



VMware® vCenter Server™ 5.5 Deployment Guide

TECHNICAL MARKETING DOCUMENTATION
V 1.0/NOVEMBER 2013/JUSTIN KING

Table of Contents

Overview	3
Components of vCenter Server 5.5	3
vCenter Single Sign-On	3
vSphere Web Client	3
vCenter Inventory Service	3
vCenter Server Database	4
vCenter Server	4
vCenter Server Desktop Client	4
Deployment Processes	5
Simple Install	5
Custom Install	5
In-Place Upgrade Versus Fresh Install	6
Performance Considerations	6
Compute	6
Storage	7
Networking	7
Reference Architectures	8
Prerequisites	8
Example 1: Deploying a Single vCenter Server Instance	9
Example 2: Deploying an Additional vCenter Server (Local or Remote)	11
Example 3: Deploying Multiple vCenter Servers with a Centralized vCenter Single Sign-On Server	12
Upgrading vSphere 5.1 Architecture	13
Post-Installation Tasks	13
Configure an Identity Source	13
Permissions	14
Linked Mode	14
Update SSL Certificates	14
Availability	15
VMware Data Protection	15
vSphere HA	15
vCenter Server Heartbeat	15
Conclusion	15

Overview

With the release of VMware vSphere® 5.5 and vCenter Server 5.5, multiple individual components are used to deliver the vCenter Server management solution. This paper discusses these components. It also describes their interaction with other components, their role within the vCenter Server stack and VMware recommended deployment of all components included with the vCenter Server 5.5 release.

Components of vCenter Server 5.5

vCenter Single Sign-On

VMware vCenter™ Single Sign-On is a critical component of the vCenter Server environment because it provides secure authentication services to many of the vSphere components. vCenter Single Sign-On constructs an internal security domain (vsphere.local) where vSphere solutions and components are registered during installation or upgrade, providing an infrastructure resource. vCenter Single Sign-On can authenticate users from its own internal users and groups, or it can connect to trusted external directory services such as Microsoft's Active Directory. Authenticated users are then ready for assignment of registered solution-based permissions and/or roles within a vSphere 5.5 environment.

In the past, vCenter Single Sign-On was complex to deploy and manage and this complexity was a key issue to address with the latest release. vCenter Single Sign-On 5.5 offers greatly improved integration of external directory services and is deployed with a simplified architecture. Multiple vCenter Single Sign-On instances can be placed into the same vsphere.local security domain, which can span geographies and can be synchronized automatically with built-in replication.

vCenter Single Sign-On is implemented as a Tomcat server container providing a Security Token Service for successful authentications and an internal LDAP directory service for the storing and replication of its configuration and embedded users and groups that have been defined. vCenter Single Sign-On uses Kerberos to communicate and installs several technology dependencies to support this.

vSphere Web Client

The VMware vSphere Web Client was introduced with vSphere 5.0 and had limited appeal due to the lack of administrative capability. Recent versions of the vSphere Web Client matched capability to that of the trusted Virtual Infrastructure Client (VI Client). The vSphere Web Client is now the only client used to manage any new technology or feature introduced with vSphere 5.1 and higher (for instance, vCenter Single Sign-On).

The latest vSphere Web Client is designed to manage thousands of objects with the use of enhanced navigation based on relationships. It is loaded with features for retrieving information quickly and effectively (tagging, filters, and so on).

The vSphere Web Client is a centralized infrastructure component delivered as a Tomcat server back end with an Adobe Flex-enabled browser on the workstation of the end user. This improved architecture removes the dependency for the thick client (VI Client) on the workstation of the end user and can upgrade all users in one simple procedure as well as centralize the use of client plug-ins.

vCenter Inventory Service

The VMware vCenter Inventory Service is a caching component used to enhance vSphere Web Client responses to queries by removing the performance tax associated with communicating directly against the already busy core vCenter processes. Approximately 90 percent of all client requests are read-only queries. These include retrieving configurations of objects, such as virtual machines in a cluster. Removing such operations from core vCenter processing enables vCenter Server to provide better resource allocation for its ongoing operations, including statistics management and service-level optimization.

The vCenter Inventory Service also stores the object-tagging feature, introduced in vSphere 5.1. This feature enables the inclusion of external metadata that can attach additional attributes. These attributes can then be used to aid in retrieving criteria based on search requirements or organizational groupings. Tags are saved directly to the vCenter Inventory Service cache, not to the vCenter database.

