Installing Horizon Workspace

Horizon Workspace 1.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com
Contents

1 About Installing and Configuring VMware Horizon Workspace 5
   Installation Overview 6
   User Authentication 7
   IdP Discovery 8

2 System and Network Configuration Requirements 11

3 Preparing to Deploy Horizon Workspace 17
   Downloading Horizon Workspace 17
   Creating DNS Records and IP Addresses with Reverse Lookup 17
   Deployment Checklists 18

4 Deploying Horizon Workspace 23
   Deploying the OVA File in the vSphere Client 23
   Running the Configurator’s Virtual Appliance Interface 24
   Configuring an SMTP Server to Work with Horizon Workspace 25
   Increasing the vCenter Timeout Settings 26
   Deleting Unused Extensions from vCenter 26
   Running the Horizon Workspace Setup Wizard 26
   Configurator Information 30
   Horizon Workspace URLs 33
   Updating to the Latest Horizon Workspace Desktop Client 33
   Installing Horizon Workspace Client for Windows 34
   Installing Horizon Workspace Client for Mac 34

5 Configuration for Horizon Workspace Virtual Machines 35
   Adding Storage to the Data Virtual Appliance 35
   Adding Additional VMDKs for Storage 35
   Adding Network Attached Storage for Storage 36
   Managing Data Storage Volumes 37
   Configuring Data Preview 37
   Installing LibreOffice Preview 37
   Installing Microsoft Windows Preview 38
   Configuring a Multi-domain Active Directory Domain Service Forest 39
   Customizing the Demo User Store 41
   Adding a User to the Demo User Store 42
   Adding Groups and Assigning Users to Groups in the Demo User Store 43
   Integrating VMware ThinApp 44
   Creating a Windows Network Share for ThinApp Packages 44
   Configuring ThinApp Packages for Horizon Workspace 45
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating VMware View</td>
<td>46</td>
</tr>
<tr>
<td>Joining Active Directory Domain</td>
<td>47</td>
</tr>
<tr>
<td>Syncing View Pools</td>
<td>48</td>
</tr>
<tr>
<td>Configuring SAML Authentication</td>
<td>48</td>
</tr>
<tr>
<td>Setting Proxy Server Settings for Manager</td>
<td>50</td>
</tr>
<tr>
<td>Logging Information</td>
<td>50</td>
</tr>
<tr>
<td>6 Advanced Configuration for Horizon Workspace Virtual Machines</td>
<td>53</td>
</tr>
<tr>
<td>Enabling External Access to Horizon Workspace</td>
<td>53</td>
</tr>
<tr>
<td>Establishing SSL Trust between Horizon Workspace vApp and Load Balancer</td>
<td>55</td>
</tr>
<tr>
<td>Enabling AUDIT Events via Proxy Server</td>
<td>56</td>
</tr>
<tr>
<td>Configuring an External Database</td>
<td>56</td>
</tr>
<tr>
<td>Configuring Redundancy/Failover for Horizon Workspace Virtual Machines</td>
<td>58</td>
</tr>
<tr>
<td>Multiple gateway-va Virtual Machines</td>
<td>59</td>
</tr>
<tr>
<td>Multiple service-va Virtual Machines</td>
<td>59</td>
</tr>
<tr>
<td>Multiple connector-va Virtual Machines</td>
<td>61</td>
</tr>
<tr>
<td>Multiple data-va Virtual Machines</td>
<td>65</td>
</tr>
<tr>
<td>Configuring SecurID for Horizon Workspace</td>
<td>69</td>
</tr>
<tr>
<td>Preparing the RSA SecurID Server for the Connector</td>
<td>70</td>
</tr>
<tr>
<td>Configuring SecurID with the Connector Web Interface</td>
<td>70</td>
</tr>
<tr>
<td>Configuring Kerberos for Horizon Workspace</td>
<td>71</td>
</tr>
<tr>
<td>Configuring Internet Explorer to Access the Web Interface</td>
<td>72</td>
</tr>
<tr>
<td>Configuring Firefox to Access the Web Interface</td>
<td>73</td>
</tr>
<tr>
<td>Configuring Chrome Browser to Access the Web Interface</td>
<td>74</td>
</tr>
<tr>
<td>Using SSL Certificates in Horizon Workspace</td>
<td>75</td>
</tr>
<tr>
<td>Applying an SSL Certificate from a Major Certificate Authority</td>
<td>75</td>
</tr>
<tr>
<td>Applying an SSL Certificate from a Private Certificate Authority</td>
<td>76</td>
</tr>
<tr>
<td>Adjusting Java Heap Size for Improved Performance</td>
<td>76</td>
</tr>
<tr>
<td>Updating Java Heap Size on the Data Virtual Machine</td>
<td>77</td>
</tr>
<tr>
<td>Updating Java Heap Size on the Connector Virtual Machine</td>
<td>77</td>
</tr>
</tbody>
</table>

Index: 79
About Installing and Configuring VMware Horizon Workspace

The *VMware Horizon Workspace Installation and Configuration Guide* guides you through the installation and configuration process. When the installation is finished, you can use VMware Horizon Workspace to entitle and access software as a service (SaaS) applications, Windows applications, files, and View desktops.

Horizon Workspace is a multiple virtual machine vApp, distributed as an Open Virtualization Archive (OVA) file. You can deploy the vApp to vCenter. The vApp includes the following virtual appliances.

### Table 1-1. Horizon Workspace Server Components

<table>
<thead>
<tr>
<th>Horizon Workspace Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Workspace Configurator Virtual Appliance (configurator-va)</td>
<td>You start configuring Horizon Workspace with this virtual appliance, using both the Configurator virtual appliance interface and the Configurator Web interface. The configurations you make with the Configurator are distributed to the other virtual appliances in the vApp.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Manager Virtual Appliance (service-va)</td>
<td>Horizon Workspace Manager handles ThinApp package synchronization and gives you access to the Administrator Web interface, from which you can manage users, groups, and resources.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Connector Virtual Appliance (connector-va)</td>
<td>Horizon Workspace Connector provides the following services: user authentication (identity provider), directory synchronization, ThinApp-catalog loading, and View pool synchronization.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Data Virtual Appliance (data-va)</td>
<td>Horizon Workspace Data Virtual Appliance controls the file storage and sharing service, stores users’ data (files), and synchronizes users’ data across multiple devices.</td>
</tr>
<tr>
<td>VMware Horizon Workspace Gateway Virtual Appliance (gateway-va)</td>
<td>Horizon Workspace Gateway Virtual Appliance is the single endpoint for all end user communication. User requests come to the gateway-va virtual machine, which then routes the request to the appropriate virtual appliance.</td>
</tr>
</tbody>
</table>

### Intended Audience

This information is intended for system and functional administrators of Horizon Workspace. The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter and ESX, networking concepts, Active Directory servers, Simple Mail Transfer Protocol (SMTP), and NTP servers. SUSE Linux 11 is the underlying operating system for the virtual appliances in the vApp. Knowledge of other technologies, such as VMware ThinApp, RSA SecurID, and Active Directory, is helpful if you plan to implement these features.
This chapter includes the following topics:

- “Installation Overview,” on page 6
- “User Authentication,” on page 7
- “IdP Discovery,” on page 8

### Installation Overview

Each deployment includes different requirements. You can select the appropriate installation tasks for your deployment.

#### Figure 1-1. VMware Horizon Workspace Architecture Diagram

The installation includes the following tasks:

**Procedure**

User Authentication

The Connector acts as an identity provider within your network, creating an in-network federation authority that communicates with Horizon Workspace using SAML 2.0 assertions. The Connector authenticates the user with Active Directory within the enterprise network (using existing network security).

The following authentication methods are supported by Horizon Workspace: Active Directory username/password, Kerberos, and RSA SecurID.

<table>
<thead>
<tr>
<th>Horizon Workspace Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username/password</td>
<td>Active Directory username/password authentication is the default user authentication method. This method authenticates users directly against your Active Directory.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>When properly configured, Kerberos authentication provides Windows users with single sign-on access to Horizon Workspace, eliminating the requirement for Windows users to log in to Horizon Workspace after they log in to the enterprise network. The Connector validates user desktop credentials using Kerberos tickets distributed by the key distribution center (KDC).</td>
</tr>
<tr>
<td>RSA SecurID</td>
<td>RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is the recommended authentication method for users accessing Horizon Workspace from outside the enterprise network.</td>
</tr>
</tbody>
</table>

Username/password authentication is the authentication method in use when you initially deploy Horizon Workspace. The username/password authentication method can authenticate users regardless of whether users are inside or outside the enterprise network. To provide user access to Horizon Workspace from outside the enterprise network, you can either require VPN access or you can install Horizon Workspace in a manner that allows Internet access.

If you decide to use username/password authentication to provide users outside the enterprise network access to Horizon Workspace, you can configure Horizon Workspace in one of the following ways:

- Install a reverse proxy server in the DMZ pointing to the Gateway virtual appliance.
- Configure firewall port forwarding or router port forwarding to point to the Gateway virtual appliance.

To implement Kerberos authentication or RSA SecurID authentication, you must deploy one or more additional Connector instances. To implement both Kerberos authentication and RSA SecurID authentication, you first deploy Horizon Workspace, which includes all the Horizon Workspace virtual appliances. See “Multiple data-center Virtual Machines,” on page 65 to create additional identity providers.

You can configure one or more Connector instances to handle Kerberos authentication and one or more Connector instances to handle RSA SecurID authentication. Configuring any single Connector instance to handle both Kerberos authentication and RSA SecurID authentication is not a best practice. When you use more than one Connector instance in your deployment, you must use the Administrator Web interface to configure IdP discovery.

If you decide to use Kerberos authentication to seamlessly authenticate Windows users (applies to users inside the enterprise network only) to Horizon Workspace, issue the `hznAdminTool addvm` command in the configurator-va virtual machine to add a new connector-va virtual machine. Since the Connector acts as an identity provider, when you add a new Connector instance you are adding a new identity provider instance.
If you decide to use RSA SecurID authentication to provide users outside the enterprise network access to Horizon Workspace, you must add the connector-va virtual machine using the `addvm` option of the `hznAdminTool` command. This command creates an additional identity provider. You can then configure the new identity provider using the Horizon Workspace Administrator Web interface.

The supported authentication types can be used in a variety of ways to provide users, both inside and outside the enterprise network, access to Horizon Workspace.

**Table 1-2. Overview of Providing User Access to Horizon Workspace**

<table>
<thead>
<tr>
<th>User Access From Inside the Enterprise Network</th>
<th>User Access From Outside the Enterprise Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Username/password authentication: Functions by default. No additional Connector instances are required for this authentication method when users are inside the enterprise network.</td>
<td>- Username/password authentication: To implement username/password authentication for users outside the enterprise network, you must enable Internet access to the Gateway virtual appliance. VPN is an option, too.</td>
</tr>
<tr>
<td>- Kerberos authentication: Requires an additional Connector instance.</td>
<td>- Kerberos authentication: Not applicable. This authentication method is not an option for authenticating users outside the enterprise network.</td>
</tr>
<tr>
<td>- RSA SecurID authentication: Not recommended. This authentication method is not recommended for authenticating users who are inside the enterprise network.</td>
<td>- RSA SecurID authentication: When practical, this authentication method is preferred for authenticating users outside the network. The best practice is to install a Connector instance dedicated to RSA SecurID authentication.</td>
</tr>
</tbody>
</table>

**NOTE** Horizon Workspace handles RSA SecurID authentication and Kerberos authentication failures differently:

- If Kerberos authentication fails for any reason, the Connector falls back to username/password authentication. In such cases, users are presented with a login page that prompts them for their username and password to access Horizon Workspace. The Connector then validates users against the directory server.

- If RSA SecurID authentication fails, the Connector does not fall back to username/password authentication. Since RSA SecurID is only recommended for users outside the enterprise network, such users will not be able to access Horizon Workspace until the cause of failure is resolved.

**IdP Discovery**

IdP discovery matches users from specific IP addresses with their corresponding identity providers (Connector instances). For example, users with IP addresses outside the enterprise network might be directed to a Connector instance dedicated to RSA SecurID authentication, while internal users might be directed to a Connector instance dedicated to Kerberos authentication.

Though different users are directed to different Connector instances, you provide all users with a single Horizon Workspace URL since IdP discovery does the work behind the scenes to locate the appropriate Connector instance.

The default IdP discovery configuration applies to the default Horizon Workspace deployment, which uses username/password authentication with a single Connector instance. If you deploy Horizon Workspace in this manner, you do not need to change the IdP discovery configuration.

When you deploy multiple Connector instances using the `addvm` option of the `hznAdminTool` command for the purpose of maintaining multiple identity providers, you need to use the Horizon Workspace Administrator Web interface to access the **Settings > Identity Providers** page, where you must perform the following:

- Locate each additional Connector instance name in the list of identity providers. When you use the `addvm` option of the `hznAdminTool` command to create a new Connector instance, that Connector instance name is added to this page.
Edit the order of the identity providers as necessary. The order in which the corresponding Connector instances are listed in Horizon Workspace is important if the IP ranges overlap. In such cases, the first Connector instance in the list to include an IP address is given precedence.

**CAUTION** When you remove or reset a Connector instance, you must remove the corresponding Connector name from the **Identity Providers** page.

You can deploy Horizon Workspace with IdP Discovery in a variety of ways, one of which is summarized in the example that follows.

**External RSA SecurID and Internal Kerberos Authentication Example of IdP Discovery**

This is one possible way to configure IdP Discovery for Kerberos and SecurID in the same Horizon Workspace deployment.

- **Internal - First Connector instance:** You configure Kerberos for this Connector instance. In the Horizon Workspace Administrator Web interface, on the Identity Providers page, you configure IP address ranges to include users within the enterprise network.

- **External - Second Connector instance:** You configure SecurID for this Connector instance. In Horizon Workspace, you configure a single IP address range that includes all possible users. Therefore, you set the IP address range from 0.0.0.0 to 255.255.255.255.

The result of this configuration is that users attempting to access Horizon Workspace from inside the enterprise network are redirected to the first Connector instance and authenticated with Kerberos or username/password authentication while users outside the enterprise network are redirected to the second Connector instance and authenticated with SecurID authentication.

**Note** When Horizon Workspace users invite an external user, either a directory server user not synched to Horizon Workspace or someone outside of the enterprise, the invited user is created as a virtual user. The virtual users feature is an optional feature that applies solely to the Data service, the file storage and sharing service. Virtual users are not prompted for SecurID credentials even when the virtual users are external to your enterprise and are redirected to a Connector instance that enforces SecurID authentication.
System and Network Configuration Requirements

When you install and configure Horizon Workspace, you install the Configurator (configurator-va), Manager (service-va), Connector (connector-va), Data (data-va), and Gateway (gateway-va) virtual appliances and use the interface of the Configurator virtual appliance and the Web interface for configuration purposes.

Prerequisites

The following components are required:

- VMware vCenter and one or more ESX servers to deploy Horizon Workspace vApp. For a list of supported vSphere versions, see the Release Notes.
- The VMware vSphere Client provides access to the virtual appliance interface. The vSphere Client is required to deploy the Open Virtual Appliance (OVA) file to vSphere and to access the deployed virtual appliance remotely to configure networking.
- The appropriate VMware licenses.

Consider your entire Horizon Workspace deployment, including how you integrate Horizon Workspace when you make decisions about hardware, resources, and network requirements. For example, you need more hardware for larger deployments.

Virtual Appliance Requirements

Ensure that the resources allocated to the virtual appliances meet the minimum requirements.

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Virtual Appliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>1</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>1GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>9GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager Virtual Appliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>4GB</td>
</tr>
</tbody>
</table>
### Table 2-2. Manager Virtual Appliance (service-va) Requirements (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk space</td>
<td>36GB</td>
</tr>
</tbody>
</table>

**Additional notes**
- A postgres database is included in the virtual appliance to make testing easier. For production, you must use an external database server (vPostgres Version 9.1).
- **Note**: You can convert (and scale) an internal postgres database to an external postgres database at a later time.
- External database sizing information: 64GB for first 100,000 users. Add 20GB for each additional 10,000 users.
- Storage: 32GB

### Table 2-3. Configurator Virtual Appliance (configurator-va) Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>1GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>5GB</td>
</tr>
</tbody>
</table>

### Table 2-4. Connector Virtual Appliance (connector-va) Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>4GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>12GB</td>
</tr>
</tbody>
</table>

### Table 2-5. Data Virtual Appliance (data-va) Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>Random-access memory</td>
<td>4GB</td>
</tr>
</tbody>
</table>
Table 2-5. Data Virtual Appliance (data-va) Requirements (Continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk space</td>
<td>175GB</td>
</tr>
<tr>
<td>Additional notes</td>
<td>Stores all the files uploaded by users. See “Adding Storage to the Data Virtual Appliance,” on page 35 for information on storage best practices.</td>
</tr>
</tbody>
</table>

**NOTE** The service-va virtual machine automatically adjusts the Java heap size when you add memory. You must adjust the Java heap size manually for the gateway-va, connector-va, and configurator-va virtual machines. See “Adjusting Java Heap Size for Improved Performance,” on page 76.

**IMPORTANT** It is recommended that each data-va virtual machine serve no more than 1,000 users. If your deployment includes multiple data-va virtual machines with 1,000 users each, you must configure all the other virtual machines using the requirements shown in the Recommended Virtual Machine Requirements table.

