your needs, and click **Next**.

On the vCenter Single Sign-On Information page, enter the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO administrator user name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>SSO administrator password</td>
<td>administrator_user_password</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sso.acme.local:7444/lookupservice/sdk">https://sso.acme.local:7444/lookupservice/sdk</a></td>
</tr>
</tbody>
</table>

Click **Yes** to accept the vCenter Single Sign-On certificate.

Verify that the user specified in the text box is **administrator@vsphere.local** and click **Next**.

In the **vCenter Inventory Service URL** text box, enter **https://vc.acme.local:10443** and click **Next**.

Complete the installation process.

Your vCenter Server is fully operational and ready to be registered with your load balancer.

**Configure the Load Balancer**

After you have configured both your SSO servers, you must configure your load balancer to manage the load to the SSO servers.

Adding a load balancer provides an active-active distribution of load as well as active-passive redundancy.

**Configure VMware NSX as Load Balancer**

After you have configured both vCenter Single Sign-On servers and vCenter Server, you must configure the VMware NSX 6.1.1 load balancer, and remove the mappings to the load balancer FQDN on the SSO and vCenter Server instances.

**Prerequisites**

- Verify that you have successfully deployed the NSX Manager and it is registered with vCenter Server.
- Verify that you have successfully configured the NSX Controller cluster.
- Verify that you have successfully deployed and configured an NSX Edge.

**Procedure**

1. Enable the load balancer on the NSX Edge.
   a. Open a browser window and log in to the vSphere Web Client where the NSX Manager is registered.
   b. In the navigator, under **Networking & Security** click **NSX Edges**.
   c. Double-click the NSX Edge services gateway.
   d. On the **Manage** tab, click the **Load Balancer** tab.
   e. Under **Global Configuration**, click **Edit**.
   f. Select the **Enable Load Balancer** check box and click **OK**.
2 Create an application profile.
   a On the left, click Application profiles, and click the Add icon.
   b Enter SSO TCP as the name.
   c Select TCP as the type and click OK.

3 On the left, click Service Monitoring, and click the Add icon.

<p>| Table 4-13. Service Monitor Settings |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>TCP Monitor</td>
</tr>
<tr>
<td>Interval</td>
<td>5</td>
</tr>
<tr>
<td>Timeout</td>
<td>15</td>
</tr>
<tr>
<td>Max Retries</td>
<td>3</td>
</tr>
<tr>
<td>Type</td>
<td>TCP</td>
</tr>
</tbody>
</table>

4 Add a server pool.
   a On the left, click Pools, and click the Add icon.
   b Enter SSO Pool as the pool name.
   c Select ROUND-ROBIN as the algorithm.
   d Select TCP Monitor as the monitor.
   e Click the Add icon to add two separate members with the following settings.

<p>| Table 4-14. Member 1 |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SSO1</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.110.41</td>
</tr>
<tr>
<td>Port</td>
<td>7444</td>
</tr>
<tr>
<td>Weight</td>
<td>256</td>
</tr>
</tbody>
</table>

<p>| Table 4-15. Member 2 |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SSO2</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.110.42</td>
</tr>
<tr>
<td>Port</td>
<td>7444</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
</tbody>
</table>

f Click OK.
On the left, click **Virtual Servers**, and click the **Add** icon to create a virtual server with the following settings.

**Table 4-16. Virtual server**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Virtual Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Application profile</td>
<td>SSO TCP</td>
</tr>
<tr>
<td>Name</td>
<td>SSO VIP</td>
</tr>
<tr>
<td>IP address</td>
<td>SSO (Load balancer) IP</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td>Port</td>
<td>7444</td>
</tr>
<tr>
<td>Default pool</td>
<td>SSO Pool</td>
</tr>
</tbody>
</table>

Remove the temporary entries in the local hosts files of the vCenter Single Sign-On servers and the vCenter Server host.

a. On SSO Server A, edit the local hosts file and remove:

```
192.168.110.41         sso.acme.local
```

b. On SSO Server B, edit the local hosts file and remove:

```
192.168.110.42         sso.acme.local
```

c. On the vCenter Server host, edit the local hosts file and remove:

```
192.168.110.41         sso.acme.local
```

**What to do next**

Test your vCenter Single Sign-On environment for authentication availability and service failure.

**Configure F5 BIG-IP as Load Balancer**

After you have configured both your vCenter Single Sign-On servers, you must configure your F5 BIG-IP load balancer, and remove the mappings to the load balancer FQDN on the SSO and vCenter Server instances.