The vCenter Inventory Service is delivered as a file-level (xDB format) cache and can be read- and write-intensive on the disk subsystem due to frequent updates and client queries.

vCenter Server Database

The database is a key component of the vCenter Server architecture. Every call to the vCenter Server instance invokes a communication with the vCenter Server database. For this reason, database performance is key to maintaining an acceptable response time. The vCenter Server database is the central storage location of almost all vCenter Server configuration parameters (15 percent of database size) as well as the storage location of all statistics and historical data (85 percent of database size). The statistics are used for analysis and provide optimization of inventory objects within a vCenter Server-managed environment. This data aids in achieving the operational and performance recommendations for a vSphere environment.

The vCenter Server database is typically deployed on a separate server from the vCenter Server instance and housed in a Microsoft SQL Server or Oracle database server solution. With the release of vSphere 5.5, the VMware vCenter Server Appliance™ has seen an increase in supported scale (100 hosts/3,000 virtual machines) with its embedded database, making it an attractive option for those that do not have the external database management skills or requirements.

vCenter Server

The vCenter Server component is the central component for managing and optimizing a vSphere environment. It provides management and monitoring of multiple vSphere hosts and it also enables essential virtualization technologies such as VMware vSphere vMotion® and VMware vSphere High Availability (vSphere HA). vCenter Server is dependent on all components listed here and is the “brain” of the management framework within the VMware vCloud® Suite.

vCenter Server is delivered as an application built with Java and .NET technologies.

vCenter Server Desktop Client

The vCenter Server desktop client has been the de facto standard client used for administrating and managing many previous vSphere releases. As vSphere environments evolved with inclusion of hundreds if not thousands of objects, the desktop client has not been able to scale to meet these demands.

VMware announced with the release of vSphere 5.1 that the desktop client would be deprecated in a future release. In the vSphere 5.5 release, several components still require the use of the desktop client, because their management has not yet been migrated to the vSphere Web Client. As it is being deprecated, the desktop client has been kept available for the management of several legacy technologies in the vSphere 5.5 release. To date, specific use cases, such as remediating vSphere hosts with VMware vSphere Update Manager™, management of direct vSphere hosts, and the operations of VMware vCenter Site Recovery Manager™, have not been converted to the vSphere Web Client, so the desktop client remains a feature-limited secondary client.

The desktop client is a C# client installed locally on the workstation of the end user and requires the installation of .NET. It is not uncommon to have multiple desktop clients installed on a single workstation, one for each vSphere release (update or version release).

Deployment Processes

There are multiple components and processes involved when deploying a vCenter server. Two categories of deployments assist with this.

Simple Install



Figure 1. Simple Install

The simple install is a deployment option that deploys vCenter Server, with its default options selected, to a single physical or virtual machine. The simple install takes the four core components of vCenter Server (vCenter Single Sign-On, vSphere Web Client, vCenter Inventory Service, and the vCenter Server instance) and chains the individual installers into a single process to install a single vCenter Server environment.

There are several limitations with the simple installer. These include the following:

1. Simple install deploys vCenter Server to the C:\Program Files\VMware\Infrastructure\ directory with no option to change the destination folder. Many customers prefer to install their applications to a volume other than the system volume.
2. Simple install provides only the vCenter Single Sign-On deployment option of "vCenter Single Sign-On for your first vCenter Server." Therefore it cannot be used for additional vCenter servers.

Custom Install

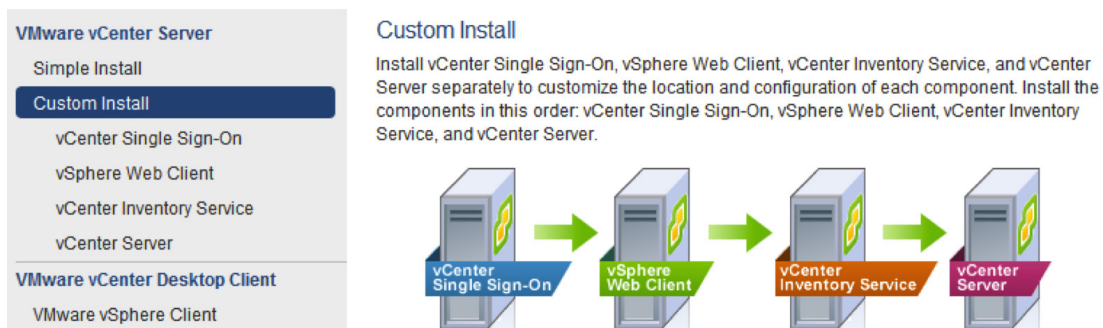


Figure 2. Custom Install

The custom install option enables the installation of each individual component independently, and it offers additional advanced configuration options. Because each component is being installed individually, it is important that the various components are installed in the following order:

1. vCenter Single Sign-On
2. vSphere Web Client
3. vCenter Inventory Service
4. vCenter Server

Use cases for using the custom install option instead of the simple install option are as follows:

1. To distribute vCenter Server components across multiple virtual machines
2. To change the destination folder of a given component
3. To deploy multiple vCenter servers, extending the vsphere.local security domain

In-Place Upgrade Versus Fresh Install

Most upgrades would typically be “in place.” This means that the current version of vCenter is replaced by the most recent. But many customers actually decide to rebuild and deploy what would be called a fresh install. Both methods have their pros and cons. The following information should help you to decide on an upgrade method.

NEW INSTALL	IN-PLACE UPGRADE
<p>Pros</p> <ul style="list-style-type: none"> • Clean start • Reconfigured architecture • New hardware 	<p>Pros</p> <ul style="list-style-type: none"> • Most common • All settings maintained • Slipstreamed process • Historical data maintained
<p>Cons</p> <ul style="list-style-type: none"> • Loss of historical data • Rebuild of environment • Settings manually recreated • Time involved 	<p>Cons</p> <ul style="list-style-type: none"> • Carryover of old/unused data • Performance (hardware)

Table 1. New Install or In-Place Upgrade

Performance Considerations

When you are designing a deployment strategy for a new environment or upgrading an existing environment, it is easy to overlook performance characteristics. This can prohibit vCenter Server from achieving its full capabilities when managing and optimizing a vSphere environment. There are several key areas that must be addressed to deploy a healthy vCenter Server environment.

Compute

Many components make up the vCenter Server framework for managing and monitoring a vSphere environment. To handle this, system requirements have been adjusted to better provide necessary resources affecting CPU and memory. Here are recommendations for deploying a vCenter server in a single virtual machine configuration as well as guidelines for deploying each component individually.

SYSTEM REQUIREMENTS (HARDWARE)	
<p>Simple install (minimum)</p> <ul style="list-style-type: none"> • 2CPU/12GB RAM/100GB disk/1Gbps 	<p>Simple install (recommended)</p> <ul style="list-style-type: none"> • 4CPU/24GB RAM/100GB disk/1Gbps
<p>Custom install (minimum)</p> <p>Single Sign-On</p> <ul style="list-style-type: none"> • 1CPU/3GB RAM/2GB disk/1Gbps <p>vSphere Web Client</p> <ul style="list-style-type: none"> • 1CPU/2GB RAM/2GB disk/1Gbps <p>vCenter Inventory Service</p> <ul style="list-style-type: none"> • 1CPU/3GB RAM/5GB disk/1Gbps <p>vCenter Server</p> <ul style="list-style-type: none"> • 2CPU/4GB RAM/60GB disk/1Gbps 	<p>Custom install (recommended)</p> <p>Single Sign-On</p> <ul style="list-style-type: none"> • 2CPU/4GB RAM/8GB disk/1Gbps <p>vSphere Web Client</p> <ul style="list-style-type: none"> • 2CPU/4GB RAM/8GB disk/1Gbps <p>vCenter Inventory Service</p> <ul style="list-style-type: none"> • 1CPU/8GB RAM/32GB disk/1Gbps <p>vCenter Server</p> <ul style="list-style-type: none"> • 4CPU/8GB RAM/100GB disk/1Gbps <p><i>Based on an inventory size of 400 hosts or 4,000 virtual machines</i></p>

Table 2. System Requirements (Hardware)

Storage

Storage for a vCenter Server environment involves three main components: the vCenter Server instance, vCenter Server database and vCenter Inventory Service cache. The vCenter Server instance itself has fairly minimal storage performance requirements. The vCenter Server database and the vCenter Inventory Service cache are heavily affected by the underlying storage subsystem due to higher than average I/O requirements. Best practices include deploying the vCenter Server database to a separate virtual machine and separating the vCenter Inventory Service cache from the vCenter Server application storage. Moving the vCenter Inventory Service cache to SSD-backed storage for fast read response is also recommended. These recommendations greatly improve the response time observed in the vSphere Web Client and vCenter Server performance. Users can also consider deploying VMware vSphere Flash Read Cache® to support the I/O requirements of the vCenter Inventory Service.