Table 2-6. Recommended Virtual Machine Requirements

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>CPU</th>
<th>RAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>configurator-va</td>
<td>1 vCPU</td>
<td>1GB RAM</td>
</tr>
<tr>
<td>connector-va</td>
<td>2 vCPU</td>
<td>4GB RAM</td>
</tr>
<tr>
<td>manager-va</td>
<td>6 vCPU</td>
<td>8GB RAM</td>
</tr>
<tr>
<td>gateway-va</td>
<td>6 vCPU</td>
<td>32GB RAM</td>
</tr>
<tr>
<td>data-va</td>
<td>6 vCPU</td>
<td>32GB RAM</td>
</tr>
</tbody>
</table>

**Network Configuration Requirements**

All the virtual appliances refer to each other by their hostnames. As a result, each IP address must map to a hostname that you can search for from each machine. Ensure that each machine can search for the Horizon Workspace FQDN.

The Connector virtual appliance might need to join the Windows domain if Kerberos, View, or ThinApp functions are enabled. In that case, the Connector hostname must be in the same domain as the Active Directory.

Table 2-7. Network Configuration Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP pool</td>
<td>Must be configured in vCenter and contain the appropriate number of free static IP addresses.</td>
</tr>
<tr>
<td></td>
<td>Must have a DNS server specified. Even though the interface allows you to specify multiple DNS servers, only one must be defined.</td>
</tr>
<tr>
<td></td>
<td>Must specify the DNS domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> IP pool network configuration is required. Horizon Workspace does not support transient addresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS records and IP addresses</th>
<th>Add DNS records and IP addresses with reverse lookup for each virtual appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall port</td>
<td>Ensure that the inbound firewall port 443 is open for users outside the enterprise network to Horizon Workspace.</td>
</tr>
</tbody>
</table>

**Port Requirements**

The following diagram depicts Horizon Workspace port requirements and represents the possible scenarios for connecting with the connector-va virtual machine. Your deployment will include only a subset of these. Here are two potential scenarios:

- To sync users and groups, the responsible connector-va virtual machine must connect to Active Directory.
To sync with ThinApp, the responsible connector-va virtual machine must connect to the ThinApp Repository share.

Figure 2-1. Horizon Workspace Ports

* Default values are shown. These ports are configurable.
** Every virtual appliance must have access to the DNS server on port 53.

### Hardware Requirements for ESX Server

Ensure that the environment for the host and the vSphere instance that runs Horizon Workspace virtual appliance meets the minimum hardware requirements.

**Note** You must turn on time sync at the host level using an NTP server. Otherwise, a time drift will occur between the virtual machines.
Table 2-8. Minimum Horizon Workspace Hardware Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 Intel Quad Cores, 3.0GHz, 4MB Cache</td>
</tr>
<tr>
<td>RAM</td>
<td>16GB DDR2 1066 MHz, ECC and registered</td>
</tr>
<tr>
<td>On-board LAN</td>
<td>One 10/100/1000Base-TX port</td>
</tr>
<tr>
<td>Storage</td>
<td>500GB</td>
</tr>
</tbody>
</table>

**Note**: Storage requirements vary per deployment based on the number of users. See “Adding Storage to the Data Virtual Appliance,” on page 35.
Preparing to Deploy Horizon Workspace

Before you deploy Horizon Workspace, you must prepare your environment. This preparation includes downloading Horizon Workspace and creating DNS records and IP addresses with reverse lookup.

Prerequisites

- Before you proceed with your deployment, review Chapter 6, “Advanced Configuration for Horizon Workspace Virtual Machines,” on page 53. If you configure any of these options, the way you deploy might change.
- SMTP server is required.

This chapter includes the following topics:

- “Downloading Horizon Workspace,” on page 17
- “Creating DNS Records and IP Addresses with Reverse Lookup,” on page 17
- “Deployment Checklists,” on page 18

Downloading Horizon Workspace

Download the Horizon Workspace OVA package file from the VMware Web site.

Creating DNS Records and IP Addresses with Reverse Lookup

A DNS entry and a static IP address that uses reverse lookup must be available for each virtual appliance in the vApp. Because each company administers their IP addresses and DNS records differently, before you begin your installation, consult your network administrator and request five DNS records and five IP addresses that use reverse lookup. You must have one IP address each for the Configurator (configurator-va), the Manager (service-va), the Connector (connector-va), the Data (data-va), and the Gateway (gateway-va) virtual appliances.

Reverse Lookup and IP Addresses

Horizon Workspace requires reverse lookup. You must define a PTR record on the DNS server so each virtual appliance uses the correct network configuration. If reverse lookup is not properly configured, Horizon Workspace installation fails.

You can use the following sample list of DNS records when you talk to your network administrator. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.
Table 3-1. Examples of Forward DNS Records and IP Addresses

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Resource Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-gateway-va.company.com</td>
<td>A</td>
<td>10.28.128.1</td>
</tr>
<tr>
<td>my-configurator-va.company.com</td>
<td>A</td>
<td>10.28.128.2</td>
</tr>
<tr>
<td>my-service-va.company.com</td>
<td>A</td>
<td>10.28.128.3</td>
</tr>
<tr>
<td>my-connector-va.company.com</td>
<td>A</td>
<td>10.28.128.4</td>
</tr>
<tr>
<td>my-data-va.company.com</td>
<td>A</td>
<td>10.28.128.5</td>
</tr>
</tbody>
</table>

This example shows reverse DNS records and IP addresses.

Table 3-2. Examples of Reverse DNS Records and IP Addresses

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Resource Type</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-gateway-va.company.com</td>
</tr>
<tr>
<td>2.128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-configurator-va.company.com</td>
</tr>
<tr>
<td>3.128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-service-va.company.com</td>
</tr>
<tr>
<td>4.128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-connector-va.company.com</td>
</tr>
<tr>
<td>5.128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-data-va.company.com</td>
</tr>
</tbody>
</table>

NOTE After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IP_address` must resolve to DNS name lookup.

Using a Unix/Linux-based DNS Server

If you are using a Unix/Linux-based DNS server and plan to join Horizon Workspace to the Active Directory domain, make sure that the appropriate service (SRV) resource records are created for each Active Directory domain controller.

Deployment Checklists

You can use Horizon Workspace deployment checklists to gather the necessary information to install Horizon Workspace. Depending on your deployment, you might only need a portion of the network information for your virtual machines when you create the static IP addresses in the DNS before the installation and during a Horizon Workspace installation.

Information for Horizon Workspace Fully Qualified Domain Name


Table 3-3. Horizon Workspace Fully Qualified Domain Name (FQDN) Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Workspace FQDN</td>
<td></td>
</tr>
</tbody>
</table>

Network Information for Configurator (configurator-va)

Table 3-4. Configurator Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>DNS name</td>
<td></td>
</tr>
</tbody>
</table>
Network Information for Manager (service-va)

Table 3-5. Manager (service-va) Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>DNS name</td>
<td></td>
</tr>
</tbody>
</table>

Network Information for Connector (connector-va)

If the Connector must join the Active Directory domain, verify that its hostname is valid in that domain.

Table 3-6. Connector Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>DNS name</td>
<td></td>
</tr>
</tbody>
</table>

Network Information for Data (data-va)

Table 3-7. Data Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>DNS name</td>
<td></td>
</tr>
</tbody>
</table>

Network Information for Gateway (gateway-va)

Table 3-8. Gateway Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>DNS name</td>
<td></td>
</tr>
</tbody>
</table>

Network Information for IP Pools

Table 3-9. IP Pools Network Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>DNS server (Only one DNS server is supported.)</td>
<td></td>
</tr>
<tr>
<td>DNS domain name</td>
<td></td>
</tr>
</tbody>
</table>
Active Directory Domain Controller

Table 3-10. Active Directory Domain Controller Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory server name</td>
<td></td>
</tr>
<tr>
<td>Active Directory domain name</td>
<td></td>
</tr>
<tr>
<td>Bind DN username and password</td>
<td></td>
</tr>
<tr>
<td>Base DN</td>
<td></td>
</tr>
<tr>
<td>Active Directory username and password</td>
<td>(Must have privileges to join computers to the domain.)</td>
</tr>
</tbody>
</table>

SMTP Server

Table 3-11. SMTP Server Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server hostname</td>
<td></td>
</tr>
<tr>
<td>SMTP server port number</td>
<td></td>
</tr>
</tbody>
</table>

vCenter Credentials

Table 3-12. vCenter Credentials Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter hostname</td>
<td></td>
</tr>
<tr>
<td>vCenter port number</td>
<td></td>
</tr>
<tr>
<td>vCenter administrator username</td>
<td></td>
</tr>
<tr>
<td>vCenter administrator password</td>
<td></td>
</tr>
</tbody>
</table>

SSL Certificate (Optional)

Table 3-13. SSL Certificate Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL certificate</td>
<td></td>
</tr>
<tr>
<td>Private key</td>
<td></td>
</tr>
</tbody>
</table>

Note The SSL certificate is optional. You can add an SSL certificate after you deploy Horizon Workspace.

HorizonWorkspace License Key

Table 3-14. Horizon Workspace License Key Information Checklist

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Workspace license key</td>
<td></td>
</tr>
</tbody>
</table>
### Microsoft Windows Preview

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows server IP address</td>
<td></td>
</tr>
</tbody>
</table>

### External Database

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database hostname</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>
Deploying Horizon Workspace

You are ready to deploy Horizon Workspace. You can use the deployment checklists you filled in to complete the installation.

Prerequisites

- If the ESX host is part of a cluster, enable DRS in the cluster. If an ESX host belongs to a non-DRS cluster, all resource pool functionality is disabled. Deploying a multi-virtual machine vApp creates a resource pool automatically. No reservation settings are added to the resource pool, so, it does not have an impact on the other hosts/virtual machines in the cluster.
- Deploy Horizon Workspace using vCenter server. If you deploy Horizon Workspace on an ESX host directly, the installation will fail.

This chapter includes the following topics:

- “Deploying the OVA File in the vSphere Client,” on page 23
- “Running the Configurator’s Virtual Appliance Interface,” on page 24
- “Running the Horizon Workspace Setup Wizard,” on page 26
- “Updating to the Latest Horizon Workspace Desktop Client,” on page 33

Deploying the OVA File in the vSphere Client

To start the Horizon Workspace installation, you must deploy the OVA file using vSphere Client.

Prerequisites

- Log in to the vSphere Client.

Procedure

1. Select File > Deploy OVF Template.

Respond to the prompts with information specific to your deployment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Type a URL or navigate to the OVA package location.</td>
</tr>
<tr>
<td>OVF template details</td>
<td>Verify that you pointed to the correct OVA template for this installation.</td>
</tr>
<tr>
<td>End user license agreement</td>
<td>Accept the end user license agreement.</td>
</tr>
<tr>
<td>Name and location</td>
<td>Name the vApp.</td>
</tr>
</tbody>
</table>
Table 4-1. Deploy OVF Template Information (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Select the location to store the virtual machine files.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Select the provisioning type.</td>
</tr>
<tr>
<td>Network mapping</td>
<td>Select the network for each virtual machine to use. Ensure you select the</td>
</tr>
<tr>
<td></td>
<td>virtual machine network associated with the IP pool you created.</td>
</tr>
<tr>
<td>IP address allocation</td>
<td>Select <strong>Fixed</strong> and type a static IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: DHCP and transient IP addresses are not supported in Horizon</td>
</tr>
<tr>
<td></td>
<td>Workspace. Only static IP addresses with reverse lookup are enabled.</td>
</tr>
<tr>
<td>Properties</td>
<td>■ Select the correct time zone.</td>
</tr>
<tr>
<td></td>
<td>■ Type the static IP address for each virtual appliance. The configurator-va</td>
</tr>
<tr>
<td></td>
<td>service-va, connector-va, data-va, and gateway-va virtual machines each</td>
</tr>
<tr>
<td></td>
<td>use a static IP address.</td>
</tr>
</tbody>
</table>

2. Click **Power On After Deployment** and click **Finish**.

**NOTE**: Depending on your network speed, this deployment can take 30 minutes or more.

3. Verify that the configurator-va virtual machine is fully powered on.

**What to do next**

Run the Configurator’s virtual appliance interface to start the initial Horizon Workspace configurations, such as the network, SSL, and vCenter extension configuration.

**Running the Configurator’s Virtual Appliance Interface**

Use Horizon Workspace virtual appliance interface to make initial configurations to Horizon Workspace, such as the network, SSL, and vCenter extension configuration.

The Configurator virtual appliance interface leads you through the basic configuration. Once you complete the wizard, you must run the Web-based Horizon Workspace Setup wizard. You can return to the Configurator’s virtual appliance interface at any time to update these settings or to perform other configurations. The advanced configuration tasks are discussed in Chapter 6, “Advanced Configuration for Horizon Workspace Virtual Machines,” on page 53.

**IMPORTANT**: During deployment, leave the virtual appliances, except the configurator-va virtual machine, powered off. Before deployment finishes, the virtual appliances will be powered on automatically. If the virtual appliances are already on, an error occurs.

**Prerequisites**

■ Log in to vSphere Client.

**Procedure**

1. Select the vApp you deployed.
2. Open the Console tab.
3. Type **y** to start the configuration.
Table 4-2. Configurator Virtual Appliance Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global root password</td>
<td>Type and confirm the global root password you want to use for all five virtual appliances in Horizon Workspace.</td>
</tr>
<tr>
<td>SMTP server name</td>
<td>Type the SMTP server name. See “Configuring an SMTP Server to Work with Horizon Workspace,” on page 25. If you want to change your SMTP settings after you install Horizon Workspace, see the CLI Commands for Horizon Workspace Data Guide.</td>
</tr>
<tr>
<td>SMTP port number</td>
<td>Type the SMTP port number.</td>
</tr>
<tr>
<td>Horizon Workspace FQDN</td>
<td>Type the Horizon Workspace FQDN. This domain will be the entry point for end users. <strong>Important</strong> After you install Horizon Workspace, you cannot reconfigure an internal gateway as an external gateway or change the name. If you want to reconfigure the gateway as external or change the name of the gateway, you must reinstall the vApp.</td>
</tr>
<tr>
<td>Horizon Workspace port number</td>
<td>Type the Horizon Workspace port number. The default port number is 443.</td>
</tr>
<tr>
<td>vCenter IP address</td>
<td>Type the vCenter IP address.</td>
</tr>
<tr>
<td>vCenter port number</td>
<td>Type the vCenter port number.</td>
</tr>
<tr>
<td>vCenter admin username</td>
<td>Type the vCenter administrator's username. The vCenter administrator only needs privileges to Horizon Workspace vApp or the resource pool that contains Horizon Workspace vApp. See <a href="http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-93B962A7-93FA-4E96-B68F-AE66D3D6C663.html">http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-93B962A7-93FA-4E96-B68F-AE66D3D6C663.html</a> for instructions on how to assign the administrator role.</td>
</tr>
<tr>
<td>vCenter admin password</td>
<td>Type and confirm the vCenter administrator's password.</td>
</tr>
<tr>
<td>Is this correct?</td>
<td>Type y if all the information is correct.</td>
</tr>
</tbody>
</table>

The Configurator virtual appliance processes your information. Depending on your network speed, this process can take up to 20 minutes or more. Once it successfully runs, you must run Horizon Workspace Setup wizard.

**CAUTION** If, for example, a networking error occurs and the hostname cannot be uniquely resolved using reverse DNS, the Configurator virtual appliance wizard will stop. In that case, you must fix the networking problems, and reboot the configurator-va virtual machine. Then, you can continue with the wizard. It is important to reboot so the new network settings are available to the Configurator.

**Configuring an SMTP Server to Work with Horizon Workspace**

You must configure the SMTP server to allow the data-va virtual machine to send emails and alerts.

If the data-va node is not on the same subnet as the SMTP server, your mail transfer agent (MTA) cannot relay email. When you configure your SMTP server to use the IP address or the subnet of the data-va node, your MTA can relay mail.

If you use a Zimbra server as your SMTP server, configure the Zimbra server using the Zimbra Admin Console.

Note Depending on the version of Zimbra you are using, the names for buttons, fields, and so on might be different.

Prerequisites

In your DNS server, ensure that the SMTP server hostname has a reverse DNS lookup.

Procedure

1. Click Configure Servers > MTA > MTA Trusted Networks.
2. Type the IP address or subnet address of the data-va node.

Increasing the vCenter Timeout Settings

In an environment with heavy traffic, a vCenter quiesce timeout problem can occur that might cause your deployment to fail. When this happens, an "Unable to execute command," error appears.

The vSphere logs show that this was caused by a, "Failed to quiesce virtual machine," error. You can prevent the error by increasing the vCenter timeout settings. See the KB article Increasing vCenter Server Timeout Settings at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002721. The default values range from 30 to 120 seconds. Increase the timeout values and redeploy.

Deleting Unused Extensions from vCenter

If you deploy Horizon Workspace multiple times after failures or upgrades, Horizon Workspace creates multiple extensions in vCenter.

You can remove the unused extensions using this procedure.

Procedure

1. Log in to this URL as a vCenter administrator at https://vcenterFQDN/mob/?moid=ExtensionManager.
2. Use the UnregisterExtension to remove the unused extension.
3. Look at the most recent heartbeat to determine the current extension.

If a deployment fails or you upgrade Horizon Workspace, run this procedure to remove unused vCenter extensions.

Running the Horizon Workspace Setup Wizard

The Horizon Workspace Setup wizard makes the initial configurations to Horizon Workspace.

Start the Horizon Workspace Setup Wizard

The Horizon Workspace Setup wizard runs in your browser using the configurator-va virtual machine hostname, for example, https://configurator-va.company.com.

Security Exceptions

You must set a security exception when you see the message, “This Connection is Untrusted.” See the instructions for your browser on setting security exceptions.
Setup

After you enter the license key provided by VMware, you create an administrator password.

This administrator account is a special account outside of your enterprise directory. If your connection to Active Directory is unavailable, you can use this account. You will also use this username and password to access the Horizon Workspace Administrator, Configurator, and Connector Web interfaces directly. See “Horizon Workspace URLs,” on page 33 for more information.