**Prerequisites**

- Verify that your BIG-IP solution is fully operational.
- Verify that you have a valid licence for the Local Traffic Manager (LTM) module.

**Procedure**

1. Log in to the BIG-IP host.
2. Copy the `\sso1.acme.local\C\certs\` directory to the C: drive of the Big-IP host.
3. Load the CA-signed certificates to BIG-IP LTM.
   a. Open a Web browser window and log in to the BIG-IP management interface.
   b. Navigate to **System > File Management > SSL Certificate List** from the menu on the left.
c Import the certificate files from C:\certs.

<table>
<thead>
<tr>
<th>Table 4-17. File 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Value</td>
</tr>
<tr>
<td>Import Type</td>
<td>Certificate</td>
</tr>
<tr>
<td>Certificate Name</td>
<td>ssoCert</td>
</tr>
<tr>
<td>Upload File</td>
<td>C:\certs\sso\rui.crt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-18. File 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Value</td>
</tr>
<tr>
<td>Import Type</td>
<td>Key</td>
</tr>
<tr>
<td>Certificate Name</td>
<td>ssoKey</td>
</tr>
<tr>
<td>Upload File</td>
<td>C:\certs\sso\rui.key</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-19. File 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Value</td>
</tr>
<tr>
<td>Import Type</td>
<td>Certificate</td>
</tr>
<tr>
<td>Certificate Name</td>
<td>ACMELocalRoot</td>
</tr>
<tr>
<td>Upload File</td>
<td>C:\certs\Root64.cer</td>
</tr>
</tbody>
</table>

d Confirm that the ssoCert entry shows sso.acme.local as common name.

4 Create the load balancer pool.

a Navigate to Local Traffic > Pools > Pool List from the menu on the left.

b On the Pool List screen, click Create.

c Enter SSO as the name.

d Under Health Monitors, move tcp to the Active box.

e Select Round Robin as the load balancing method.

f Add two members to the new pool.

<table>
<thead>
<tr>
<th>Table 4-20. Member 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Value</td>
</tr>
<tr>
<td>Node Name</td>
<td>sso1</td>
</tr>
<tr>
<td>Address</td>
<td>192.168.110.41</td>
</tr>
<tr>
<td>Service Port</td>
<td>7444</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4-21. Member 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Value</td>
</tr>
<tr>
<td>Node Name</td>
<td>sso2</td>
</tr>
<tr>
<td>Address</td>
<td>192.168.110.42</td>
</tr>
<tr>
<td>Service Port</td>
<td>7444</td>
</tr>
</tbody>
</table>

g Click Finished.
Create an SSL client.

a Navigate to **Local Traffic > Profiles > SSL > Client** from the menu on the left.

b On the Client page, click **Create**.

c Enter **SSO-Client** as the name and select the **Custom** check box.

d In the Configuration section, select **Advanced** from the drop-down menu.

e Select the **Custom** check box.

f Select **ssoCert** as the certificate.

g Select **ssoKey** as the key.

h In the **Ciphers** text box, replace the contents with the following string to enable **SSLv3** protocol support.

```
SSLv3:RSA+AES:
```

i Click **Add** and click **Finished**.

Create an SSL Server.

a Navigate to **Local Traffic > Profiles > SSL > Server** from the menu on the left.

b On the Server page, click **Create**.

c Enter **SSO-Server** as the name and enable **Custom** settings.

d Select **ssoCert** as the certificate.

e Select **ssoKey** as the key and click **Finished**.

Create a virtual server.

a Navigate to **Server > Local Traffic** from the menu on the left.

b On the Server page, click **Create** and configure the virtual server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SSO-VIP</td>
</tr>
<tr>
<td>Destination Address</td>
<td>192.168.110.40</td>
</tr>
<tr>
<td>Service Port</td>
<td>7444</td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>http</td>
</tr>
<tr>
<td>SSL Profile (Client)</td>
<td>SSO-Client</td>
</tr>
<tr>
<td>SSL Profile (Server)</td>
<td>SSO-Server</td>
</tr>
<tr>
<td>Default Pool</td>
<td>SSO</td>
</tr>
</tbody>
</table>

c Click **Finished**.