Networking

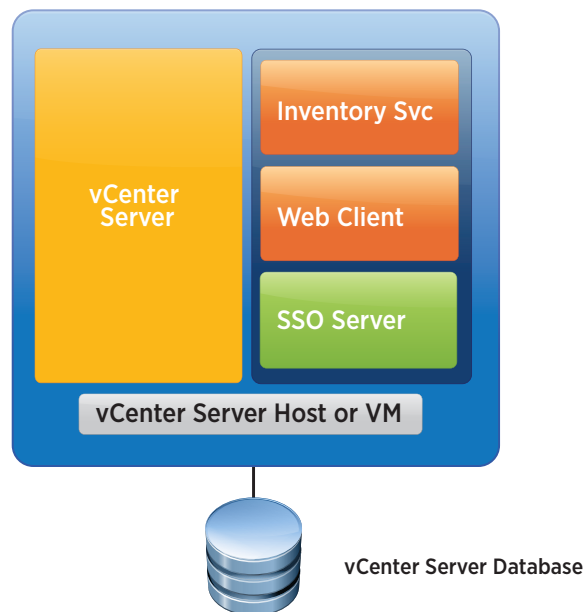
VMware testing continues to identify latency as one of the single biggest factors in performance degradation. Tests clearly show that a lower latency provides better overall performance when compared to high latency or even larger network throughput. To have the multiple components of vCenter Server, as described in the previous section, communicating with minimal latency is a key objective for the achievement of a healthy and optimal vCenter Server environment. Minimizing the following essential communications in vCenter Server provides the biggest increase in its performance:

- vCenter Server application to vCenter Server database
- vCenter Server application to managed vSphere hosts
- vCenter Server application to vCenter Inventory Service
- vSphere Web Client to vCenter Inventory Service
- vCenter Single Sign-On to all vCenter Server components

The lowest latency is achieved by running all components within a single virtual machine. However, this eliminates the benefits of separating the vCenter Server database from the vCenter Server application. Nearly identical latency benefits can be achieved by running the vCenter Server components over multiple virtual machines on the same vSphere host. For example, users can configure the vCenter Server application and its components in one virtual machine and the vCenter Server database in another virtual machine on the same host and set host affinity rules to maintain this configuration.

Reference Architectures

The recommended approach for deploying vCenter Server in almost all scenarios involves a single virtual machine for the vCenter Server components and a separate virtual machine for the vCenter Server database.



Uses simple installer

Installs/upgrades core components with a single virtual machine

1. vCenter Single Sign-On
2. vSphere Web Client
3. vCenter Inventory Service
4. vCenter Server

- No change to architecture
- All services are local
 - Reduced complexity
- Supports 1-1,000 hosts/
1-10,000 virtual machines

Figure 3. vCenter Server 5.5 – Deployment Best Practice

Prerequisites

- a. Deploy, and name accordingly, two Windows-based virtual machines with two volumes each.
- b. Assign a static IP address to both virtual machines.
- c. Confirm forward and reverse DNS resolution of hostname and IP address on both virtual machines.
- d. Add the Windows virtual machines to the Active Directory environment.
- e. Confirm that virtual machine time is synchronized with an Active Directory domain controller.
- f. On one virtual machine, install and configure Microsoft SQL Server.
- g. Create an empty database.
- h. On the other virtual machine, create and name an x64 ODBC data source name for the newly created database.
- i. Create an Active Directory domain account to be used as the service account for running vCenter Server.

Example 1: Deploying a Single vCenter Server Instance

In this example, we will deploy a single vCenter Server instance that meets the requirements for most customers, paying careful consideration to the various steps and configurations.

vCenter Single Sign-On

1. Connect the vCenter Server ISO image to the virtual machine.
2. On the DVD menu, select the **vCenter Single Sign-On** option listed under Custom Install.
3. Select **Install**.
4. After the Welcome to the vCenter Single Sign-On Setup screen is shown, select **Next**.
5. Select **I agree to the terms of the license agreement** and select **Next**.
6. Review the vCenter Single Sign-On prerequisites. Select **Next**.
7. On the vCenter Single Sign-On Information screen, select the first option, **vCenter Single Sign-On for your first vCenter Server**, because this is the first vCenter Server to deploy.
8. Provide a **Password** for the built-in administrator@vsphere.local account. (Refer to [KB2060746](#) for a list of illegal characters that cannot be used.)
9. On the vCenter Single Sign-On Site Configuration screen, provide a **Site Name**. This can be based on location or organization (for example, Production).
10. On the vCenter Single Sign-On Port Settings screen, select **Next**.
11. On the Change Destination Folder screen, select **Change** and edit the path to install on the second volume. Select **Next**.
12. Review the Review Install Options screen and select **Install**.
13. On the Completed the vCenter Single Sign-On Setup Wizard screen, select **Finish**.