After you have performed the initial configuration of Horizon Workspace, you can use the Configurator Web interface to perform advanced configuration tasks, such as to change the administrator password.

Database Connection Setup

You can select an Internal Database or an External Database. If you choose an external database, see Configure an External Database.

**IMPORTANT** In reference to database storage, you can use the internal database for the proof-of-concept phase. Do not use the internal database server in production. For production, install and configure an external database server.

Directory

You enter your configuration information on the Directory page to establish a connection to Active Directory, which is used to verify a user’s credentials when they attempt to log in to Horizon Workspace.

If your deployment uses a multi-domain Active Directory Domain Server (AD DS) forest, see “Configuring a Multi-domain Active Directory Domain Service Forest,” on page 39.

After you select the correct Directory Type in the Horizon Workspace Setup wizard, you must enter the correct directory information for your environment. Horizon Workspace includes the directory types, Active Directory and Demo User Store (for evaluation only).

**Table 4-3.** Active Directory Information

<table>
<thead>
<tr>
<th>Directory Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server host</td>
<td>The text box for the Active Directory host address.</td>
</tr>
</tbody>
</table>
| Server port           | The text box for the port number for the Active Directory host.  
For a single domain Active Directory Domain Service, the default port for LDAP is 389 while the default port for LDAP over SSL is 636.  
For a multi-domain Active Directory Domain Service (AD DS) forest, the default ports for the global catalog are 3268 without SSL and 3269 with SSL. |
| Use SSL               | You can select the **Use SSL** check box if that’s what you use for your directory connection. |
| Search attribute      | The drop-down menu for the Active Directory attribute that contains the username.  
For a single domain Active Directory Domain Service, the appropriate selection is sAMAccountName.  
For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate selection is userPrincipalName. |
<table>
<thead>
<tr>
<th>Directory Information</th>
<th>Description</th>
</tr>
</thead>
</table>
| Base distinguished name (DN) | The text box for the Base DN, which is the starting point for directory server searches. You can use either Active Directory or Demo User Store (for evaluation only) directory types. See the following examples for best practices when selecting the Base DN and Bind DN:  
  - Base DN: dc=example, dc=com (It is recommended that you use the topmost level for Base DN so you include all users and groups.)  
  - Bind DN: cn=admin user, ou=users, dc=example, dc=com (Ensure that Bind DN is included in the Base DN you select.)  
  You can promote other Active Directory users to the administrator role using Horizon Workspace Administrator Web interface. For a single domain Active Directory Domain Service, this is the text box for the DN of the starting point for directory server searches. For example: DC=mycompany,DC=com. The Connector starts from this DN to create master lists from which you can later filter out individual users and groups. For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave this text box blank. |
| Bind DN | The text box for the Bind distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users. You can use either Active Directory or Demo User Store (for evaluation only) directory types. The Bind DN account becomes the first administrative account for Horizon Workspace that supports Active Directory. The Bind DN account user record in Active Directory must include a username, first name, last name, email address, any required extended attributes, and a distinguishedName attribute defined in Active Directory. See the following examples for best practices when selecting the Base DN and Bind DN:  
  - Base DN: dc=example, dc=com (It is recommended that you use the topmost level for Base DN so you include all users and groups.)  
  - Bind DN: cn=admin user, ou=users, dc=example, dc=com (Ensure that Bind DN is included in the Base DN you select.)  
  You can promote other Active Directory users to the administrator role using Horizon Workspace Administrator Web interface. For a single domain Active Directory Domain Service, the Bind DN entry must be located in the same branch and below the Base DN. For a multi-domain Active Directory Domain Service (AD DS) forest, because you leave the Base DN text box empty, the restrictions that apply for a single domain do not apply for a multi-domain forest. |
| Bind password | The text box for the Active Directory password for the Bind DN account. |

**Map User Attributes**

During the push process, Horizon Workspace maps the attributes you select from your directory to Horizon Workspace.

**IMPORTANT** If you plan to integrate with View, you need to select the **Required** checkbox for UPN. See “Integrating VMware View,” on page 46.

**Select Users**

Use the Select Users page to filter the users you want to sync with Horizon Workspace. You can filter users using three different methods. First, you start with the base DNs that you want to sync with Horizon Workspace. Next, you can filter by including or excluding users. Using an exclude filter is best when you want to exclude a smaller number of users. This method extracts all the users defined by DN first, and then based on the filters you create, excludes the users you do not want to sync with Horizon Workspace. If you want to exclude hundreds of users, it is best to add additional user attributes to your query to include them rather than trying to exclude large numbers individually.
You can sync users from multiple DNs. However, only users under the Base DN that you defined in the Directory step can be authenticated.

If you include additional user attributes to the basic query you create when you enter your base DN, you can restrict users without having to create multiple exclusion filters. For example, by using the include method, you can include 100 users and exclude 900 users without having to determine the correct filter to create to exclude the 900 users. When you add user attributes to your query, processing occurs at the LDAP level rather than in Horizon Workspace. Processing an inclusion query optimizes the memory and resources of Horizon Workspace.

In some case, you might need to use include and exclude filters together.

<table>
<thead>
<tr>
<th>Table 4-4. Type of Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Query</strong></td>
</tr>
</tbody>
</table>
| Base DN with exclude filter | 1. Enter the DN where the users are located. For example, if you want to include all the users in the base DN for Company A’s Active Directory, use the following query: ou=Users,DC=testDC,DC=acme,DC=com  
2. Create filters to exclude users you don’t want to sync to Horizon Workspace, for example: name contains John Smith |
| Base DN with user attributes to include | 1. Enter the DN where the users are located.  
2. Append a semicolon after the user base DN you want to filter.  
3. After the semicolon, add attribute information to narrow your query and include only the users you want to sync with Horizon Workspace. For example, if you want to include only the sales team in Company A, use the following query: ou=Users,DC=testDC,DC=acme,DC=com;(&(objectClass=user)(objectCategory=person)( department=Sales)) |

**NOTE** If you do not want to include additional user attributes in your query, do not use the default filter ((&(objectClass=user)(objectCategory=person))) in the **Enter the DN for Users** field.

**Select Groups**

You add group information from your directory type that you want to import to Horizon Workspace during the synchronization. You can assign a new name to your Directory group in Horizon Workspace.

**NOTE** When you select a group, all members of the group are synced to Horizon Workspace. You can sync users from multiple DNs. However, only users under the Base DN that you defined in the Directory step can be authenticated.

**Configure Scheduling**

You schedule a sync to run as frequently as every hour or as infrequently as once a week. If you select Manually as the frequency, your directory and Horizon Workspace will only sync when you trigger a push.

**Push to Horizon**

You review the number of directory users and groups you want to add, remove, or update based on your changes.

**IMPORTANT** Do not log into Horizon Workspace until after the Push operation is complete. If you add a large number of users, the synchronization process can take time. Verify that the users and groups are under the Base DN for successful authentication.
SSL Setup

You paste an SSL certificate and a private key for external access service. See “Using SSL Certificates in Horizon Workspace,” on page 75.

**IMPORTANT** (Optional) You must include the entire certificate chain in the SSL certificate section. You can upload a trusted certificate later. Horizon Workspace includes a self-signed certificate.

Select Modules

You click **Enable this module** for each module you want to enable. The modules described below are available.

**Table 4-5. Module Information**

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data module</td>
<td>The data module is available in the catalog-services section. After it is enabled, the administrator can entitle users or groups to upload and share files with enterprise and non-enterprise users.</td>
</tr>
<tr>
<td>Webapps and mobile apps</td>
<td>You can add or import SAML-based Webapps or referred mobile apps from a published global catalog (hosted by VMware) from Google Play and iTunes applications stores. Then the administrator can grant users and groups access to these applications. Users can use single sign-on to access the SAML-based Web applications or install referred mobile applications on their mobile devices.</td>
</tr>
<tr>
<td>ThinApp packages</td>
<td>You can download ThinApp packages from a Windows network share. You must log in to the Connector and load the ThinApp packages. The administrator can entitle ThinApp packages to users and groups from the Manager Administrator Web interface, and end users can launch these applications using the Horizon Workspace Client for Windows.</td>
</tr>
<tr>
<td>View pools</td>
<td>While enabling the module, the administrator can sync information about the available View pools and entitlements from the View Connection Server. Once enabled, end users can launch the View desktops they have access to from the Horizon Workspace Web interface. If you want to enable the View module, you must join the Active Directory domain, sync the View Connection Server with it, and enable SAML authentication. See “Integrating VMware View,” on page 46 for more information on View integration.</td>
</tr>
</tbody>
</table>

Go to Horizon Workspace

When the setup wizard finishes, you can click **Go to Horizon Workspace** to open the Horizon Workspace Web interface.

Clicking this button opens the login page for the Horizon Workspace Administrator Web interface. The log in requires the Bind DN username and password that you entered for the Directory step. If you can log into the Horizon Workspace Administrator Web interface, your Horizon Workspace deployment was successful.

Now, you can continue with resource entitlement. See the *Horizon Workspace Administrator Guide* for details.

Configurator Information

After you run the Horizon Workspace Setup wizard, you can open the Configurator to update your configuration or perform advanced configuration tasks. You can use the Connector to perform specialized Connector configurations.

System Information

Find system information about each of the following virtual appliances:

- Connector (connector-va)
The system information provided includes:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>DNS resolved label assigned to uniquely identify each virtual appliance.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Installed version of the application.</td>
</tr>
<tr>
<td>VM Time</td>
<td>Date and time on the virtual machine.</td>
</tr>
<tr>
<td>Relative Drift</td>
<td>Time difference between the virtual appliance time and the configurator-va</td>
</tr>
<tr>
<td></td>
<td>virtual machine time. A large time drift can cause issues with the</td>
</tr>
<tr>
<td></td>
<td>authentication and certification process.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address for the specified virtual appliance.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address for the specified virtual appliance.</td>
</tr>
<tr>
<td>Status</td>
<td>Powered On – virtual appliance is turned on.</td>
</tr>
<tr>
<td></td>
<td>Powered Off – virtual appliance is turned off.</td>
</tr>
<tr>
<td></td>
<td>Maintenance Mode – virtual appliance might be powered on, but it is not</td>
</tr>
<tr>
<td></td>
<td>available to serve any user requests. Only certain virtual appliances can</td>
</tr>
<tr>
<td></td>
<td>use maintenance mode, such as the connector-va virtual machine with the</td>
</tr>
<tr>
<td></td>
<td>role of directory-based load balancing, data-va virtual machine, and</td>
</tr>
<tr>
<td></td>
<td>service-va virtual machine. The configurator-va, gateway-va, and</td>
</tr>
<tr>
<td></td>
<td>connector-va virtual machines with the authentication role cannot use</td>
</tr>
<tr>
<td></td>
<td>maintenance mode.</td>
</tr>
<tr>
<td></td>
<td>Status Unknown – virtual appliance is not responding.</td>
</tr>
</tbody>
</table>

**Database Connection**

You must select an internal or external database. You can choose either the internal database installed by the Horizon Workspace Setup wizard, or you can use your own external database. If you use an external database, you must point to an initialized, populated database. For example, a database configured during a successful run of the Horizon Workspace Setup wizard, a database from a backup, or an existing database from a recovered snapshot.

**Note** You cannot switch from an external to an internal database to create a new install of Horizon Workspace or vice versa.

**Important** In reference to database storage, you can use the internal database for the proof-of-concept phase. Do not use the internal database server in production. For production, install and configure an external database server.

**SSL Certificate**

If you require external access service, you must paste an SSL certificate and a private key. See “Using SSL Certificates in Horizon Workspace,” on page 75.

**Important** This step is optional. You must include the entire certificate chain in the SSL certificate section. You can upload a trusted certificate later. Horizon Workspace includes a self-signed certificate. If you are using an external gateway or a load balancer, you must manually copy the certificate to the end point.
Module Configuration

Click on each module you want to enable. After you enable a module, you cannot disable it. The modules are described as follows:

Data Module
The data module is available in the catalog-services section. After it is enabled, the administrator can entitle users or groups to upload and share files with enterprise and non-enterprise users.

Webapps and Mobile Apps
You can add or import SAML-based Webapps or referred mobile apps from a published global catalog (hosted by VMware) from Google Play and iTunes applications stores. Then the administrator can grant users and groups access to these applications. Users can use single sign-on to access the SAML-based Web applications or install referred mobile applications on their mobile devices.

ThinApp
You can download ThinApp packages from a Windows network share. You must log in to the Connector and load the ThinApp packages. The administrator can entitle ThinApp packages to users and groups from the Manager Administrator Web interface, and end users can launch these applications using the Horizon Workspace Client for Windows.

View Pools
While enabling the module, the administrator can sync information about the available View pools and entitlements from the View connection server. Once enabled, end users can launch the View desktops they have access to from the Horizon Workspace Web interface. If you want to enable the View module, you must join the Active Directory domain, sync the View Connection Server with it, and enable SAML authentication.

License Key
Type the license key provided by VMware.

Password
You are changing the administrator user password on the service-va, configurator-va, and connector-va virtual machines. This process takes time. The system validates that the password you type in the Old Password field matches the administrator user password on the service-va, configurator-va, and connector-va virtual machines. Then the system changes the old password to the password you specify in the New Password field.

Logging
Horizon Workspace provides log files for you to use during testing and troubleshooting. See more information on logging at “Logging Information,” on page 50.

Changing vCenter Administrator Password
If you change your vCenter administrator password, you must use the hznAdminTool to change it on the configurator-va virtual machine as well.

You must update your password on the configurator-va virtual machine. Otherwise, when you log in to the Horizon Workspace Configurator Web interface, you can only see the System Information page.

Procedure
1. Log in to the configurator-va.
2 Run the following command:
```
hznAdminTool editproperty --fileName=/usr/local/horizon/conf/horizon-configurator.properties
--set=secure_vim_password:<yournewpassword>
```

3 Run the `configurator-vc restart` command to restart the configurator-vc virtual machine.

**What to do next**

Log in to the Horizon Workspace Configurator Web interface and verify that the System Information page appears.

### Horizon Workspace URLs

You use different URLs to access the different Horizon Workspace Web interfaces.

Each interface gives you access to different functions. Each Web interface URL listed uses a placeholder, such as `HorizonWorkspaceFQDN`, `ConnectorHostname`, and `ConfiguratorHostname` for the hostname. Replace the placeholder names with the actual values.

**Table 4-6. Horizon Workspace URLs**

<table>
<thead>
<tr>
<th>URL</th>
<th>User Interface</th>
<th>What you can do here</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/admin">https://HorizonWorkspaceFQDN/admin</a></td>
<td>Administrator Web interface (Active Directory user)</td>
<td>Manage the Catalog, users and groups, entitlements, reports, etc. (Login as Active Directory user with administrator role.)</td>
</tr>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/SAAS/login/0">https://HorizonWorkspaceFQDN/SAAS/login/0</a></td>
<td>Administrator Web interface (non-Active Directory user)</td>
<td>Use this URL if you cannot login as the Active Directory user with the administrator role. (Log in as an administrator using the username <code>admin</code> and the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://HorizonWorkspaceFQDN/web">https://HorizonWorkspaceFQDN/web</a></td>
<td>Web Client (end user)</td>
<td>Manage files, launch applications, or launch View pools. (Login as an Active Directory user or virtual user.)</td>
</tr>
<tr>
<td><a href="https://ConnectorHostname/hc/admin/">https://ConnectorHostname/hc/admin/</a></td>
<td>Connector Web interface</td>
<td>Configure additional ThinApp settings, View pool settings, check directory sync status, or alerts. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
<tr>
<td><a href="https://ConfiguratorHostname/cfg">https://ConfiguratorHostname/cfg</a></td>
<td>Configurator Web interface</td>
<td>See system information, check modules, set license key, or set admin password. (Log in as an administrator using the password you set during configuration.)</td>
</tr>
</tbody>
</table>

### Updating to the Latest Horizon Workspace Desktop Client

You can download native clients, such as Windows and Mac, by going to the Horizon Workspace Download page at https://HorizonWorkspaceFQDN/download.

When VMware releases new versions of these clients, administrators can test the clients and then update the download links to the latest clients. Afterward, end users can download the latest clients using the instructions that follow.

**Note** End users must download Android and iOS clients from the app stores, GooglePlay and iTunes respectively.
Installing Horizon Workspace Client for Windows

Download and install the current version of the Horizon Workspace Client for Windows. For the latest file, go to the VMware Horizon Workspace download page. Install this file on each data-va virtual machine.

Procedure

1. Copy the Horizon Workspace file to each data-va virtual machine’s download directory.
   
   scp VMware-Horizon-Workspace-<#.0.0-#####>.exe
   root@yourDataServer:/opt/zimbra/jetty/webapps/zimbra/downloads

2. Ensure the file has the correct permissions.
   
   # chmod a+r VMware-Horizon-Workspace-<#.0.0-#####>.exe

3. Change to the Zimbra user.
   
   su - zimbra

4. Edit the ZoMsg properties file at /opt/zimbra/jetty/webapps/zimbra/WEB-INF/classes/messages.

5. Update the winSyncClientUrl parameter value to the downloaded file name and version number.
   
   winSyncClientUrl = /data/downloads/VMware-Horizon-Workspace-<#.0.0-#####>.exe
   
   (Optional) Update the windowsClientVersion parameter value with the version number, -<#.0.0-#####>.

6. Restart the server.
   
   zmmailboxdctl restart

Installing Horizon Workspace Client for Mac

Download and install the current version of the Horizon Workspace Client for Mac. Install this file on each data-va virtual machine.