Configure Source Network Address Translation (SNAT).

a Navigate to **Local Traffic > Address Translation > SNAT List** from the menu on the left.

b On the SNAT List page, click **Create**.

c Enter **SNAT--SSO-NGC** as the name.

d In the translation section, select **IP Address** and enter **192.168.110.40**.

e Click **Finished**.
9. Remove the temporary entries in the local hosts files of the vCenter Single Sign-On servers and the vCenter Server host.
   
a. On SSO Server A, edit the local hosts file and remove:

   192.168.110.41     sso.acme.local

   b. On SSO Server B, edit the local hosts file and remove:

   192.168.110.42     sso.acme.local

   c. On the vCenter Server host, edit the local hosts file and remove:

   192.168.110.41     sso.acme.local

What to do next
Test your vCenter Single Sign-On environment for authentication availability and service failure.

Configure VMware vCloud Networking and Security Edge as Load Balancer
After you have configured both your vCenter Single Sign-On servers, you must configure your vCNS load balancer, and remove the mappings to the load balancer FQDN on the SSO and vCenter Server instances.

Prerequisites
- Verify that you have successfully deployed the vShield Manager and it is registered with vCenter Server.
- Verify that you have successfully deployed and configured a vShield Edge.

Procedure
1. Log in to the VMware vShield Manager interface.
2. Configure the virtual IP address.
   
a. On the left pane, click the data center that your vCenter Single Sign-On resides in.
   b. Click the Network Virtualization tab.
   c. Select your Edge gateway device.
   d. From the Actions menu, click Manage.
   e. Click the Configure tab.
   f. Select the vNIC to house the VIP IP address.
   g. Click Edit.
   h. Click the Add icon.
   i. Enter 192.168.110.40 as the IP address of the load balancer.
   j. Click Add.
3 Create the virtual server pool.
   a Click the **Load Balancer** tab on the edge screen.
   b Click **Add** to add a pool and configure it.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>SSO POOL</td>
</tr>
</tbody>
</table>

**Table 4-24. Services Tab**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service enabled</td>
<td>TCP</td>
</tr>
<tr>
<td>Balancing Method</td>
<td>LEAST_CONN</td>
</tr>
<tr>
<td>Port</td>
<td>7444</td>
</tr>
</tbody>
</table>

**Table 4-25. Health Check Tab**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service enabled</td>
<td>TCP</td>
</tr>
<tr>
<td>Monitor Port</td>
<td>7444</td>
</tr>
<tr>
<td>Mode</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Table 4-26. Members Tab, Member 1**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.10.41</td>
</tr>
<tr>
<td>Weight</td>
<td>256</td>
</tr>
</tbody>
</table>

**Table 4-27. Members Tab, Member 2**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.10.42</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
</tbody>
</table>

4 Update the load balancer configuration and enable it.
   a Click **Enable**.
   b Click **Publish changes**.

5 Create a virtual server.
   a Switch from Pools to **Virtual Servers**.
   b Click the **Add** icon to add a new virtual server.

**Table 4-28. Virtual Server Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SSO-VIP</td>
</tr>
<tr>
<td>IP address</td>
<td>192.168.110.40</td>
</tr>
<tr>
<td>Enabled Service</td>
<td>TCP</td>
</tr>
<tr>
<td>Port</td>
<td>7444</td>
</tr>
</tbody>
</table>

c Click **Publish changes**.

6 Remove the temporary entries in the local hosts files of the vCenter Single Sign-On servers and the vCenter Server host.
   a On SSO Server A, edit the local hosts file and remove:
      192.168.110.41         sso.acme.local
   b On SSO Server B, edit the local hosts file and remove:
      192.168.110.42         sso.acme.local
   c On the vCenter Server host, edit the local hosts file and remove:
      192.168.110.41         sso.acme.local

**What to do next**

Test your vCenter Single Sign-On environment for authentication availability and service failure.

**Test Your Highly Available vCenter Single Sign-On Environment**

After you have deployed and configured all nodes, you must test your highly available vCenter Single Sign-On deployment.

**Table 4-29. Authentication Based Tests**

<table>
<thead>
<tr>
<th>Goal</th>
<th>Instructions</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test integrated Windows authentication.</td>
<td>1 Add an Active Directory user from the acme.local domain to the vCenter Single Sign-On administrators group.</td>
<td>After each login attempt you see the vCenter Single Sign-On administration page in the vSphere Web Client.</td>
</tr>
<tr>
<td></td>
<td>2 Log in to the vSphere Web Client as the added domain user.</td>
<td></td>
</tr>
<tr>
<td>Test Active Directory over LDAP authentication.</td>
<td>1 Add an Active Directory group that contains users, from the acme.local domain to the vCenter Single Sign-On Administrators group.</td>
<td>Deploy an untrusted domain to the acme.local domain.</td>
</tr>
<tr>
<td></td>
<td>2 Log in to the vSphere Web Client as a user from the added group.</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-29. Authentication Based Tests (Continued)