vSphere Web Client Install

14. Return to the DVD menu and select the **vSphere Web Client** option listed under Custom Install.
15. Select **Install**.
16. Select **OK** for the required language.
17. On the Welcome to the InstallShield Wizard for VMware vSphere Web Client screen, select **Next**.
18. On the End User License Agreement screen, select **I accept the terms in the license agreement** and select **Next**.
19. On the Destination Folder screen, select **Change** and edit the path to install on the second volume (for example, D:\Program Files\VMware\Infrastructure\).
20. On the Configure Ports screen, select **Next**.
21. On the vCenter Single Sign-On Information screen, provide the **Password** entered in step 8 of the vCenter Single Sign-On installation.
22. If presented with a VMware vSphere Web Client dialogue box for the certificate, select **Yes** to accept and continue.
23. On the Certificate Installation for Secure Connection, select **Install certificates**.
24. On the Ready to Install screen, select **Install**.
25. On the VMware vSphere Web Client Installation Completed screen, select **Finish**, acknowledging the pop-up dialogue box.

vCenter Inventory Service

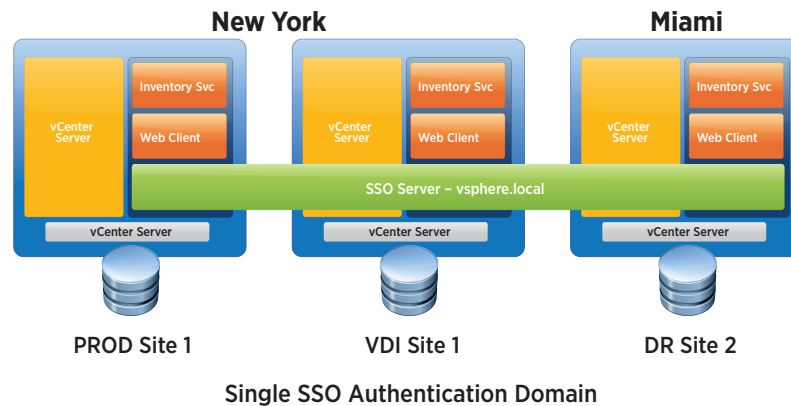
26. Return to the DVD menu and select the **vCenter Inventory Service** option listed under Custom Install.
27. Select **Install**.
28. Select **OK** for the required language.
29. On the Welcome to the Installation Wizard for VMware vCenter Inventory Service screen, select **Next**.
30. On the End User License Agreement screen, select **I accept the terms in the license agreement** and select **Next**.
31. On the Destination Folder screen, select **Change** and edit the path to install on the second volume (for example, D:\Program Files\VMware\Infrastructure\).
32. On the Local System Information screen, confirm the FQDN of the vCenter Inventory Service host name and select **Next**.

33. On the Configure Ports screen, select **Next**.
34. On the JVM Memory screen, select the appropriate inventory size for your environment, and select **Next**.
35. On the vCenter Single Sign-On Information screen, provide the **Password** entered in step 8 of the vCenter Single Sign-On installation.
36. If presented with a VMware vCenter Inventory Service dialogue box for the certificate, select **Yes** to accept and continue.
37. On the Ready to Install screen, select **Install**.
38. On the InstallShield Wizard Completed screen, select **Finish**.

vCenter Server

39. Return to the DVD menu and select the **vCenter Server** option listed under Custom Install.
40. Select **Install**.
41. Select **OK** for the required language.
42. On the Welcome to the Installation Wizard for VMware vCenter Server screen, select **Next**.
43. On the End User License Agreement screen, select **I accept the terms in the license agreement** and select **Next**.
44. On the License Key screen, enter your **license key** for vCenter Server. Alternatively, you can leave it blank to invoke a 60-day trial key. Select **Next**.
45. On the Database Options screen, select **Use an existing supported database** and select the **data source name** defined during the prerequisites. Select **Next**.
46. On the vCenter Server Service screen, provide a **Password** for the service account defined in the prerequisites.
47. On the vCenter Server Linked Mode Options screen, select **Create a standalone VMware vCenter server instance**.
48. On the Configure Ports screen, select **Next**.
49. On the JVM Memory screen, select the appropriate inventory size for your environment, and select **Next**.
50. On the vCenter Single Sign-On Information screen, provide the **Password** entered in step 8 of the vCenter Single Sign-On installation.
51. If presented with a VMware vCenter Server dialogue box for the certificate, select **Yes** to accept and continue.
52. On the vCenter Single Sign-On Information screen, select **Next**.
53. On the vCenter Inventory Service Information screen, select **Next**.
54. On the Destination Folder screen, select **Change** and edit the path to install on the second volume (for instance, D:\Program Files\VMware\Infrastructure\).
55. On the Ready to Install Program screen, select **Install**.
56. On the Installation Completed screen, select **Finish**.