Procedure

1. Copy the Horizon Workspace file to each data-va virtual machine’s download directory.

   scp VMware-Horizon-Workspace-<#.0.0-#####>.dmg
   root@yourDataServer:/opt/zimbra/jetty/webapps/zimbra/downloads

2. Ensure the file has the correct permissions.

   # chmod a+r VMware-Horizon-Workspace-<#.0.0-#####>.dmg

3. Change to the Zimbra user.

   su - zimbra

4. Edit the ZoMsg properties file at /opt/zimbra/jetty/webapps/zimbra/WEB-INF/classes/messages.

5. Update the macSyncClientUrl parameter value to the downloaded file name and version number.

   macSyncClientUrl = /data/downloads/VMware-Horizon-Workspace-<#.0.0-#####>.dmg
   
   (Optional) Update the macClientVersion parameter value with the version number, -<#.0.0-#####>.

6. Restart the server.

   zmmailboxdctl restart
After you complete the Horizon Workspace setup wizard, you might need to complete other configuration steps that you perform in the Configurator, such as View and ThinApp integration, or cloning virtual machines.

This chapter includes the following topics:

- “Adding Storage to the Data Virtual Appliance,” on page 35
- “Configuring Data Preview,” on page 37
- “Customizing the Demo User Store,” on page 41
- “Integrating VMware ThinApp,” on page 44
- “Integrating VMware View,” on page 46
- “Setting Proxy Server Settings for Manager,” on page 50
- “Logging Information,” on page 50

## Adding Storage to the Data Virtual Appliance

When Horizon Workspace data-va virtual machine is configured, several default virtual machine disks (VMDK) are configured. The combined size of all configured VMDK storage is 175GB. One of these is configured to store Data blobs and by default is only 10GB.

You must add additional disk storage to manage your Data storage resources. You can either add additional VMDKs for Data blob storage or you can use shared Network-attached storage (NAS) configured with the Network File System (NFS) protocol. The storage option you choose depends on your storage requirements. For example, small deployments that require less than six terabytes for storage can be configured using VMDKs. Whereas for large deployments, VMware recommends that you use NFS protocol to manage your Data blob storage.

### Adding Additional VMDKs for Storage

Adding additional VMDKs for storage is done via the normal vSphere mechanism.

**Prerequisites**

- Verify that the data-va virtual machine is running.
- Recommended storage requirement is 2.5 times the user’s quota per account, which provides sufficient space for multiple file revisions.
- Use vSphere to add VMDKs for storage.
Procedure

1. Log in to the vSphere Client and select the Data server.
2. Click OK.
3. Click the Console tab and click Enter.
4. Type root to log in.
5. Enter the root password you created for all virtual appliances during Horizon Workspace installation.
6. Type /opt/vmware-hdva-installer/bin/zca-expand-lv to run the script.
   The newly added disk is detected and added to the store logical volume by default.
7. Exit the server.

**Note** Replacing or retiring underlying storage is not covered in this document. If you want to retire or upgrade disks underlying the data volume, the Linux Documentation Project provides a detailed description of how to remove physical volumes from a LVM by first migrating their file systems (extent). See sample steps at [http://tldp.org/HOWTO/LVM-HOWTO/removeadisk.html](http://tldp.org/HOWTO/LVM-HOWTO/removeadisk.html).

What to do next

You can use network storage to store your files. See “Adding Network Attached Storage for Storage,” on page 36.

Adding Network Attached Storage for Storage

When you add an NFS mount, this becomes the working data volume. The VMDK disk that is configured during install becomes a secondary data volume and no new data files are added to the VMDK disk.

**Prerequisites**

- Create a directory on the NFS server that can be accessed from the data-va virtual machine. You identify the hostname or IP address and the directory when you mount the NFS volume.

**Procedure**

1. Log in to the vSphere Client and select the Data server.
2. Click OK.
3. Click the Console tab and press Enter.
4. Type root to log in.
5. Enter the administrator password you created for all virtual appliances during Horizon Workspace installation.
6. Change the directory.
   ```
   cd /opt/vmware-hdva-installer/bin
   ```
7. Mount the NFS volume.
   ```
   ./mount-nfs-store.pl --nfs <nfs_serverhostname>:/<directory_to_use>
   ```
   A new mount point is created and the new volume is now the current primary volume for the data-va virtual machine.
8 Verify the newly mounted NFS volume ID.
   a  Change to the Zimbra user.
      su - zimbra
   b  Type zmvolume -l to see the volume ID.

What to do next
You can also manage your data storage volumes. See “Managing Data Storage Volumes,” on page 37.

Managing Data Storage Volumes
When you add files to the Horizon Workspace Data My Files folder, the files are saved to the current Data volume. You can create additional volumes, but only one volume is configured as the current volume where new files are stored. When the current volume is full, you can configure a new current volume. The current data volume receives all new files. New files are never stored in a previous volume.

A current volume cannot be deleted and volumes that have referenced that volume cannot be deleted.

Use the zmvolume CLI to manage storage volumes on your data-va virtual machine. See the CLI Command for Horizon Workspace Data Guide for usage.

Configuring Data Preview
To preview files in the Data Web client, you must install either LibreOffice or Microsoft Windows Preview.

CAUTION  When the contents of a file contains Simplified Chinese, Traditional Chinese, Korean, or Japanese characters, the file might not preview correctly. You must install the CJK fonts on the server to fix this issue.

IMPORTANT  Password protected Microsoft Office documents cannot be previewed.

Installing LibreOffice Preview
You can install LibreOffice Preview to view Horizon Workspace documents.

Procedure
1  Log in to the vSphere Client and select the Data server.
2  Click OK.
3  Click the Console tab and click Enter.
4  Type root to log in.
5  Type the administrator password you created for all the virtual appliances during the Horizon Workspace installation.
6  If you use a proxy to reach the Internet, type export http_proxy="http://[proxy.example.com:3128]".
7  Type /opt/zimbra/libexec/libreoffice-installer.sh.

   NOTE  You can run tail -f /tmp/libreoffice.download.txt to monitor the progress of the installation.

8  Change to the Zimbra user after LibreOffice installation is complete.
    su - zimbra
9  Type zmmailboxdctl restart to apply the change to the data server.
Installing Microsoft Windows Preview

You can configure the Horizon Workspace Preview server to preview Microsoft Office documents when using the Horizon Workspace Web interface.

Prerequisites

If your company is licensed to use Microsoft Windows products, you can install Microsoft Windows Preview as well.

- Microsoft Windows 7 Enterprise or Windows Server 2008 R2 Standard
- Microsoft Office 2010 Professional, 64 bit
- An administrative account with permission to create local accounts.
- Turn off UAC.

Procedure

1. Download the .msi file from the Horizon Workspace downloads directory at /opt/zimbra/jetty/webapps/zimbra/downloads/VMware-Horizon-Data-Preview-Server-<buildnumber>.msi.
2. Open the .msi file and click Next.
3. Accept the end user license agreement and click Next.
4. Click Next twice.
   The Controller/Worker Account Password is VMwarePv123!. This password meets the default complexity requirements for Windows Server 2008. If you use stricter password requirements, you can change this.
   If you change the Number of Worker Accounts from 5, follow this standard: 2 x (number of CPUs) x (number of cores per CPU).
   The Configure Installation dialog box appears with the text fields populated. You do not need to change these fields.
5. If you are prompted to reboot, click Yes.

The controller account is logged in after the reboot. This account must be logged in for the server to run. The preview server starts each time the controller account is logged in.

What to do next

To complete the setup, see “Pointing the Data Server to the Windows Server,” on page 38.

Pointing the Data Server to the Windows Server

After you install the .msi file, configure the Preview feature on the Data server.

Procedure

1. Log in to the vSphere Client and select the Data server.
2. Click the Console tab and click Enter.
3. Type root to log in.
4. Type the administrator password that you created for all the virtual appliances during the Horizon Workspace installation.
5 Change to the Zimbra user.
   `su - zimbra`

6 Type the Windows Server URL with this command.
   `zmlocalconfig -e ms_converter_url="http://xx.xx.xx.xx"`

7 Type `zmmailboxdctl restart` to restart mailboxd.

8 Type `zmprov mc {cosname} hzndataConverterHints UseMsPDFConverter` to modify each class of service, including the `externaldefault` class.

   **Note** Run the `zmprov` command for each COS.
   `zmprov mc {cosname} hzndataConverterHints UseMsPDFConverter`

### What to do next

You can change the configuration settings for the Preview Server, such as change conversion timeout, delete account behavior, and so on.

## Modifying the Preview Server Localconfig File

You can change the configuration settings for the Preview Server to suit your environment.

<table>
<thead>
<tr>
<th>Change Conversion timeout</th>
<th>Determines how long the server waits for Microsoft Office to export a file to PDF.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete accounts on uninstall</td>
<td>Specifies whether the controller and worker accounts are deleted during uninstall.</td>
</tr>
<tr>
<td>Customize the Temp directory</td>
<td>This directory is created under <code>C:\ProgramData\Vmware\Octopus Preview Server</code> by default. It can be moved, but the Users group must have full access to custom directories.</td>
</tr>
<tr>
<td>Customize the Log directory</td>
<td>This log is created under <code>C:\ProgramData\Vmware\Octopus Preview Server</code> by default. It can be moved, but the Users group must have full access to any custom directories.</td>
</tr>
</tbody>
</table>

**Note** Changes you make to the `localconfig` file are overwritten when you upgrade. If you make changes to this file, make a copy of your changes before upgrading.

## Configuring a Multi-domain Active Directory Domain Service Forest

If your deployment uses a Multi-domain Active Directory Domain Service (AD DS) forest, you must base the Horizon Workspace general configuration and individual Connector configuration on the Active Directory global catalog instead of LDAP.

### Active Directory Global Catalog

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a Multi-domain Active Directory DS forest. The global catalog is stored on domain controllers that have been designated as global catalog servers. The global catalog is distributed through multi-master replication.
Searches that are directed to the global catalog are faster because they do not involve referrals to different
domain controllers. A global catalog server is a domain controller that, in addition to its full, writable domain
directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the
forest. The additional domain directory partitions are partial because only a limited set of attributes is included
for each object. By including only the attributes that are most used for searching, every object in every domain
in even the largest forest can be represented in the database of a single global catalog server.

The global catalog is built and updated automatically by the Active Directory DS replication system. The
attributes that are replicated to the global catalog are identified in the schema as the partial attribute set (PAS)
and are defined by default by Microsoft. However, to optimize or extend searching, you can edit the schema
by adding or removing attributes that are stored in the global catalog.

Access to a global catalog server is required for successful user authentication. If a global catalog server is not
available, the user login fails. The global catalog stores the membership (the member attribute) of only universal
groups. You can change the scope of a group from local domain or global to universal.

By using different ports for standard LDAP queries (ports 389, 636) than for global catalog queries (ports
3268,3269), Active Directory DS effectively separates forest-wide queries that require a global catalog server
from local, domain-wide queries that can be serviced by the domain controller in the user’s domain.

Users must log in to Application Manager with a user principal name (UPN). When a user account is created,
the UPN suffix is generated by default as userName@DnsDomainName, but you as an administrator can
change this default setting.

For example, in a forest that has four domains, the UPN suffix might be configured to map to the external DNS
name for the organization. The userPrincipalName attribute of the user account in Active Directory identifies
the UPN and is replicated to the global catalog.

Horizon Workspace General Configuration and Individual Connector Configuration

The installation and configuration of the Horizon Workspace (and Connector) is similar for an Active Directory
DS forest scenario as it is for a single domain scenario. However, you must configure a few of the Directory
pages differently when your deployment uses an Active Directory DS forest.

You can reference the links that follow for instructions to specific Connector Web interface pages. Instructions
specific to an Active Directory DS forest scenario are integrated into each of these topics. The Connector Web
Interface Configurations Specific to an Active Directory DS Forest table provides a summary of all the
instructions specific to an Active Directory DS forest scenario. See “Running the Horizon Workspace Setup

<table>
<thead>
<tr>
<th>Connector Web Interface Page</th>
<th>Configurations Specific to an Active Directory DS Forest</th>
</tr>
</thead>
</table>
| Directory                   | ■ Server Port: You enter the global catalog port number. The default ports for the global catalog are 3268 without SSL and 3269 with SSL.  
                                 ■ Search Attribute: You select userPrincipalName from the drop-down menu.  
                                 ■ Base DN: You leave the Base DN text box empty. |
| User Attributes             | IMPORTANT On the Map User Attributes page, you must map the Horizon Workspace userName attribute to the Directory userPrincipalName attribute. This mapping must occur automatically since the userPrincipalName value is carried forward from the Directory page. Do not change this value from userPrincipalName.  
                                 On the Map User Attributes page, you must only add attributes that are stored in the global catalog. If you want to synchronize a special user attribute, such as employeeID, with Horizon Workspace, you must first add the attribute to the global catalog. |
Table 5-1. Connector Web Interface Configurations Specific to an Active Directory DS Forest (Continued)

<table>
<thead>
<tr>
<th>Connector Web Interface Page</th>
<th>Configurations Specific to an Active Directory DS Forest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Users (The Select Users page is available in the Horizon Workspace Setup wizard and from the Connector Directory Sync page).</td>
<td>On the Select Users page, you can add users from multiple domains of the same Active Directory DS forest by clicking <em>Add another</em> in the DN section and providing another DN.</td>
</tr>
<tr>
<td>Select Groups (The Select Groups page is available in the Horizon Workspace Setup wizard and from the Connector Directory Sync page).</td>
<td>On the Selected Groups page, multiple group DNs can exist. They are automatically prepopulated with values from the Select Users page. You can only use universal groups. If you want to synchronize special local or global group membership information with Horizon Workspace, you must change the scope of the group to universal.</td>
</tr>
</tbody>
</table>

**Customizing the Demo User Store**

The embedded OpenLDAP service is typically used for demonstration or test configurations. When using the embedded OpenLDAP service, you might want to perform common LDAP operations, such as adding new users, deleting existing users, and changing user passwords.

This information is intended for experienced system administrators who are familiar with standard LDAP operations and commands.

The embedded OpenLDAP server runs on TCP port 389. The OpenLDAP server is only accessible locally from the Linux console on connector-va virtual machine. You can use standard LDAP commands to perform operations in the embedded OpenLDAP server. The required binaries (ldapadd, ldapsearch, ldapdelete, and ldapmodify) are installed in the virtual appliance.

You must use the following parameters when you configure OpenLDAP in the Configurator and Connector Web interfaces.

**Table 5-2. OpenLDAP Configuration Information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>&lt;ConnectorFullyQualifiedDomainName&gt; or &quot;localhost&quot;</td>
</tr>
<tr>
<td>Search attribute</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Server port</td>
<td>389</td>
</tr>
<tr>
<td>Base DN</td>
<td>ou=users, dc=test, dc=example, dc=com</td>
</tr>
<tr>
<td>Bind DN</td>
<td>cn=test user1, ou=users, dc=test, dc=example, dc=com</td>
</tr>
<tr>
<td>Bind password</td>
<td>password</td>
</tr>
</tbody>
</table>

**NOTE** You must use sAMAccountName as your Search Attribute in the Demo User Store. Horizon Workspace does not support userPrincipalName when using Demo User Store.

The Demo User Store includes 10 sample users and 1 group for demonstration purposes. Horizon Workspace stores the sample information on the connector-va virtual machine.

The Sample Data Information table shows the specific sample data that is included with the Demo User Store. During deployment, the Horizon Workspace Setup wizard loads this data into the sample database.
If you want to add users or groups, create new files and name them `ldapusers.ldif` and `ldapgroups.ldif`. Use the original files, `users.ldif` and `groups.ldif`, as templates. See “Adding a User to the Demo User Store,” on page 42 and “Adding Groups and Assigning Users to Groups in the Demo User Store,” on page 43.

**Table 5-3. Sample Data Information**

<table>
<thead>
<tr>
<th>Sample Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample files</td>
<td><code>users.ldif</code></td>
</tr>
<tr>
<td></td>
<td><code>groups.ldif</code></td>
</tr>
<tr>
<td>Directory path</td>
<td><code>/etc/openldap</code></td>
</tr>
<tr>
<td>Sample usernames</td>
<td>testuser1 – testuser10</td>
</tr>
<tr>
<td>Password for all users</td>
<td><code>password</code></td>
</tr>
<tr>
<td>Sample group</td>
<td><code>testgroup1</code></td>
</tr>
</tbody>
</table>

(The sample group, `testgroup1`, contains the 10 sample users.)

**Adding a User to the Demo User Store**

When you set up your Demo User Store, you determine the number of users you want to add based on your production environment. You need to add enough users so that testing produces results that are relevant to your production environment.

You add a user to the Demo User Store by modifying the `ldapusers.ldif` file and running the `ldapadd` command on the Connector virtual machine.

**Procedure**

1. Replace the `<value>` tag in the `ldapusers.ldif` file with your information. See Sample `ldapusers.ldif` File table.
2. Copy the ldif file to the Connector virtual machine.
3. Run the `ldapadd` command to add a new user to the Demo User Store.

    ```bash
    /usr/bin/ldapadd -D "cn=Manager,dc=test,dc=example,dc=com" -w Horizon! -x -f <ldif file path>
    ```

    You can add multiple users by using different values in a single ldif file.
4 Restart the LDAP service.