<table>
<thead>
<tr>
<th>Goal</th>
<th>Instructions</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test vCenter Single Sign-On service failure.</td>
<td>1 Add an Active Directory user from the acme.local domain to the vCenter Single Sign-On Administrators group.</td>
<td>■ When you power off SSO Server A, SSO Server B must take over the authentication process and you should not be asked to log in again.</td>
</tr>
<tr>
<td></td>
<td>2 Log in to the vSphere Web Client, or the respective administration interface, as the added domain user.</td>
<td>■ When you power on SSO Server A again and power off SSO Server B, SSO Server A must take over the authentication process.</td>
</tr>
<tr>
<td></td>
<td>3 Power off SSO Server A while the login session is active and examine the result.</td>
<td>■ When you power on SSO Server B, the replication between the SSO servers returns to normal.</td>
</tr>
<tr>
<td></td>
<td>4 Continue working in the current session.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Log out and log back in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 Power on SSO Server A.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7 Power off SSO Server B and examine the result.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 Power on SSO Server B.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9 Continue working in the current session and examine the result.</td>
<td></td>
</tr>
</tbody>
</table>

When you install other products that use vCenter Single Sign-On, for example vCloud Automation Center, vSphere Data Protection, and vCenter Orchestrator, you should perform the service level tests again. Use the administration interfaces of each product, not the vSphere Web Client in step 2.

Configure vCloud Suite Products to Use the Virtual IP as vCenter Single Sign-On

When the load balancer is fully configured as an entry point for all requests to the vCenter Single Sign-On, you can configure other vCloud Suite products to use the virtual IP of the load balancer as their SSO.

Products below can use vCenter Single Sign-On as authentication service.

- Configure vSphere Data Protection to Use vCenter Single Sign-On on page 101
  Configure vSphere Data Protection appliance to use the IP of the load balancer as vCenter Single Sign-On.

- Configure vCloud Automation Center to Use vCenter Single Sign-On on page 101
  Configure vCloud Automation Center to use the IP of the load balancer as vCenter Single Sign-On.
Configure vCenter Orchestrator to Use vCenter Single Sign-On on page 102

Configure vCenter Orchestrator to use the IP of the load balancer as vCenter Single Sign-On.

Configure vSphere Data Protection to Use vCenter Single Sign-On

Configure vSphere Data Protection appliance to use the IP of the load balancer as vCenter Single Sign-On.

**Prerequisites**

Verify that you have successfully deployed vSphere Data Protection appliance.

**Procedure**

1. In a Web browser, go to https://192.168.110.46:8543/vdp-configure/ and log in to the configuration interface of the vSphere Data Protection appliance.
2. On the Configuration page, in the VDP Appliance section, click the All Actions icon, and click vCenter registration.
3. Review the information on the screen and select the check box at the bottom of the page, and click Next.
4. On the vCenter Configuration page, enter the following settings and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter username</td>
<td>vsphere.local\administrator</td>
</tr>
<tr>
<td>vCenter password</td>
<td>administrator_user_password</td>
</tr>
<tr>
<td>vCenter FQDN or IP</td>
<td>192.168.110.45</td>
</tr>
<tr>
<td>vCenter HTTP port</td>
<td>80</td>
</tr>
<tr>
<td>vCenter HTTPS port</td>
<td>443</td>
</tr>
<tr>
<td>Use vCenter for SSO authentication</td>
<td>Leave deselected</td>
</tr>
<tr>
<td>SSO FQDN or IP</td>
<td>sso.acme.local</td>
</tr>
<tr>
<td>SSO port</td>
<td>7444</td>
</tr>
</tbody>
</table>

5. Click Finish to complete the wizard and wait for the new changes to take effect.

You have successfully configured your vSphere Data Protection instance to use the virtual IP address of the load balancer.

**What to do next**

Verify vSphere Data Protection authentication settings.

1. Log out and log back in to the vSphere Data Protection appliance configuration interface.
2. Perform service level tests, as described in “Test Your Highly Available vCenter Single Sign-On Environment,” on page 99.

Configure vCloud Automation Center to Use vCenter Single Sign-On

Configure vCloud Automation Center to use the IP of the load balancer as vCenter Single Sign-On.