You now have an operational vCenter server that you can log in to using a support browser and the following URL:
<http://<FQDN of vCenter hostname>:9443/>

Example 2: Deploying an Additional vCenter Server (Local or Remote)**Figure 4.** vCenter Server 5.5 – Deployment Best Practice (Multiple)

It is not uncommon to have multiple vCenter servers located either together in a single location or geographically separate from branch offices or disaster recovery sites. When deploying additional vCenter Server instances, the process is very similar to that of the single virtual machine shown in example 1. However, it is important to complete the following steps so that all additional vCenter Server instances participate in the same vCenter Single Sign-On security domain. This simplifies administration and offers the option to enable Linked Mode.

Prerequisites

1. Follow the prerequisites as shown in example 1 for any additional vCenter servers.

vCenter Single Sign-On

2. Follow steps 1–6 as shown in example 1.
3. On the vCenter Single Sign-On Information screen, select the second or third option, **vCenter Single Sign-On for an additional vCenter Server in an existing site** or **vCenter Single Sign-On for an additional vCenter Server with a new site**, depending on whether it is in the same location as an existing vCenter server or the first in a new location.
4. Provide a **Partner host name** for an existing vCenter Single Sign-On server to replicate from as well as the **Password** for the built-in administrator@vsphere.local account defined in step 8 from example 1. (Refer to the previously mentioned Knowledge Base article for a list of illegal characters.)
5. On the Partner Certificate screen, select **Continue** to accept the host certificate.
6. On the vCenter Single Sign-On Site Configuration screen, provide a **Site Name**. This can be based on location or organization (for instance, Disaster Recovery).
7. Follow and complete steps 10–13 from example 1 (with no changes).

vSphere Web Client

8. Follow and complete steps 14–25 from example 1 (with no changes).

vCenter Inventory Service

9. Follow and complete steps 26–38 from example 1 (with no changes).

vCenter Server

10. Follow and complete steps 39–56 from example 1 (with no changes).

Example 3: Deploying Multiple vCenter Servers with a Centralized vCenter Single Sign-On Server

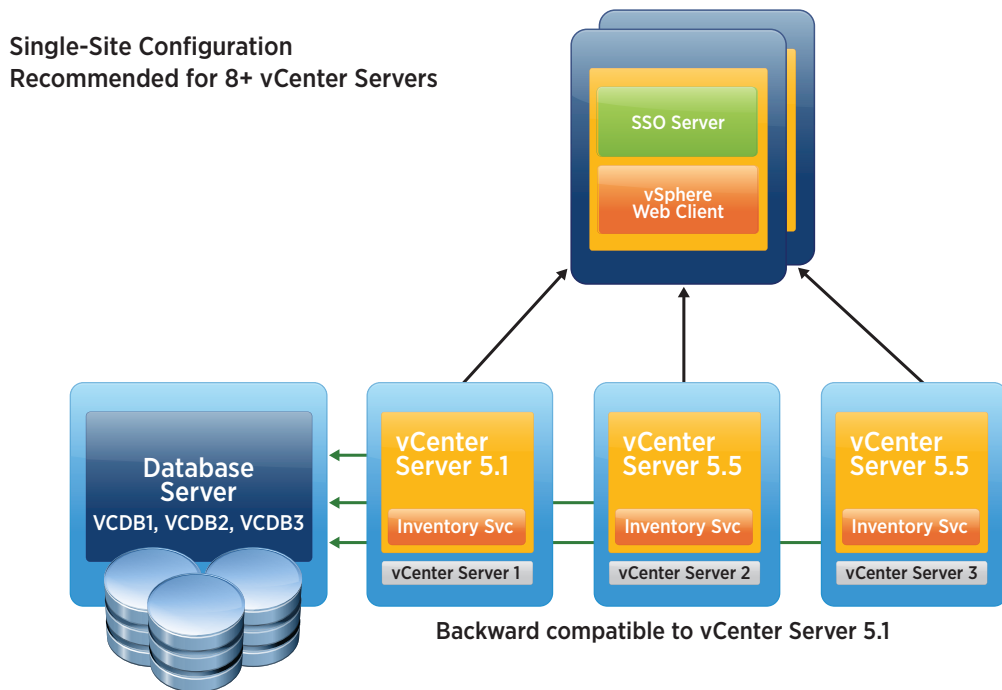


Figure 5. vCenter Server 5.5 – Deployment Best Practice (Multiple)