/sbin/service ldap restart

**Note** To generate an encrypted password for each new user, see “Generating an SSHA Encrypted Password,” on page 43.

- **Table 5-4. Sample ldapusers.ldif File**

  **Sample ldapusers.ldif**
  
  ```
  dn: cn=<value>,ou=users,dc=test,dc=example,dc=com
  objectClass: user
  objectCategory: person
  cn: <value>
  sn: <value>
  sAMAccountName: <value>
  mail: <value>
  givenName: <value>
  distinguishedName: cn=<value>,ou=users,dc=test,dc=example,dc=com
  objectGUID: <value> (e.g. cd0ff02b-f9d6-4fac-a5bc-6380d1867999) - Must be unique
  userPassword: <value>(e.g. {SSHA}WbipwJh13Jdy2ltppdkFMzzNV5fksZ)
  ```

**What to do next**

Now, you want to generate an encrypted password for use by your Demo User Store users.

**Generating an SSHA Encrypted Password**

The salted secure hash algorithm (SSHA) is an improved version of the SHA algorithm that randomizes the hash and decreases the likelihood that the hash can be unencrypted.

You must generate an SSHA encrypted password. You can use the same password for all demo user accounts. If you need a different password for each user, you must follow these instructions and encrypt each password one at a time.

**Procedure**

1. Open the Connector virtual machine.
2. Run the `slappasswd` command
3. Type and verify a new password.
   - The SSHA encrypted value appears.
4. Add this value to the `ldif` file to set the user password.

**What to do next**

Add groups and assign users to the Demo User Store.

**Adding Groups and Assigning Users to Groups in the Demo User Store**

When you set up your Demo User Store, determine the number of groups and users you want to add based on the size of your production environment. You want to add enough groups and users to create an environment that closely resembles your production environment.

You add a group to the Demo User Store by modifying the `ldapgroups.ldif` file and running the `ldapadd` command on the Connector virtual machine.
Procedure

1. Replace the `<value>` and `<User DN>` tags in the `ldapgroups.ldif` file. The user DN must be the distinguished name of an existing user in LDAP. Replacing the `<value>` tag creates a group, and replacing the `<User DN>` tag assigns a user to the new group you are creating.