**Prerequisites**

Verify that you have successfully deployed vCloud Automation Center appliance.

**Procedure**

1. In a browser, go to https://192.168.110.47:5480 and log in to the vCloud Automation Center appliance interface.
2 Under vCAC Settings, click SSO, provide the SSO settings, and click Save Settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Host and Port</td>
<td>sso.acme.local:7444</td>
</tr>
<tr>
<td>SSO Default Tenant</td>
<td>vsphere.local</td>
</tr>
<tr>
<td>SSO Admin User</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>SSO Admin Password</td>
<td>admin_user_password</td>
</tr>
</tbody>
</table>

You have successfully configured your vCloud Automation Center appliance to use the virtual IP address of the load balancer.

What to do next
Verify vCloud Automation Center authentication settings.
1 Log out and log back in to the vCloud Automation Center appliance interface.
2 Perform service level tests, as described in “Test Your Highly Available vCenter Single Sign-On Environment,” on page 99.

Configure vCenter Orchestrator to Use vCenter Single Sign-On
Configure vCenter Orchestrator to use the IP of the load balancer as vCenter Single Sign-On.

Prerequisites
Verify that you have successfully deployed vCenter Orchestrator.

Procedure
1 In a Web browser, go to https://192.168.110.48:8283 and log in to the vCenter Orchestrator administration interface.
2 Under Startup Options, click Stop service to stop the vCenter Orchestrator service.
3 Import the SSL certificates from your load balancer and vCenter Server.
   a Under Network, select the SSL Trust Manager tab.
   b Under Import from URL, enter https://192.168.110.48:443 to import the vCenter Server certificate, and click Import.
   c When the properties of the certificate are displayed, click Import again.
   d Under Import from URL, enter https://sso.acme.local:7444, to import the load balancer certificate, and click Import.
4 Under Authentication, enter the following values to set vCenter Single Sign-On as authentication method, and click Register Orchestrator.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td><a href="https://sso.acme.local:7444">https://sso.acme.local:7444</a></td>
</tr>
<tr>
<td>Admin user name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Admin password</td>
<td>administrator_user_password</td>
</tr>
</tbody>
</table>

5 Under Startup Options, click Start Service to start the vCenter Orchestrator service.

You have successfully configured your vCenter Orchestrator to use the virtual IP address of the load balancer as vCenter Single Sign-On authentication method.
What to do next

Verify vCenter Orchestrator authentication settings.

1. Log out and log back in to the vCenter Orchestrator client.

2. Perform service level tests, as described in “Test Your Highly Available vCenter Single Sign-On Environment,” on page 99.
Symbols
$(\text{random})$ 70, 72

A
activate vCloud Suite components 46
add the vCloud Suite license 44
application blueprint 70, 72
Application Services, creating applications 69
applications, deploying 74
assign license 48
assign license key 46
assign licenses 44
assign vCloud Suite license
vCenter Operations Management Suite 46
vCenter Site Recovery Manager 47
assign vCloud Suite License, vCloud Networking
and Security 47

B
basic application blueprint 70, 72
blueprint for an application 70, 72
business continuity 53, 58
business groups, vCloud Automation Center 66

C
cloud logical templates, adding to the library 68
cloud providers, vCloud Automation Center 66
commom services 41
conceptual design 15

D
Deployment 29
deployment environment, creating vCloud
Director 67
Deployment Profile wizard 74
design considerations 19
disaster recovery to cloud
configure network connection 57
deploy vSphere Replication 56
DR2C 53, 58

E
encryption and security certificates 41
ESXi and the ESX Management Interfaces 40
execution plan 74
external dependencies 32

G
glossary 5

H
Highly Available SSO
Configure products 100
Configure vCAC 101
Configure vCO 102
Configure vDP 101
Deployment Overview 75
Load Balancer Configuration 92, 94, 97
OpenSSL Certificates 83
Preparation 80
SSO Configuration 85, 88
SSO Installation 82
Test Environment 99
vCenter Install 90
host name 70, 72

I
IaaS
customize VM 62
provision VM 61
provision workload 62
retire VM 63
take VM snapshot 63
IaaS diagram 26
intended audience 5
introduction 9
iSCSI storage 39
iSCSI storage security 39
isolation, virtual machines 34

L
license, usage 51
license capacity, processor 44
license key
add 45
assign 45, 48
license usage
CPU usage 50
export report 51, 52
monitor 50
license assignment 48
licensing, vCloud Suite 44
logical templates, virtual machine 68