A common scenario in large enterprise environments is to have many vCenter servers local to a single location. If this is also coupled with remote sites (disaster recovery sites or branch offices) that also have vCenter servers, it is preferable to reduce the replication between instances and centralize vCenter Single Sign-On and the vSphere Web Client. This is recommended for environments that might have eight or more vCenter servers present in any single physical location.

Prerequisites

1. Follow the prerequisites as shown in example 1.
2. A third virtual machine will be required for vCenter Single Sign-On.

vCenter Single Sign-On

3. On the third virtual machine, follow steps 1-13 as shown in example 1.

vSphere Web Client

4. On the third virtual machine, follow and complete steps 14-25 in example 1 (with no changes).

vCenter Inventory Service

5. On the second virtual machine, follow and complete steps 26-34 in example 1 (with no changes).
6. On the vCenter Single Sign-On Information screen, provide the **Password** entered in step 8 of the vCenter Single Sign-On installation and **edit the Lookup Service URL** for the vCenter Single Sign-On server defined in step 3 of example 3.
7. Follow and complete the steps 35-38 of example 1 (with no changes).

vCenter Server

8. Follow and complete steps 39–49 of example 1 (with no changes).
9. On the vCenter Single Sign-On Information screen, provide the **Password** entered in step 8 of the vCenter Single Sign-On installation and **edit the Lookup Service URL** for the vCenter Single Sign-On server defined in step 3 of example 3.
10. Follow and complete steps 50–56 of example 1 (with no changes).

Upgrading vSphere 5.1 Architecture

With the vSphere 5.1 release, VMware recommended distribution of all of the vCenter Server components across multiple virtual machines for maximum performance. Although this practice did help with performance, it added complexity to the management of vCenter Server. Customers wanting to revert to a single-virtual-machine architecture as recommended previously might be put off by the thought of having to start over. The actual process of reverting the vCenter Server architecture to a single virtual machine is relatively straightforward.

The following example involves a fully distributed vSphere 5.1 environment (each component is deployed on a separate virtual machine):

1. Upgrade the current vCenter Single Sign-On 5.1 to version 5.5.
2. Deploy a new vCenter Single Sign-On server to the vCenter server or single virtual machine, specifying that vCenter Single Sign-On instance is an additional instance and placing it in the already created vsphere.local security domain.
3. On the vCenter server, install the vSphere Web Client 5.5 using the local vCenter Single Sign-On instance.
4. On the vCenter server, install the vCenter Inventory Service using the local vCenter Single Sign-On instance.
5. On the vCenter server, install the vCenter server using the local vCenter Single Sign-On instance.
6. Power off and remove the original separate vCenter Single Sign-On instance.

Post-Installation Tasks

After vCenter Server has been installed you are up and running. However, it is recommended to finalize the installation with some of the post-installation steps listed here.

Configure an Identity Source

On a fresh installation of vCenter Server, the only account generated is [administrator@vsphere.local](#), which is a vCenter administrator as well as a vCenter Server administrator. To populate vCenter Server permissions to other user accounts, you must first make them available to the vSphere environment by configuring vCenter Single Sign-On. To trust external identities such as Microsoft Active Directory or OpenLDAP, you must provide connection information. This is called an identity source. To add an identity source, follow these simple steps:

1. Open and log in to the vSphere Web Client using [administrator@vsphere.local](#).
2. Navigate to **administration\Single Sign-On** and select **configuration**.
3. Select the **Identity sources** tab.
4. Select the **plus sign**.
5. Select **Active Directory (integrated Windows authentication)**.
6. Provide a **domain name**.
7. Select **machine account**.
8. Select **Test connection**.
9. Select **Close**.