2. Copy the ldif file to the Connector virtual machine.

3. Run the `ldapadd` command to add a group to the Demo User Store.

   ```bash
   /usr/bin/ldapadd -D "cn=Manager,dc=test,dc=example,dc=com" -w H0rizon! -x -f <ldif file path>
   ``

   You can add multiple groups by using different values in a single ldif file.

4. Restart the LDAP service.

   ```bash
   /sbin/service ldap restart
   ```

Table 5-5. Example of the `ldapgroups.ldif` File

<table>
<thead>
<tr>
<th>Sample Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dn: cn=&lt;value&gt;,ou=users,dc=test,dc=example,dc=com</code></td>
</tr>
<tr>
<td><code>objectClass: group</code></td>
</tr>
<tr>
<td><code>objectCategory: group</code></td>
</tr>
<tr>
<td><code>sAMAccountName: &lt;value&gt;</code></td>
</tr>
<tr>
<td><code>mail: &lt;value&gt;</code></td>
</tr>
<tr>
<td><code>distinguishedName: cn=&lt;value&gt;,ou=users,dc=test,dc=example,dc=com</code></td>
</tr>
<tr>
<td><code>objectGUID: &lt;value&gt; (e.g. cd0ff02b-f9d6-4fac-a5bc-6380d1867899) - Must be unique</code></td>
</tr>
<tr>
<td><code>member: &lt;User DN1&gt; (e.g. cn=user1,ou=users,dc=test,dc=example,dc=com)</code></td>
</tr>
<tr>
<td><code>member: &lt;User DN2&gt;</code></td>
</tr>
<tr>
<td><code>member: &lt;User DN3&gt;</code></td>
</tr>
<tr>
<td><code>member: &lt;User DN4&gt;</code></td>
</tr>
</tbody>
</table>

Integrating VMware ThinApp

To use VMware® ThinApp® with Horizon Workspace, you must have a ThinApp repository that contains your ThinApp packages. This repository must be a Windows Common Internet File System (CIFS) share.

**IMPORTANT** Other shares, such as NetApp and DFS, are not supported.

You must join the connector to the Active Directory domain so the connector can join the Windows network share.

**NOTE** Windows authentication is not required.

See “Configuring Kerberos for Horizon Workspace,” on page 71 for more information on how to join the domain.

Creating a Windows Network Share for ThinApp Packages

If you want to enable the VMware ThinApp management capabilities of Horizon Workspace and allow users to access ThinApp packages from the user application catalog, you must create a Windows network share and store your ThinApp packages in that Windows network share folder.

The Connector synchronizes with the Windows network share regularly to communicate ThinApp package metadata to Horizon Workspace.

**Prerequisites**

- Verify that you are using ThinApp 4.7.2 or later.
- Verify that you are using a Windows network share.
- Use Horizon Workspace to capture Windows applications that can be managed with Horizon Workspace.

**Procedure**

1. Create a Windows network share and verify that it meets the following conditions:
   - The Windows network share folder is accessible using a Uniform Naming Convention (UNC) path from each system running Horizon Workspace. For example, a Windows network share named `appshare` on a host named `server` is accessible using the UNC path `\server\appshare`.
   - The fully qualified hostname of the Windows network share folder is resolvable from the Connector.
   - The host of the Windows network share folder is joined to the same Active Directory domain as Horizon Workspace.
   - The Horizon Workspace Active Directory computer account and users have read access to the Windows network share folder.
   - The Active Directory groups or authenticated users and domain computers have read-only access to the Windows network share folder. Access privileges can be more specific to allow only Horizon Workspace computer account and Horizon Workspace users.

2. In the Windows network share, create a Windows network share subfolder for each ThinApp package.

   **Note**  Do not use non-ASCII characters when you create your Windows network share subfolder names.

   Verify that the subfolders for each ThinApp package is an application-named subfolder of the Windows network share. For example, if the application is called `abceditor`, the folder for the ThinApp package is available at `\server\appshare\abceditor`.

   After you copy the ThinApp `.exe` and `.dat` files to the application-named subfolder as described in the ThinApp Horizon Workspace Integration Guide, the folder will include files such as these:
   - `\server\appshare\abceditor\abceditor.exe`
   - `\server\appshare\abceditor\abceditor.dat`

**What to do next**

Populate the application-named subfolders with the appropriate ThinApp packages. See the ThinApp Horizon Integration Guide.

**Configuring ThinApp Packages for Horizon Workspace**

You can provide Horizon Workspace users with access to Windows applications captured as ThinApp packages. To use ThinApp packages with Horizon Workspace, you must join the Active Directory domain and sync ThinApp packages from the Windows network share.

First, the administrator must enable the ThinApp module from the Configurator Web interface. Otherwise, ThinApp packages will not be available in the Admin Web interface.

Providing Horizon Workspace users access to ThinApp packages requires other configurations.
### Table 5-6. ThinApp Configuration Descriptions

<table>
<thead>
<tr>
<th>Item to Configure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Windows Apps</td>
<td>The check box to enable Horizon Workspace users access to ThinApp packages.</td>
</tr>
</tbody>
</table>
| Path | The text box for the path to the Windows network share. For example: `\DirectoryHost\ThinAppFileShare`

**CAUTION** For `DirectoryHost`, provide the hostname, not the IP address.

| Scheduling | The drop-down list of options for how often the Connector synchronizes the information about ThinApp packages in the Windows network share with Horizon Workspace. |

### Changing the ThinApp Share Folder

After configuring ThinApp packages and Horizon Workspace, you might need to change the ThinApp share folder.

You change the ThinApp share folder for ThinApp packages by stopping, deleting, and restarting the repo service database.

You must change the ThinApp share folder's name for ThinApp packages in the Connector Web interface. Before you change the ThinApp share folder's name, however, you must clear the repodb on the connector-va virtual machine so it can read from the new ThinApp share folder. To clear the repodb, you must run the following commands on the connector-va virtual machine.

### Table 5-7. Repo Service Commands

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop repo service</td>
<td><code>/opt/likewise/bin/lwsms stop thinapprepo</code></td>
</tr>
<tr>
<td>Delete repo service database</td>
<td><code>rm /var/lib/vmware/tam/repo/repodb</code></td>
</tr>
<tr>
<td>Start the repo service</td>
<td><code>/opt/likewise/bin/lwsms start thinapprepo</code></td>
</tr>
</tbody>
</table>

### Integrating VMware View

To use View with Horizon Workspace, you must join the Active Directory domain and sync with the View Connection Server.

**Prerequisites**

- Use VMware View 5.2 or later.
- Deploy and configure View to use the default port, 443. Horizon Workspace does not support other ports for View integration.
- Deploy and configure View pools and desktops with entitlements set for Active Directory users and groups.
- Ensure that you create the View pools as a user with administrator permissions on the root folder in View. If you give the user administrator permissions on a folder other than the root folder, Horizon Workspace will not recognize the SAML Authenticator you configure in View, and you cannot configure the pool in Horizon Workspace.
- Deploy and configure Horizon Workspace.
- Enable the UPN attribute on Horizon Workspace.
- Verify that you have a DNS entry and an IP address that uses reverse lookup for each View Connection Server in your View setup. Horizon Workspace requires reverse lookup for View Connection Servers, the View Security server, and the load balancer. If reverse lookup is not properly configured, the Horizon Workspace integration with View fails.

- Sync Active Directory users and groups with View pool entitlements to Horizon Workspace. You can sync with the Horizon Workspace Setup wizard or from the Directory tab.

### Joining Active Directory Domain

To use View with Horizon Workspace, you must join the Active Directory domain.

During the setup process, you will be prompted to enter information for Horizon Workspace to join the Active Directory domain.

#### Prerequisites

- Verify that UPN is enabled.
- Verify that users and groups with View pool entitlements assigned are synced using Directory sync.

#### Procedure

1. In the Select Modules pane of the Horizon Workspace Setup wizard, click Enable this Module for View.
2. Type the domain information for Horizon Workspace and click Join Domain.

<table>
<thead>
<tr>
<th>Table 5-8. Active Directory Domain Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Join Domain</strong></td>
</tr>
</tbody>
</table>
| AD FQDN | Type the fully qualified domain name of the Active Directory to join.  
**IMPORTANT** The Active Directory FQDN must be in the same domain as the View Connection Server. Otherwise, your deployment will fail.  
**NOTE** Do not use non-ASCII characters when you enter your hostname or domain name. |
| AD User | Type the username of the user in Active Directory that has the right to join the computer to the domain.  
**NOTE** Do not use non-ASCII characters when you create your username. |
| AD Password | Type the password associated with the username. This password is not stored by Horizon Workspace.  
**IMPORTANT** Each time you import the Connector’s configuration you must rejoin the domain. |

3. Type the domain information for View and click Sync to propagate your View information to Horizon Workspace.

<table>
<thead>
<tr>
<th>Table 5-9. View Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Initial Connection Server</td>
</tr>
<tr>
<td>FQDN for Client Access</td>
</tr>
</tbody>
</table>
Table 5-9. View Information (Continued)

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Choose an account that has the Administrators or Administrators (Read only) role in View Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password associated with the Active Directory username.</td>
</tr>
</tbody>
</table>

**Note**: If you want View integration to work in a multi-domain environment, you must follow these steps.

a. Verify that Horizon Workspace and the View servers are joined to the same domain.

b. Verify that the Directory Server Host and the View servers are joined to the same domain. The Directory Server Host (defined on the Horizon Workspace Directory configuration page) must be an Active Directory host. Do not specify parent or sibling domain controller information.

c. On the Horizon Workspace Directory configuration page, you must provide global catalog information to allow users in sub-domains and sibling domains to access Horizon Workspace and View desktops.

**What to do next**

Sync View with Horizon Workspace to propagate changes you make in View.

### Syncing View Pools

Each time you change information in View, such as add an entitlement, add a user, and so on, you must force a sync to propagate the changes to Horizon Workspace.

After you enable View in the Configurator Web interface, you can also sync the View pools.

**Procedure**

1. Go to https://<ConnectorHostname>/hc/admin/ to open the Connector Web interface.
2. Enter admin password.
3. Click View Pools and click Sync Now.
4. Verify that you can sync View Pools and their entitlements from View Connection Server to Horizon Workspace.
   
   a. Log in to Horizon Workspace Administrator Web interface.
      
      https://HorizonWorkspaceFQDN/SAAS/login
   
   b. Click the Catalog tab.
   
   c. Select a View pool and check the Details and Entitlements tabs.

If you make changes in View, you must sync with Horizon Workspace to propagate your changes.

**What to do next**

If you want to launch a View desktop from Horizon Workspace and use SSO, you must configure SAML authentication in the View server.

### Configuring SAML Authentication

Ensure that you select the **Enable SSO** function on Horizon Workspace Connector Admin Web interface.

However, if you configure Horizon Workspace using the Horizon Workspace Setup wizard, by default, the **Enable SSO** function is selected.
Procedure
1. Log in to the View Administrator as a user with the Administrator role assigned.
2. Configure SAML authentication for each replicated server in your View infrastructure.

**CAUTION** View and Horizon Workspace must be in time sync. If View and Horizon Workspace are not in time sync, when you try to launch View desktop, an invalid SAML message occurs.

What to do next
You must establish and maintain SSL Trust between the Connector and the View Connection Server.

**Establishing or Updating SSL Trust between the Connector and the View Connection Server**
Initially, you must accept an SSL certificate on the View Connection Server to establish trust between the Connector and the View Connection Server. If you change an SSL certificate on the View Connection Server after the integration, you must return to the Connector and reestablish that trust.

**Prerequisites**
- Verify that View has an SSL certificate installed. By default, View has a self-signed certificate.
- In View, change the certificate of the View Connection Server to a root-signed certificate. See Configure a View Connection Server Instance or Security Server to Use a New Certificate in the VMware View documentation.

**Procedure**
1. Log in to the Connector Admin Web interface.
2. Open the View Pools page.
3. Click the **Update SSL Cert** link next to the Replicated Server Group.
4. Click **Accept** on the Certificate Information page.

If the Horizon Workspace certificate changes after the initial configuration, you must accept the SAML Authenticator from View again. If the View certificate changes, you must accept the SSL certificate in Horizon Workspace.

**Launching a View Pool**
Users can launch a View pool from Horizon Workspace.
You can switch the display protocol between Open with View Client (PCoIP or RDP) or Open with Browser (Blast) by right-clicking the **Pool** icon.

**Prerequisites**
- If View Administrator uses PCoIP or RDP as the display protocol, install View Client 1.6 or later. You must install View Client on the machine that launches Horizon Workspace.

**Procedure**
1. Log in to your Horizon Workspace instance.
2. Click the **Computers** tab.
3. Select your View pool.
4. Right-click the selected View pool and choose a protocol to launch the View desktop.
What to do next

If necessary, you can modify the View integration configuration.

Modifying the View Integration Configuration

You can modify the View integration configuration in the Connector.

The following View integration configuration settings can be changed on the Connector.

- Disable the association between Horizon Workspace and the View environment.
- Adjust the sync schedule and monitor your sync status. You can schedule automatic syncing for times that suit your environment, such as during off-peak hours.
- Re-accept an SSL certificate.

You use the View Connection Server to entitle Horizon Workspace users to View pools.

Procedure

1. Log in to the Connector as the admin user.
2. Click View Pools.
3. Update the View integration configuration settings and click Save.

(Optional) Setting Proxy Server Settings for Manager

Horizon Workspace Manager virtual machine accesses the global catalog and other Web services on the Internet. If your network configuration provides Internet access through HTTP proxy, you might need to adjust your proxy settings on the Manager (service-va) virtual machine.

Procedure

1. Log in as root to the Manager (service-va) virtual machine. See “Running the Configurator’s Virtual Appliance Interface,” on page 24 for more information about the global root password.
2. Append the line from the following table to export JAVA_OPTS in setenv.sh. The file is located in the directory listed in the table.

<table>
<thead>
<tr>
<th>Directory</th>
<th>/opt/vmware/horizon/horizoninstance/bin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Append line to JAVA_OPTS</td>
<td>-Dhttp.proxyHost=&lt;YOUR_PROXY_SERVER&gt; -Dhttp.proxyPort=&lt;PROXY_PORT&gt; -Dhttp.nonProxyHosts=&lt;LOCAL_PROXY_EXCEPTIONS&gt; -Dhttp.proxyHost=&lt;YOUR_PROXY_SERVER&gt; -Dhttp.proxyPort=&lt;PROXY_PORT&gt; -Dhttp.nonProxyHosts=&lt;LOCAL_PROXY_EXCEPTIONS&gt; -Dhttps.proxyHost=&lt;YOUR_PROXY_SERVER&gt; -Dhttps.proxyPort=&lt;PROXY_PORT&gt; -Dhttps.nonProxyHosts=&lt;LOCAL_PROXY_EXCEPTIONS&gt;</td>
</tr>
</tbody>
</table>

Example:


NOTE: When you modify the line in setenv.sh, replace proxy.mycompany.com with your proxy. Your company might also use a different port number. The default port number is 3128.

3. Run the service horizon-frontend restart command to restart the tcserver.

Logging Information

During testing or troubleshooting, you will need feedback about the activity and performance of the virtual appliances as well as information about any problems that occur. Horizon Workspace includes these log files.
### Table 5-10. Log File Information

<table>
<thead>
<tr>
<th>Component</th>
<th>Log File Name</th>
<th>Location of Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>horizon.log</td>
<td>/opt/vmware/horizon/horizon_instance/logs/horizon.log</td>
<td>Information about activity on the Horizon Workspace manager appliance, such as entitlements, users, groups, and so on.</td>
</tr>
<tr>
<td>Configurator</td>
<td>configurator.log</td>
<td>/opt/vmware/var/log/configurator.log</td>
<td>Configuration details from the vApp deployment and installation.</td>
</tr>
<tr>
<td>Configurator</td>
<td>configurator.log</td>
<td>/opt/vmware/horizon/configuratorinstance/logs/configurator.log</td>
<td>Requests that the Configurator receives from the REST client and the Web interface.</td>
</tr>
<tr>
<td>Configurator</td>
<td>catalina.log</td>
<td>/opt/vmware/horizon/configuratorinstance/logs/catalina.out</td>
<td>Apache Tomcat records messages that are not recorded by the configurator.log files.</td>
</tr>
<tr>
<td>Connector</td>
<td>connector.log</td>
<td>/opt/vmware/c2/c2instance/logs/connector.log</td>
<td>A record of each request received from the Web client. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.</td>
</tr>
<tr>
<td>Data</td>
<td>mailbox.log</td>
<td>/opt/zimbra/log/mailbox.log</td>
<td>A record of output messages related to requests received by the mail server.</td>
</tr>
<tr>
<td>Data</td>
<td>audit.log</td>
<td>/opt/zimbra/log/audit.log</td>
<td>A record of output messages related to security events.</td>
</tr>
<tr>
<td>Data</td>
<td>access_log.yyyy-mm-dd</td>
<td>/opt/zimbra/log/access_log.yyyy-mm-dd</td>
<td>A record of output messages related to requests received by the data server.</td>
</tr>
<tr>
<td>Gateway</td>
<td>access.log</td>
<td>/opt/nginx/logs/access.log</td>
<td>URLs that were requested and the status of each request.</td>
</tr>
<tr>
<td>Gateway</td>
<td>error.log</td>
<td>/opt/nginx/logs/error.log</td>
<td>Errors reported from the Web server running on the gateway.</td>
</tr>
</tbody>
</table>
After you complete the basic Horizon Workspace installation, you might need to complete other configuration
tasks in the Configurator, such as configuring View, integrating ThinApp, or cloning virtual machines.
Each component has multiple instances and custom functionality. Additionally, each virtual machine offers
different features. The Horizon Workspace architecture diagram demonstrates what you can build using the

This chapter includes the following topics:

- “Enabling External Access to Horizon Workspace,” on page 53
- “Configuring Redundancy/Failover for Horizon Workspace Virtual Machines,” on page 58
- “Configuring SecurID for Horizon Workspace,” on page 69
- “Configuring Kerberos for Horizon Workspace,” on page 71
- “Using SSL Certificates in Horizon Workspace,” on page 75
- “Adjusting Java Heap Size for Improved Performance,” on page 76

### Enabling External Access to Horizon Workspace

During deployment, the Horizon Workspace Setup wizard installs the Horizon Workspace vApp inside the
internal network. If you want to provide access to Horizon Workspace for users connecting from outside
networks, you must install a reverse load balancer, such as Apache, nginx, F5, and so on.

If you do not use a load balancer, you cannot expand the number of gateway-va virtual machines in the future.
You might need to add more gateway-va virtual machines to provide redundancy and load balancing.
Typically, if you have more than 2000 users, you may need to add an additional gateway-va virtual machine.
Additionally, if your deployment exceeds 2,000 users, you must also deploy the public service hostname and
IP address with a load balancer. The following diagram shows the basic deployment architecture you can use
to enable external access.
Specify Horizon Workspace FQDN during Deployment

During deployment for the configurator-va virtual machine, you must enter the Horizon Workspace FQDN and Horizon Workspace port number. These values must point to the hostname that you want end users to access.

**CAUTION** After you deploy, you cannot change the Horizon Workspace FQDN.

The gateway-va virtual machine in the Horizon Workspace vApp always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment time.

All the virtual machines in the Horizon Workspace vApp must be able to ping the Horizon Workspace FQDN. If one of the virtual machines cannot ping Horizon Workspace FQDN, the deployment process fails. Additionally, if the Horizon Workspace FQDN does not resolve to the gateway-va virtual machine, the configuration process in the Web interface fails.

You can run the following commands to check your installation after the command-line setup process is complete.

- `curl -kv https://<HorizonWorkspaceFQDN>/SAAS`
- `curl -kv https://<HorizonWorkspaceFQDN>/web`

Use Configurator Web Interface to Complete Deployment

You can complete the Horizon Workspace configuration process using the Configurator Web interface.

IDP Discovery and X-Forwarded-For Headers

You must enable X-Forwarded-For on your load balancer. Horizon Workspace identifies the source IP address in the X-Forwarded-For. Horizon Workspace determines which Connector to log in to based on this IP address. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.

Load Balancer Timeout

For Horizon Workspace to function correctly, you must increase the load balancer request timeout from the default. The value is set in minutes. For Horizon Workspace, the recommended value is 30 minutes. If the timeout setting is too low, you might see this error, “502 error: The service is currently unavailable.”

Enable Sticky Session on the Load Balancer to the Gateway

Ensure that you enable sticky session on the load balancer to the gateway servers if your deployment uses multiple gateway servers. Sticky session improves Web interface performance. If sticky session is not enabled, some functions might fail.

Establishing SSL Trust between Horizon Workspace vApp and Load Balancer

By default, the Horizon Workspace Setup wizard configures the Horizon Workspace vApp with a self-signed certificate. The Horizon Workspace Setup wizard enables HTTPS communication between the virtual machines and the vApp.

You must establish SSL trust between the load balancer and gateway-va virtual machine before you go to the Configurator Web interface for additional configuration.

Procedure

2. Paste the root certificate to the correct location on your load balancer. See the documentation provided by your load balancer vendor.
3. Run the following commands to check your installation.
   - curl -v https://<horizon workspace FQDN>:<Horizon Workspace port>/SAAS
   - curl -v https://<horizon workspace FQDN>:<Horizon Workspace port>/web

What to do next

Now, you can proceed to the Configurator to continue configuring your deployment.
Enabling AUDIT Events via Proxy Server

Horizon Workspace audits various user events, such as login, logout, entitlement, and provisioning. The service-va virtual machine uses a Web application to audit the events. The Web application runs on /AUDIT endpoint. Horizon Workspace does not authenticate the /AUDIT endpoint application to maintain performance. For security purposes, the gateway-va virtual machine only permits virtual machines in the Horizon Workspace vApp to use the /AUDIT endpoint.

If there are network proxy servers between the load balancer and gateway, these restrictions might prevent /AUDIT from working correctly.

Procedure

1. Verify that you can access the /AUDIT endpoint from the service-va virtual machine.
   b. Click Reports and click Audit Events.
      If no Audit Events appear in the table or you see an error, Audit Events are not working.

2. Modify the gateway-va virtual machine to update the Real_IP to resolve the issue.
   b. Add the set_real_ip_from <IP of Load Balancer>; line after the include gen/real_ip.conf; statement.
      The new line is the last in the sample.
      real_ip_header X-Forwarded-For;
      real_ip_recursive off;
      include gen/real_ip.conf;
      set_real_ip_from <IP of Load Balancer>;
   c. Type /etc/rc.d/nginx restart to restart nginx.

3. (Optional) If the audits still do not work, you can turn off the IP-based checks.
   b. Search for /AUDIT.
   c. Comment out # allow 127.0.0.1; # include gen/all.allow; and # deny all;.
   d. Type /etc/rc.d/nginx restart to restart nginx.

With the Audit function configured, you can use the audit information for tracking or troubleshooting.

Configuring an External Database

The service-va virtual machine provides a database for trial purposes only. If your production environment requires more than one service-va virtual machine for load-balancing, you must use an external database.

For high availability and load balancing, Horizon Workspace uses virtual machine clustering with the Add VM functionality.

To configure clustering for Horizon Workspace, you must connect the Horizon Workspace instance to an external database server. You can then add additional Manager (service-va) virtual machine instances to the deployment.

You can configure an external database connection when you run the Horizon Workspace Setup wizard, or after you run the wizard, you can go to the Database Connections page in the Configurator.