Permissions

With the introduction of vCenter Single Sign-On as an authentication service for the vSphere platform, permissions defined within the vSphere platform are now authenticated against the vCenter Single Sign-On service. With this in mind, it is important to highlight the correct way of assigning permissions at the vCenter level. In the past, the local operating system (OS) administrators group, by default, would be given the vCenter administrator role during installation. It became the practice to populate the local OS administrators group with additional local and domain accounts to provide vCenter administrator access. With vCenter Single Sign-On, it is required to assign the permissions based on the identity sources configured.

Here are some following examples:

- Domain accounts – domain\user name or group
- Local OS accounts – host name\user name or group

Any domain users that are members of a local OS group cannot authenticate unless they also have the permissions mapped as described.

Linked Mode

If you are deploying multiple vCenter Server instances, management of each vCenter Server instance as a separate entity might be considered unnecessary overhead. One helpful technology is Linked Mode. Enabling this places all vCenter Server instances running the same version into a Linked Mode group and provides a single-pane-of-glass management view of all linked vCenter Server instances. It also replicates the roles and permissions between vCenter Server instances. It is possible to enable Linked Mode during installation (step 47 during the vCenter Server installation). However, it is usually more successful post installation. To enable Linked Mode, follow these steps:

1. Select **Start > All Programs > VMware > vCenter Server Linked Mode Configuration**.
2. Select **Next**.
3. Select **Modify Linked Mode configuration** and select **Next**.
4. Select **Join this vCenter Server instance to an existing Linked Mode group or another instance** and select **Next**.
5. Enter the server name and LDAP port number of a remote vCenter Server instance that is a member of the group and select **Next**.
6. Select **Finish**.

Update SSL Certificates

When you are installing vCenter Single Sign-On, each component that is registered with it — including vCenter Single Sign-On itself — uses SSL to communicate between components and registered solutions. By default, VMware autogenerates the SSL certificates during the installation and upgrade process. These are sufficient for the operational security of most VMware customers. Some customers prefer to use their own self-signed or purchased SSL certificates. A tool has been developed to assist with the insertion of these certificates after vCenter Server installation. Due to the additional knowledge required to create and install self-signed certificates, VMware recommends reviewing the following VMware Knowledge Base articles:

[Deploying and Using the SSL Certificate Automation Tool](#)

(VMware Knowledge Base article 2057340)

[Generating Certificates for Use with the VMware SSL Certificate Automation Tool](#)

(VMware Knowledge Base article 2044696)

Availability

With vCenter Server now installed, it is best to review your recovery point objectives for keeping vCenter Server up and running. vCenter Server availability has been more important over recent releases due to the nature of the operations and functionality that vCenter Server provides. vSphere hosts still operate and their virtual machines do remain running when vCenter Server is down. However, the absence of vCenter Server greatly impacts the management and optimization of the vSphere environment. The type of availability required is based on your recovery time objective (RTO), and VMware solutions can offer various levels of protection.

VMware Data Protection

VMware vSphere Data Protection™ provides a disk-level backup and restore utilizing storage-based snapshots. With the release of vSphere Data Protection 5.5, VMware now provides the option of host-level backup. Now users can back up the vCenter Server environment using vSphere Data Protection and can employ the capability later to restore as necessary to a specified vSphere host.

vSphere HA

When deploying vCenter Server to a vSphere virtual machine environment, users can employ vSphere HA to enable recovery of vCenter Server virtual machines. vSphere HA monitors virtual machines via heartbeats from the VMware Tools™ package, and it can initiate a reboot of the virtual machine when the heartbeat is no longer received. vSphere HA requires vCenter Server availability to enable and configure recovery options for a virtual machine, but it will execute a recovery (a virtual machine restart) without the dependency on vCenter Server.

vCenter Server Heartbeat

VMware vCenter Server Heartbeat™ provides a richer availability model for the monitoring and redundancy of vCenter Server. Deployed on physical or virtualized vCenter Server instances, vCenter Server Heartbeat places vCenter Server into an active/passive architecture. In this scenario, vCenter Server is monitored for accessibility and the passive node is on standby for physical host or virtual machine failure. This helps further reduce vCenter Server downtime in the environment.

Conclusion

With the release of vCenter Server 5.5, there are many considerations to review prior to installing or upgrading. This document should give you a better understanding of the individual components, how vCenter Server utilizes these components and what to look out for when building a high-performing vCenter Server that can handle workloads of all sizes.

This paper provides recommendations for deployment of vCenter Server with the least amount of complexity. It guides users through the steps required to get them up and running and to start building out a virtual data center and provision workloads.



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

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-TWP-VCTR-SVR-5.5-DEPLY-GUIDE-USLET-101 Docsource: OIC - 13VM004.08