When you configure a connection from a Horizon Workspace instance to an external database server, it automatically disables the internal database server.

**NOTE** When you add (using the `hznAdminTool addvm` command) the Manager virtual machine to a deployment that is configured to use an external database, the newly added (cloned) Manager virtual machine automatically connects to the external database server. You do not need to configure an external database connection for the additional instance.

### Using Horizon Workspace Setup Wizard to Configure an External Database

If you configure your database using the Horizon Workspace Setup wizard, you must point Horizon Workspace to a database that has been prepared with a clean schema.

**Prerequisites**

Before you connect Horizon Workspace to an external database server, you must perform these tasks.

- Install and configure PostgreSQL 9.1 as the external database server, with the citext module installed. (The citext module supports the CITEXT data type, a case insensitive text type.)
- Install and configure the load balancing implementation.
- A clean database must include basic characteristics. You can see the characteristics in the script on the service-va virtual machine at `/usr/local/horizon/bin/setupExternalDb.sh`.
- Ensure that the database machine allows external connections. You can allow external connections by following these steps:
  
  a. Modify the following files to open the local postgres database for external access.
     
     - Open the `/db/data/pg_hba.conf` file and add this line at the bottom.
       ```
       host all all 0.0.0.0 0.0.0.0 md5
       ```
     - Open the `/db/data/postgresql.conf` file and change the listen address to listen on all addresses not just localhost.
       ```
       listen_addresses = '*'
       ```
     - Restart postgres.
       ```
       /etc/rc.d/vpostgres restart
       ```
  
  b. Restart postgres.

**Procedure**

1. Select **External Database** as a Database Type.
2. Enter information about the database connection.
   
   a. Type the JDBC URL of the database server.
      ```
      jdbc:postgresql://<IP_ADDRESS>/as?stringtype=unspecified
      ```
   
   b. Type the name of the user with read and write privileges to the database.
   
   c. Type the password for the user with read and write privileges to the database.
3. Click **Test Connection** to verify and save the information.

**What to do next**

Complete the Horizon Workspace configuration.
Using the Configurator to Configure an External Database

After you run the Horizon Workspace Setup wizard, you might want to change the database to an external database. Then, you can configure your database using the Configurator.

You must point Horizon Workspace to an initialized, populated database. For example, you can use a database configured as the result of a successful run of the Horizon Workspace Setup wizard, a database from a backup, or an existing database from a recovered snapshot.

Prerequisites

Before you connect Horizon Workspace to an external database server, you must perform these tasks.

- Install and configure Postgres 9.1 as the external database server, with the citext module installed. (The citext module supports the CITEXT data type, a case insensitive text type.)
- Install and configure the load balancing implementation.
- Install and configure Horizon Workspace. See Run Horizon Workspace Setup Wizard.

Procedure

1. Select External Database as a Database Type.
2. Enter information about the database connection.
   - Type the JDBC URL of the database server.
     jdbc:postgresql://<IP_ADDRESS>/saas?stringtype=unspecified
   - Type the name of the user with read and write privileges to the database.
   - Type the password for the user with read and write privileges to the database.
3. Click Test Connection to verify and save the information.

What to do next

Complete the Horizon Workspace configuration.

Configuring Redundancy/Failover for Horizon Workspace Virtual Machines

Horizon Workspace lets enterprises achieve failover and redundancy by adding multiple virtual machines of the same type in Horizon Workspace vApp. For instance, you can add a second gateway-va virtual machine and enable the load balancer to redirect requests to both gateways. If one of the gateway virtual machines shuts down for any reason, the Horizon Workspace will still be available.

In order to add a new virtual machine of any type, you must log in to the configurator-va virtual machine as root user and run the hznAdminTool addvm –type=<VMType> --ip=<new VM ip address> command.

NOTE This command must be executed only after both the command-line and Web interface configuration of Horizon Workspace vApp is completed successfully.

The new virtual machine IP address must follow the same guidelines as the IP addresses for the base virtual machines. It must resolve to a valid hostname using forward and reverse DNS. This IP address must be set up using the same netmask, network gateway, and DNS server name used in the original IP pool to deploy the vApp.

For Connector and Data virtual machines, this command creates the new virtual machine by cloning a base snapshot of the original virtual machine of the same type. The base snapshot is captured for all virtual machines during the initial deployment. The command fails if the base snapshot does not exist.
For service and gateway virtual machines, this command creates the new virtual machine by cloning the current virtual machine snapshot.

The Configurator virtual machine is a singleton. You cannot create multiple Configurator virtual machines.

**CAUTION** Base snapshots of the Connector and Data virtual machines must not be deleted.

### Multiple gateway-va Virtual Machines

Your enterprise can create multiple gateways of the same type to distribute traffic and eliminate potential downtime.

Adding multiple gateway virtual machines helps your enterprise:

- Improve availability to Horizon Workspace.
- Load balance requests to Horizon Workspace and decrease response time to the end user.

Response time is especially important if multiple end users frequently upload and download files using the data functionality.

**Procedure**

1. Obtain an IP address that is resolvable using reverse DNS.
   
   This IP address must be set up using the same netmask, network gateway, and DNS server name that was used in the original IP pool to deploy the vApp.

2. Go to configurator-va virtual machine and run the `hznAdminTool addvm --type=GATEWAY --ip=<new VM ip address>` command.

3. Add the new gateway to your load balancer so the requests are sent to both gateway virtual machines.

**What to do next**

You can configure your load balancer to route traffic to the new gateway-va virtual machine and add additional Connector, Service, or Data virtual machines.

### Multiple service-va Virtual Machines

Your enterprise can create multiple service-va virtual machines of the same type to distribute traffic and eliminate potential downtime.

Multiple service-va virtual machines help your enterprise with the following needs:

- Improve availability to Horizon Workspace.
- Load balance requests to Horizon Workspace and decrease response time to the end user.

**Prerequisites**

- You can only add additional service-va virtual machines if you use an external database.

**Procedure**

1. Obtain an IP address that is resolvable using reverse DNS.
   
   You must set this IP address using the same netmask, network gateway, and DNS server name used in the original IP pool to deploy the vApp.

2. Go to configurator-va virtual machine and run the `hznAdminTool addvm --type=APPLICATION_MANAGER --ip=<new VM ip address>` command.
3. Go to the Configurator Web interface at https://<ConfiguratorHostname> and open the System Information page.

The new service-va virtual machine is now in maintenance mode. When a virtual machine is in maintenance mode, the gateway-va virtual machine does not see it or route requests to it. Verify that the virtual machine was added correctly by checking the IP address.

4. Configure the IP table to rebuild the IP table rules.

**Note:** Horizon Workspace overwrites the IP table rules each time you add a new virtual machine and run the `addvm` command. As a result, you must rerun these commands each time you add a new virtual machine of any type.

### Table 6-1. Multiple service-va Virtual Machines IP Configuration Commands

<table>
<thead>
<tr>
<th>Action</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run this command on configurator-va virtual machine to list the IP addresses for all the service-va virtual machines, including the newly added service-va virtual machine.</td>
<td><code>hznAdminTool listvms</code></td>
</tr>
</tbody>
</table>
| Run these commands on all existing service-va virtual machines. The value of the `<OTHER_service_va_IP>` parameter equals the IP address of each existing or newly added service-va virtual machine. | `iptables -A INPUT -i eth0 -s <OTHER_service_va_IP> -p tcp --dport 9300:9400 --m state --state NEW,ESTABLISHED -j ACCEPT`  
`iptables -A OUTPUT -o eth0 -s <OTHER_service_va_IP> -p tcp --sport 9300:9400 --m state --state ESTABLISHED -j ACCEPT`  
`iptables -A INPUT -i eth0 -s <OTHER_service_va_IP> -p udp --dport 54328 --m state --state NEW,ESTABLISHED -j ACCEPT`  
`iptables -A OUTPUT -o eth0 -s <OTHER_service_va_IP> -p udp --sport 54328 --m state --state ESTABLISHED -j ACCEPT` |

For example, if you have two service-va virtual machines in your environment and add a third, you must go to the console for each service-va virtual machine and run these commands one at a time in order to rebuild the IP tables.

a. Run `hznAdminTool listvms` command.
b. Write down only the service-va virtual machine IP addresses.
c. Log in to the service-va virtual machine for IP address1 as root and go to the console.
d. Run the `iptables` command and use IP address2 as the value for the `<OTHER_service_va_IP>` parameter.
e. Run the `iptables` command and use IP address3 as the value for the `<OTHER_service_va_IP>` parameter.
f. Log in to the service-va virtual machine for IP address2 as root and go to the console.
g. Run the `iptables` command and use IP address1 as the value for the `<OTHER_service_va_IP>` parameter value.
h. Run the `iptables` command and use IP address3 for the value of the `<OTHER_service_va_IP>` parameter.
5 Run the following commands on the new service-va virtual machine and the existing service-va virtual machines to establish communication and record audit events.

<table>
<thead>
<tr>
<th>Action</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Run these commands on all existing service-va virtual machines. | service elasticsearch stop  
  hznAdminTool configureElasticSearch -ES_MULTICAST_ENABLED true  
  service elasticsearch start  
  service elasticsearch status |
| Run these commands on newly added service-va virtual machines. | service rabbitmq-server stop  
  service elasticsearch stop  
  rm /var/run/rabbitmq/pid  
  rm /var/run/rabbitmq/lock  
  rm /var/run/elasticsearch/elasticsearch.pid  
  rm /var/lock/subsys/elasticsearch  
  rm -R /db/rabbitmq/data/*  
  rm -R /db/elasticsearch/*  
  service rabbitmq-server start  
  service rabbitmq-server status  
  rabbitmqctl stop_app  
  rabbitmqctl force_reset  
  rabbitmqctl start_app  
  hznAdminTool configureElasticSearch -ES_MULTICAST_ENABLED true  
  service elasticsearch start  
  service elasticsearch status |


The Configurator updates all the gateway-va virtual machines and starts sending requests to the new service-va virtual machine as well.

In the future, if you want to stop routing requests to a service-va virtual machine, go to the Configurator Web interface and return the virtual machine to maintenance mode.

**What to do next**

You can add additional connector or data virtual machines.

### Multiple connector-va Virtual Machines

Your enterprise can create multiple connector-va virtual machines of the same type to reduce traffic and eliminate potential downtime.

Multiple connector-va virtual machines help your enterprise:

- Improve load balancing, failover, and availability to the Horizon Workspace authentication functionality.

- You can authenticate end users to Horizon Workspace using multiple methods of authentication, such as Active Directory username and password, username and RSA SecurID passcode, or Kerberos-based Windows authentication. To enable multiple forms of authentication, you must set up multiple connector-va virtual machines. See the sample multiple connector deployment with different kinds of authentication.

When you add an additional virtual machine for either the data-va or connector-va virtual machine, you must use a base snapshot. A base snapshot is taken automatically after deployment.
Horizon Workspace Authentication

Horizon Workspace authentication flow posts SAML authentication requests to the IdP URL.

The Horizon Workspace authentication flow follows a specific sequence to post SAML authentication requests to the IdP URL. The IdP URL can be one of the following:

- Connector hostname
- Load balancer server that load balances the requests among multiple connectors. When you use a load balancer server this way, the connectors it load balances must use the same type of authentication.
- Load balancing with Kerberos requires special URL rewriting configuration at the load balancer.
- Horizon Workspace FQDN redirects to the gateway and can also load balance the requests among multiple Connectors. The Connectors that are load balanced using this option must use the same type of authentication.
Enabling SecurID Authentication

In many cases, enterprises enable RSA SecurID-based authentication for their end users who connect from external networks.

You can enable RSA SecureID authentication with Horizon Workspace.

Procedure

1. Obtain an IP address that is resolvable using reverse DNS and select an IDP URL. This IP address must be set up using the same netmask, network gateway, and DNS server name used in the original IP pool to deploy the vApp.

2. Go to the configurator-va virtual machine and run the `hznAdminTool addvm --type=CONNECTOR --ip=<new VM ip address> --useGatewayAsIDP=<y or n> --directoryPassword=<AD BindDN password>` command.

3. Set the flag `useGatewayAsIDP` to `y` if you use the Horizon Workspace FQDN as the IDP URL.

   The new connector is automatically activated and connected to Active Directory.

4. Type the password for the BindDN user that you used during initial configuration.

   When `useGatewayAsIDP` is set to `y`, maintenance mode is turned on for the new connector-va virtual machine. When a virtual machine is in maintenance mode, the gateway-va virtual machine will not be aware of the virtual machine or route requests to it.

5. Go to the Configurator Web interface at `https://<ConfiguratorHostname>`.

   a. Click System Information.

   b. Find the new virtual machine you added.

   c. Click Exit Maintenance Mode.

   The Configurator updates all the gateway virtual machines and sends new requests to the new connector virtual machine.

   **Note** In the future, if you do not want requests routed to that connector-va virtual machine, return to the Configurator Web interface and put the virtual machine in maintenance mode.
6 Go to the Connector you just created using the Web interface at https://<ConnectorHostname>/hc/admin.
   a Log in using the admin password.
   b Click on SecurID.
   c Click on Enable SecurID.

7 Go to the Manager Web interface at https://<HorizonWorkspaceFQDN>/admin.
   a Click the Settings tab.
   b Click Identity Providers.
   c Edit the new Identity Provider.
   d Edit the IP address list.

What to do next
To configure SecurID for end users who connect to the network from external networks, see “Configuring SecurID for Horizon Workspace,” on page 69.

Enabling Kerberos Authentication
Enterprises can enable Kerberos authentication for their end users who connect from internal Windows machines. When you use Kerberos authentication, end users can log in to Horizon Workspace without typing a username and password.

You can enable Kerberos authentication with Horizon Workspace.

Procedure
1 Obtain an IP address that is resolvable using reverse DNS and select the IDP URL. This IP must be set up using the same netmask, network gateway, and DNS server name used in the original IP pool to deploy the vApp.

2 Go to the configurator-va virtual machine at https://<configurator-va hostname>.
   a Run the hznAdminTool addvm --type=CONNECTOR --ip=<new VM ip address> --useGatewayAsIDP=<y or n> --directoryPassword=<AD BindDN password> command.

   Kerberos authentication requires that the Connector’s IDP URL and the hostname are the same.
   b Set the flag useGatewayAsIDP to n.

   NOTE The new connector is automatically activated and connected to Active Directory. Provide the password for the BindDN user that you used during initial configuration.

3 Go to Connector Web interface at https://<new connector-va hostname>/hc/admin and log in with the admin password.
   a Join the new connector to the domain.
   b Click Windows Auth.
   c Enable Windows Authentication.

4 Go to Service Web interface at https://<Horizon workspace FQDN>/admin.
   a Click Settings tab.
   b Click Identity Providers.
   c Edit the new Identity Provider.
   d Edit the IP address list.
What to do next

To enable Kerberos authentication for end users who connect to the network using internal Windows machines, see “Configuring Kerberos for Horizon Workspace,” on page 71.

Multiple data-va Virtual Machines

Horizon Workspace Data provides file-sharing functionality that the data-va virtual machine manages. When a large number of users store and read files at the same time, the intense input/output processing can affect performance of the data-va virtual machine. You can add additional data-va virtual machines.

**IMPORTANT** It is recommended that each data-va virtual machine serve no more than 1000 users.

User Sharding

User accounts are provisioned to a specific data-va virtual machine that handles their file activity. The account’s class of service (COS) determines the data-va virtual machine where the account is provisioned. If the host pool in the COS specifies only one data-va virtual machine, users entitled to that COS are provisioned on that data-va virtual machine. If the host pool in the COS specifies multiple data-va virtual machines, users are randomly provisioned to any of the data-va virtual machines in the list.

When you add a new data-va virtual machine, the new data-va virtual machine automatically becomes available from the default COS host pool. The host pool for other classes of service that are created displays the new data-va virtual machine, but it is not enabled in that COS. To use a new data-va virtual machine in the other classes of service, the administrator must modify the COS and enable the data-va virtual machine.

When you add an additional virtual machine for either the data-va or connector-va virtual machines, you must use a base snapshot. A base snapshot is taken automatically after deployment.

**IMPORTANT** The first data-va virtual machine in the Horizon Workspace configuration is the master node. This node contains the metadata for the data-va virtual machine user accounts. If you create additional data-va virtual machines, these data-va virtual machines are file stores only. When the master node is down, users cannot log in to their data accounts.

You can configure the host pool in the COS to use specific data-va virtual machines. In this way, you can manage where accounts are provisioned. For example, you add a second data-va virtual machine because disk space on the first data-va virtual machine is low. You do not want the first data-va virtual machine to be provisioned with any more new accounts once you have added the second node. From the Horizon Workspace Administrator Web interface, edit each COS to select the new data-va virtual machine in the Host Pool and deselect the other data-va virtual machine.

**NOTE** When a user signs in to access their Horizon Workspace Folders, the gateway-va virtual machine routes the request to the data-va virtual machine where they are provisioned. When a data-va virtual machine is down, users receive a 502 error. The user’s authentication request is denied. In addition, when the data-va virtual machine is down, files shared from accounts on that machine cannot be accessed.

Creating a New data-va Virtual Machine

To maximize performance for the Data module, you can add a new data-va virtual machine.

**IMPORTANT** It is recommended that each data-va virtual machine serve no more than 1,000 users. If your deployment includes multiple data-va virtual machines with 1,000 users each, you must configure all the other virtual machines using the requirements shown in the Recommended Virtual Machine Requirements table. See Chapter 2, “System and Network Configuration Requirements,” on page 11 for more information.
Procedure

1. Obtain an IP address that is resolvable using reverse DNS.
   You must set this IP address using the same netmask, network gateway, and DNS server name used in
   the IP pool to deploy the vApp.

2. Go to configurator-va and run the addvm command.
   
   hznAdminTool addvm -type=DATA --ip=<new VM ip address>
   
   The new data-va virtual machine is now in maintenance mode.

3. Enable Preview functionality for the new data-va virtual machine.
   a. Log in to the new data-va virtual machine as the root user.
   b. Set the proxy information, if you use a proxy, to reach the Internet.
      
      export http_proxy="proxy url:port"
   c. If you use LibreOffice, download and install it by running /opt/zimbra/libexec/libreoffice-
      installer.sh.
      
      If you use Microsoft Windows Preview Server, run the zmlocalconfig command to configure the new
      data-va virtual machine to point to the Microsoft Windows Preview Server.

4. Restart each existing data-va virtual machine after it is added.
   
   Restarting the existing virtual machines ensures that they are aware of the newly installed data-va virtual
   machine.

5. Populate the ssh keys on each machine.
   a. Log in to each data-va virtual machine as the root user.
   b. Reboot each machine.
      
      reboot
   c. Change to the Zimbra user.
      
      su – zimbra
   d. Run the zmupdateauthkeys command.
      
      /opt/zimbra/.ssh/authorized_keys/zmupdateauthkeys

6. Restart memcached as the root user.
   
   /etc/rc.d/memcached restart

7. Go to the Configurator Web interface at https://<configurator-va hostname> and open the System
   Information page.

8. Find the virtual machine you added on the System Information page and click Exit maintenance mode.
   
   The new data-va virtual machine is ready to use.

What to do next

Modify the COS host pools from the Administrator Web interface. See Horizon Workspace Administrator Guide.
Distributing External Virtual Users

External virtual users are given a COS called `defaultExternal` that is not visible from the Horizon Workspace Administrator Web interface. This COS determines the data-va virtual machine that external virtual users are provisioned on.

By default, all data-va virtual machines are enabled in the host pool on the `defaultExternal` COS. You must modify this COS to specify the data-va virtual machines to use.

If you want virtual users to be assigned to a specific data-va virtual machine or you want to change the machines that are enabled, modify the `defaultExternal` COS to enable the machine you want to use.

Procedure

1. Log in to the new data-va virtual machine as the root user.
2. Change to the Zimbra user.
   ```
   su - zimbra
   ```
3. Run the `zmprov` command on the ID of the data-va virtual machine you want to use.
   ```
   zmprov gs <data-va> hzndataId
   ```
   Horizon Workspace uses this ID format: 45c3e8ce-5617-4bf7-9c92-334ab36f9f7b.
4. Find the names of the data-va virtual machine nodes that are in the DefaultExternal COS host pool

   **NOTE** If the `defaultExternal` COS has not been modified to add specific data-va virtual machines to the host pool, this command does not return a value. If you use the default value, all data-va virtual machines are enabled in the host pool.

   - Modify the `defaultExternal` COS host pool to add, remove, or replace a data-va node using one of the following commands. Add a data-va node to the host pool.
     ```
     zmprov mc defaultExternal +hzndataHostPool <data-vaname.com|ID>
     ```
   - Remove a data-va node from the host pool.
     ```
     zmprov mc defaultExternal -hzndataHostPool <data-vaname.com|ID>
     ```
   - Replace all data-va virtual machines in the host pool.
     ```
     zmprov mc defaultExternal hzndataHostPool <data-vaname.com|ID>
     ```

What to do next

If there is a problem with a data-va virtual machine, you can permanently remove it.

Removing a data-va Virtual Machine Temporarily

To add storage or perform other maintenance on a specific data-va virtual machine, you can shut down the machine temporarily. No new accounts are provisioned on the data-va virtual machine while it is down.

While the data-va virtual machine is down, users provisioned to this virtual machine cannot access the Data Web Client interface.

**NOTE** When a user signs in to access their Horizon Workspace Folders, the gateway-va virtual machine routes the request to the data-va virtual machine where they are provisioned. When a data-va virtual machine is down, users receive a 502 error. The user's authentication request is denied. In addition, when the data-va virtual machine is down, files shared from accounts on that machine cannot be accessed.
Procedure

2. Click the **Enter maintenance mode** link next to the data-va virtual machine you want to temporarily disable.
3. Log in to the data-va virtual machine as root.
   a. Change to the Zimbra user.
      ```
      su - zimbra
      ```
   b. Remove the data store mailbox service.
      ```
      zmprov -l -hzndataServiceEnabled mailbox
      ```
      **NOTE** The attribute **hzndataServiceEnabled** is a multi-valued Data LDAP attribute.
   c. Stop the Jetty process.
      ```
      zmmailboxdctl stop
      ```

**What to do next**

If you need to remove a data-va virtual machine permanently, see “Removing a data-va Virtual Machine Permanently,” on page 69.

**Adding a data-va Virtual Machine Back into Rotation**

When you finish with the maintenance on the data-va virtual machine, you can add it back to the rotation.

Once a data-va virtual machine returns to the rotation, you can provision users to it and users can access the Data Web Client interface.

**Procedure**

   a. Log in to the data-va virtual machine as the root user.
   b. Change to the Zimbra user.
      ```
      su - zimbra
      ```
   c. Add the mailbox service back.
      ```
      zmprov -l +hzndataServiceEnabled mailbox
      ```
   d. Start the Jetty process.
      ```
      zmmailboxdctl start
      ```
3. Click the **Enter maintenance mode** link next to the appropriate data-va virtual machine.

**What to do next**

If you need to remove a data-va virtual machine permanently, see “Removing a data-va Virtual Machine Permanently,” on page 69.
Removing a data-va Virtual Machine Permanently

When a data-va virtual machine is damaged and no longer operational, you can move the users provisioned to that virtual machine to another data-va virtual machine before removing the data-va virtual machine.

Procedure

1. Log in to a data-va virtual machine as the root user.
2. Change to the Zimbra user.
   `su - zimbra`
3. List user accounts on the server.
   `zmprov -l gaa -s <server>`
4. Type the following command for each account you want to move to another data-va virtual machine.
   `zmboxmove -a useraccount --from <src> --to <dest> [sync]`
   This sample command moves user1 from the data2 data-va virtual machine to data1 data-va virtual machine. When an account move finishes, a success or failure notice appears.
   `zmboxmove -a user1@domain.com -f data2.domain.com -t data1.domain.com sync`
5. Restart each Horizon Workspace gateway-va virtual machine.
   a. Log in to the gateway-va as the root user.
   b. Restart the memcached.
      `/etc/rc.d/memcached restart`
6. Flush the memcached without stopping.
   `wget -O - --quiet http://<GatewayIP:port>/flush`
7. Log in to the destination data-va virtual machine.
8. Verify that you can access the user accounts before shutting down the old data-va virtual machine.
9. Delete the old data-va virtual machine from the metadata.
   `zmprov ds <server>`
10. Power the data-va virtual machine off.

What to do next

When you remove the data-va virtual machine permanently, if you want to restore it, you must re-add the server. See “Creating a New data-va Virtual Machine,” on page 65.

Configuring SecurID for Horizon Workspace

When you configure RSA SecurID server, you must prepare the RSA SecurID server for the Connector and configure SecurID with the Connector Web interface.

After you deploy Horizon Workspace, you can configure SecurID to provide additional security. You must ensure your network is properly configured for your Horizon Workspace deployment. For SecurID specifically, you must ensure that the appropriate port is open to enable SecurID to authenticate users outside the enterprise network.

After you run the Horizon Workspace Setup wizard, you have the information necessary to prepare the RSA SecurID server. After you prepare the RSA SecurID server for the Connector, you use the Connector Web interface to configure the SecurID page.
Preparing the RSA SecurID Server for the Connector

If you want to provide RSA SecurID security, prepare the RSA SecurID server for the Connector.

You must change the Connector-specific information necessary to configure the Connector with RSA SecurID. For detailed information about configuring the RSA SecurID server, see RSA documentation.

**IMPORTANT** After you restart the RSA SecurID server, the system takes time to become operational. Wait time can vary, but expect from several minutes to half an hour of delay before the system can process authentication requests from the Connector.

**Prerequisites**

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network to allow communication with the Connector: 6.1.2, 7.1 SP2, or 7.1 SP3. Horizon Workspace uses AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), which only supports the preceding versions of RSA Authentication Manager (the RSA SecurID server). For information about installing and configuring RSA Authentication Manager (RSA SecurID server), see RSA documentation.
- Install and configure the Connector. After you install the Connector and use the Configurator Web interface to run the setup wizard, you have the information necessary to prepare the RSA SecurID server.

**Procedure**

1. On a supported version of the RSA SecurID server, add the Connector as an authentication agent.
2. Type in the following Connector-related information when you add the Connector as an agent.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>The hostname of the Connector.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the Connector.</td>
</tr>
<tr>
<td>Alternate IP address</td>
<td>If traffic from the Connector passes through a network address translation</td>
</tr>
<tr>
<td></td>
<td>(NAT) device to reach the RSA SecurID server, enter the private IP address</td>
</tr>
<tr>
<td></td>
<td>of the Connector.</td>
</tr>
</tbody>
</table>

Be prepared to provide this information again in the Connector Web interface when you configure the SecurID page that is available on the **Advanced** tab.

3. Download the compressed configuration file and extract the `sdconf.rec` file.

Be prepared to upload this file later with the Connector Web interface when you configure the SecurID page that is available on the **Advanced** tab.

**What to do next**

Using the Connector Web interface, configure the SecurID page that is available on the **Advanced** tab.

Configuring SecurID with the Connector Web Interface

After you run the Horizon Workspace Setup wizard, you can configure the SecurID page.

**Prerequisites**

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the compressed file from the RSA SecurID server and extract the server configuration file. See “Preparing the RSA SecurID Server for the Connector,” on page 70.
Procedure

1. Click Advanced > SecurID to open the SecurID page.
2. Click the Enable SecurID check box.
3. Configure the SecurID page.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page. See “Preparing the RSA SecurID Server for the Connector,” on page 70.

Table 6-3. SecurID Configuration Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector Address</td>
<td>Enter the appropriate Connector IP address. The value you enter matches the value you used to configure the RSA SecurID Server when you added the Connector as an authentication agent. If your RSA SecurID server has a value assigned to the Alternate IP address prompt, enter that value as the Connector IP address. If no alternate IP address is assigned, enter the value assigned to the IP address prompt instead.</td>
</tr>
<tr>
<td>Agent IP Address</td>
<td>Enter the value assigned to the IP address prompt in the RSA SecurID server.</td>
</tr>
<tr>
<td>Server Configuration</td>
<td>Upload the server configuration file. First, you must download the compressed file from the RSA Secure ID server and extract the server configuration file, which by default is named sdconf.rec.</td>
</tr>
<tr>
<td>Node Secret</td>
<td>Leaving the node secret blank allows the node secret to autogenerate. It is recommended that you clear the node secret file on the RSA SecurID server and intentionally do not upload the node secret file to the Connector. Ensure that the node secret file on the RSA SecurID server and on the Connector always match. If you change the node secret at one location, change it respectively at the other location. For example, if you clear or generate the node secret on the RSA SecurID server, clear or upload the node secret file on the Connector as well.</td>
</tr>
</tbody>
</table>

4. Save your SecurID settings.

Configuring Kerberos for Horizon Workspace

When you configure Kerberos for Horizon Workspace, you must consider many different components. Configuring Kerberos for the Connector involves installation, and possibly configuration tasks. Kerberos authentication provides another layer of security for your Horizon Workspace deployment.

Active Directory Configuration

You do not need to directly configure Active Directory to make Kerberos function with your Horizon Workspace deployment.

Connector Installation

After you install the Connector, you use the Connector Web interface to enable the Connector to use Kerberos authentication. To enable the Connector, you must first join the domain on the Join Domain page and then enable Windows Authentication on the Windows Authentication page.

Configure Join Domain

You can configure the join domain functionality in the Connector on the Join Domain tab. You must enable join domain functionality to provide single sign-on to the Web interface using Windows authentication (Kerberos).

The Active Directory information that you provide for the Join Domain page is for the user who has permission to join machines to the Active Directory domain.
Table 6-4. Active Directory Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD FQDN</td>
<td>The text box for the fully qualified domain name of an Active Directory instance. The domain name you enter must be the same Windows domain where the Connector resides.</td>
</tr>
<tr>
<td>AD Username</td>
<td>The text box for the username associated with the user account that has permission to join machines to the Active Directory domain.</td>
</tr>
<tr>
<td>AD Password</td>
<td>The text box for the password associated with the user account that has permission to join machines to the Active Directory domain.</td>
</tr>
<tr>
<td>Join Domain/Leave Domain</td>
<td>The button to join and leave the domain. The wording on the button changes to and from Join Domain and Leave Domain depending on whether you last joined or left the domain.</td>
</tr>
</tbody>
</table>

Enabling Windows Authentication

You can enable Windows authentication (Kerberos) in the Connector on the Windows Auth tab. You must enable Windows authentication to allow the Kerberos protocol to secure interactions between users’ browsers and Horizon Workspace.

Prior to enabling Windows authentication on this page, you must join the Connector to the Active Directory domain on the Join Domain page.

Table 6-5. Windows Authentication Information

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Windows Authentication</td>
<td>The check box to extend authentication interactions between users’ browsers and Horizon Workspace.</td>
</tr>
</tbody>
</table>

Kerberos Authentication Operating System Support

Currently, interactions between a user’s browser and Horizon Workspace are authenticated by Kerberos on the Windows operating systems only. Accessing Horizon Workspace from other operating systems does not take advantage of Kerberos authentication.

Browser Configuration

These browsers, Firefox, Internet Explorer, and Chrome, can support Horizon Workspace, on Windows only, during Kerberos authentication. All the browsers require additional configuration.

Configuring Internet Explorer to Access the Web Interface

You must configure the Internet Explorer browser if Kerberos is configured for your Horizon Workspace deployment and if you want to grant users access to the Web interface using Internet Explorer.

Kerberos authentication works in conjunction with Horizon Workspace on Windows operating systems.

**Note** Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

Configure the Internet Explorer browser, for each user, or provide users with the instructions, after you configure Kerberos.

Procedure

1. Verify that you are logged in to Windows as a user in the domain.
2 In Internet Explorer, enable automatic log on.
   a Select Tools > Internet Options > Security.
   b Click Custom level.
   c Select Automatic login only in Intranet zone.
   d Click OK.

3 Verify that this instance of the Connector is part of the local intranet zone.
   a Use Internet Explorer to access the Connector login URL at
      https://ConnectorHostname.DomainName/authenticate/.
   b Locate the zone in the bottom right corner on the status bar of the browser window.
      If the zone is Local intranet, Internet Explorer configuration is complete.

4 If the zone is not Local intranet, add the Connector to the intranet zone.
   a Select Tools > Internet Options > Security > Local intranet > Sites.
   b Select Automatically detect intranet network.
      If this option was not selected, selecting it might be sufficient for adding the Connector to the intranet zone.
   c (Optional) If you selected Automatically detect intranet network, click OK until all dialog boxes are closed.
   d In the Local Intranet dialog box, click Advanced.
      A second dialog box named Local intranet appears.
   e Type the Connector URL in the Add this Web site to the zone text box.
      https://ConnectorHostname.DomainName/authenticate/
   f Click Add > Close > OK.

5 Verify that Internet Explorer is allowed to pass the Windows authentication to the trusted site.
   a In the Internet Options dialog box, click the Advanced tab.
   b Select Enable Integrated Windows Authentication.
      This option takes effect only after you restart Internet Explorer.
   c Click OK.

6 Log in to the Connector Web interface at https://ConnectorHostname.DomainName/authenticate/ to check access.
   If Kerberos authentication is successful, the test URL goes to the Web interface.

The Kerberos protocol secures all interactions between this Internet Explorer browser instance and Horizon Workspace. Now, users can use single sign-on access to Horizon Workspace.

**Configuring Firefox to Access the Web Interface**

You must configure the Firefox browser if Kerberos is configured for your Horizon Workspace deployment and if you want to grant users access to the Web interface using Firefox.

Kerberos authentication works in conjunction with Horizon Workspace on Windows operating systems.

**Note** Do not implement these Kerberos-related steps on other operating systems.
Prerequisites

Configure the Firefox browser, for each user, or provide users with the instructions, after you configure Kerberos.

Procedure

1. In the URL text box of the Firefox browser, type about:config to access the advanced settings.
2. Click I’ll be careful, I promise!.
4. Type your Connector URL in the text box.
   
   https://<ConnectorHostname>

5. Click OK.
7. Type your Connector URL in the text box.
   
   https://<ConnectorHostname>

8. Click OK.
9. Test Kerberos functionality by using the Firefox browser to log in to the Connector at https://<ConnectorHostname>.
   
   If the Kerberos authentication is successful, the test URL goes to the Web interface.

The Kerberos protocol secures all interactions between this Firefox browser instance and Horizon Workspace. Now, users can use single sign-on access to Horizon Workspace.

Configuring Chrome Browser to Access the Web Interface

You must configure the Chrome browser if Kerberos is configured for your Horizon Workspace deployment and if you want to grant users access to the Web interface using the Chrome browser.

Kerberos authentication works in conjunction with Horizon Workspace on Windows operating systems.

Note: Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

- Configure Kerberos.
- Since Chrome uses the Internet Explorer configuration to enable Kerberos authentication, you must configure Internet Explorer to allow Chrome to use the Internet Explorer configuration. See http://dev.chromium.org/developers/design-documents/http-authentication on how to configure Chrome for Kerberos authentication.

Procedure

1. Test Kerberos functionality by using the Chrome browser.
2. Log in to the Connector at https://<Horizon workspace FQDN>.
   
   If Kerberos authentication is successful, the test URL connects with the Web interface.

If all related Kerberos configurations are correct, the relative protocol (Kerberos) secures all interactions between this Chrome browser instance and Horizon Workspace. Now, users can use single sign-on access to Horizon Workspace.
Using SSL Certificates in Horizon Workspace

SSL protects communications to Horizon Workspace and within it. During the Horizon Workspace Web interface initialization, the Configurator randomly generates a self-signed Horizon Workspace root CA certificate.

The Horizon Workspace Setup wizard generates individual certificates for each virtual machine in the vApp and chains those certificates to the newly generated root CA. Horizon Workspace uses the hostname as the CN within the certificate for all machines except the Gateway. The Horizon Workspace Setup wizard uses the Horizon Workspace FQDN to generate the SSL certificate for the Gateway.

Since the initial SSL certificates in the vApp do not chain to a publicly available root CA, the generated root CA must be distributed to establish trust between Horizon Workspace and its clients. The initial Horizon Workspace Setup wizard automatically distributes the root CA certificate to all virtual machines in the vApp to establish trust for intra-workspace communication.

If you deploy Horizon Workspace with our generated SSL certificates, the Horizon Workspace root CA certificate must be available as a trusted CA for any client who accesses Horizon Workspace. The clients can include end user machines, load balancers, proxies, and so on. You can download the Horizon Workspace root CA from http://<gateway hostname>/horizon_workspace_rootca.pem.

Applying an SSL Certificate from a Major Certificate Authority

All communication in the vApp is processed by the Horizon Workspace FQDN server. Horizon Workspace pre-loads the machines in the vApp to trust the major certificate vendors. As a result, if custom SSL certificates chain to one of the major certificate vendors, you can apply the new certificate by copying it to the load balancers, Gateway, or Connector.

If Horizon Workspace FQDN points to a load balancer, the SSL certificate can only be applied to the load balancer. Since the load balancer communicates with the gateway-va virtual machine, you must copy the Horizon Workspace root CA certificate to the load balancer as a trusted root certificate. When you update your certificate, if you are using View integration, you must follow the steps in “Establishing or Updating SSL Trust between the Connector and the View Connection Server,” on page 49.

When you use multiple load balancers, you must copy the certificate to all of them. If you do not use a load balancer, the Horizon Workspace FQDN points to the gateway-va virtual machine. In this case, you must apply the SSL certificate to the gateway-va virtual machine.

Procedure

1. Apply the certificate to each of your load balancers. Refer to the documentation from your load balancer vendor.

2. Apply the certificate to the gateway-va virtual machine.
   a. Go to https://<configurator va>.
   b. Log in and click SSL Certificate.
   c. Copy the complete certificate chain and private key. Ensure that the certificate includes the Horizon Workspace FQDN hostname in the CN.
   d. Save the SSL certificate.

   The Configurator copies the certificate to the gateway-va virtual machine.

3. If your deployment uses external connectors that grant users access to the connector as an IDP URL either directly or through a load balancer, apply the certificate to the connector-va virtual machine.
   a. Go to https://<connector va>/hc/admin.
   b. Log in and click SSL Certificate.
c Copy the complete certificate chain and private key. Ensure that the certificate includes the FQDN hostname for the connector-va virtual machine in the CN.

d Save the SSL certificate.

The Configurator copies the certificate to the connector-va virtual machine.

4 Verify that users can log in successfully.

If SSL authentication related errors occur, your root CA certificate might not be included in the Horizon Workspace trusted certificate list. In that case, see “Applying an SSL Certificate from a Private Certificate Authority,” on page 76 to correct the issue.

Applying an SSL Certificate from a Private Certificate Authority

Some enterprises use certificates generated by their own company or other certificate authorities. These certificates have not been included in the trusted certificate authority list.

In this case, even if you apply the certificate correctly, some processes might not trust the certificate and will fail. You must apply the certificate using these steps. Install your CA certificate on all the virtual machines in the vApp.

Procedure

1 Copy both the root CA and issuing CA certificates in PEM format to all the virtual machines.

/etc/ssl/certs/

2 Run the c_rehash command.

3 Run the cacerts command on the service-va and connector-va virtual machines.

- Root CA certificate command: /usr/java/jre1.6.0_37/bin/keytool -import -trustcacerts -file /etc/ssl/certs/horizon_private_root_ca.pem -alias horizon_private_root_ca -keystore /usr/java/jre-vmware/lib/security/cacerts

- Issuing CA certificate command: /usr/java/jre1.6.0_37/bin/keytool -import -trustcacerts -file /etc/ssl/certs/horizon_private_issuing_ca.pem -alias horizon_private_issuing_ca -keystore /usr/java/jre-vmware/lib/security/cacerts

4 Run the cacerts command on the data-va virtual machine.

- /opt/zimbra/jdk1.7.0_05/jre/bin/keytool -import -trustcacerts -file /etc/ssl/certs/horizon_private_root_ca.pem -alias horizon_private_root_ca -keystore /opt/zimbra/jdk1.7.0_05/jre/lib/security/cacerts

- /opt/zimbra/jdk1.7.0_05/jre/bin/keytool -import -trustcacerts -file /etc/ssl/certs/horizon_private_issuing_ca.pem -alias horizon_private_issuing_ca -keystore /opt/zimbra/jdk1.7.0_05/jre/lib/security/cacerts

Now, you can be sure that the virtual appliances trust the new root certificate. You must apply the certificate on the gateway, load balancers, and any external connectors. See “Applying an SSL Certificate from a Major Certificate Authority,” on page 75.

Adjusting Java Heap Size for Improved Performance

The Java heap size settings must be changed manually on the data-va and connector-va virtual machines if you add or remove memory. The service-va virtual machine automatically adjusts the settings.
Updating Java Heap Size on the Data Virtual Machine

If you increase the capacity of the virtual machines, you must increase the Java heap size settings. As a best practice, you set the Java heap size to half the total memory allocated to the data-va virtual machine.

The maximum value for the `mailboxd_java_heap_size` must be less than 10GB.

**Procedure**

1. Open the data-va.
2. Log in as a root user.
3. Change to the Zimbra user.
   
   `su - zimbra`
4. Type `zmlocalconfig -e mailboxd_java_heap_size` to edit the heap size.
5. Type the new value to update the heap size setting.
6. Type `zmcontrol restart` to restart the server.

----

Updating Java Heap Size on the Connector Virtual Machine

If you increase the capacity of the virtual machines, you must also increase the Java heap size settings. As a best practice, you set the Java heap size to include the total memory allocated to the connector-va virtual machine minus 1GB. The 1GB of memory is reserved for use by the system and the ThinApp repo server.

The maximum value for the `mailboxd_java_heap_size` must be less than 10GB.

**Procedure**

1. Open the connector-va.
2. Log in as a root user.
3. Modify the `Xmx` property in `/opt/vmware/c2/c2instance/bin/setenv.sh`.
4. Type the new value for the Java heap size.

   The new value must include all the memory allocated to the connector-va virtual machine minus 1GB.
Index

A
Active Directory
  domain service forest 39
  global catalog 39
  groups 26
  join 47
  users 26
  add, storage 35
  add user, Demo User Store 42
  add VM to rotation 68
  audience 5
  AUDIT events 56
  authentication 63, 64

C
  checklist
    Active Directory Domain Controller 18
      network information
        Configurator 18
        Connector 18
        Data 18
        Gateway 18
        IP Pools 18
        Manager 18
  Chrome 74
  configurator-va 24, 30
  configure
    data preview 37, 38
    logging 50
    SAML authentication 48
    virtual machines 53
  connector-va 58, 59, 61
    create, Windows applications network share 44

D
  data preview 37
  data-va 35, 58, 65
  delete extensions 26
  demo user store 41
  deployment
    checklists 18
    preparation 17
    distributing external virtual users 67
  DNS 17
  download OVA file 17

E
  external access 53
  external database
    Configurator 58
    Horizon Workspace Setup wizard 57

F
  failover 58, 59, 61, 65
  Firefox 73
  forward DNS 17

G
  gateway-va 58, 59
  groups, assign users 43

H
  hardware
    ESX 11
    Horizon Workspace 11
    requirements 11
  Horizon Workspace
    deploy 23
    install 23
    license key 18
  Horizon Workspace Setup wizard 26

I
  IdP discovery 8
  IdP URL 62
  install
    Mac desktop client 34
    Windows desktop client 34
  Internet Explorer 72

J
  Java Heap Size
    connector-va 77
    data-va 77
  join, Active Directory Domain 47

K
  Kerberos 64, 71–74
L
Linux
  SUSE 5
    system administrator 5
load balancer 55
logging 50

M
Microsoft Windows Preview 18, 38
modify, preview server 39
MTA 25
multiple virtual machines 58, 59, 61, 65

N
NAS 36
network configuration, requirements 11

O
OVA file
  deploy 23
  install 23
overview, install 6

P
port, 3268, 3269 39
preview
  LibreOffice 37
  Microsoft Windows 38
proxy server 56
proxy server settings 50

Q
quiesce timeout 26

R
redundancy 58, 59, 61, 65
remove
  data-va permanently 69
  data-va temporarily 67
reverse DNS 17
reverse lookup 17
RSA SecurID server 70
run, Configurator Virtual Appliance 24

S
SAML authentication 48, 62
SecurID, configure 70
server components 5
service-va 58, 59
setup wizard, setup wizard 26
SMTP server 25
SMTP Server 18
SSHA encrypted password 43
SSL certificate
  major certificate authority 75
  private authority 76
SSL trust, update on View Connection Server 49
storage 35, 36
storage, adding 37
SUSE Linux 5
sync
  View Connection Server 47
  View pools 48
system and functional administrator
  Linux 5
  Windows 5

T
ThinApp
  change share folder 46
  configure 35, 45
  packages 44

U
update Windows desktop client 33
URLs 33
user authentication 5, 7

V
vApp 55
vCenter
  credentials 18
  extensions 26
  password 32
  timeout 26
View 46
View desktop, start 49
View pools
  configuration 50
  sync 48
virtual appliance, requirements 11
VMDK 35, 36

W
Windows
  applications network share 44
  system administrator 5