Installing and Configuring VMware Workspace Portal

Workspace Portal 2.1.1

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

EN-001538-04
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
7 Advanced Configuration for VMware Workspace Portal Appliance 39
   Using a Load Balancer to Enable External Access to Workspace 39
   Apply Workspace Root Certificate to the Load Balancer 41

8 Configuring Redundancy 43
   Configuring Redundancy/Failover for Workspace Appliance in the Same Data Center 43
   Create Multiple Workspace Virtual Appliances 43
   Deploying Workspace in Secondary Data Center with Active-Active Read-Only Capability 46
   Setting Up a Secondary Data Center 48

9 Setting Up User Authentication 53
   Configuring SecurID for Workspace 53
      Prepare the RSA SecurID Server for the Connector Services Admin 54
      Configure RSA SecurID Authentication in Workspace 54
   Configuring Kerberos for Workspace 55
      Configure Kerberos on Workspace 56
      Configure Internet Explorer to Access the Web Interface 57
      Configure Firefox to Access the Web Interface 58
      Configure the Chrome Browser to Access the Web Interface 58

10 Customizing the Demo User Store 61
   Add a User to the Demo User Store 62
      Generate an SSHA Encrypted Password 63
      Add Groups and Assign Users to Groups in the Demo User Store 64

Index 65
The VMware Workspace Portal Installation and Configuration Guide leads you through the installation and configuration process for the Workspace appliance. When the installation is finished, you can use VMware Workspace™ Portal to entitle users to managed multi-device access to your organization’s applications, including Windows applications, software as a service (SaaS) applications, and View desktops.

**Intended Audience**

This information is intended for system and functional administrators of VMware Workspace™ Portal. The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, vSphere®, and View™, networking concepts, Active Directory servers, Simple Mail Transfer Protocol (SMTP), and NTP servers. SUSE Linux 11 is the underlying operating system for the virtual appliance. Knowledge of other technologies, such as VMware ThinApp®, RSA SecurID, and Active Directory is helpful if you plan to implement those features.
Preparing to Install VMware Workspace Portal

The tasks to deploy and set up VMware Workspace Portal requires that you complete the prerequisites, deploy the Workspace OVF file and complete the set up from the Workspace set up wizard.

**Figure 2-1. VMware Workspace Portal Architecture Diagram for Typical Deployments**

This chapter includes the following topics:

- “Workspace System and Network Configuration Requirements,” on page 8
- “Preparing to Deploy Workspace,” on page 10
Workspace System and Network Configuration Requirements

Consider your entire Workspace deployment, including how you integrate Workspace when you make decisions about hardware, resources, and network requirements.

Workspace Virtual Appliance Requirements

Ensure that the resources allocated to the Workspace virtual appliance meet the minimum requirements.

Table 2-1. VMware Workspace Portal Virtual Appliance (workspace-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>6GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>36GB</td>
</tr>
</tbody>
</table>

Additional notes:
- A PostgreSQL database is included in the workspace-va configuration, and you can use an external database server. For information about specific database versions and service pack configurations supported with Workspace, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- External database sizing information: 64GB for first 100,000 users. Add 20GB for each additional 10,000 users.
- Storage: 32GB

Network Configuration Requirements

The Workspace server must join the Windows domain if Kerberos, View, or ThinApp functions are enabled. In that case, the Workspace host name must be in the same domain as the Active Directory domain it is joining.

Table 2-2. Network Configuration Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS record and IP address</td>
<td>IP address and DNS record</td>
</tr>
<tr>
<td>Firewall port</td>
<td>Ensure that the inbound firewall port 443 is open for users outside the enterprise network to Workspace.</td>
</tr>
</tbody>
</table>

Port Requirements

Ports used in Workspace are described below. Your deployment might include only a subset of these. Here are two potential scenarios:

- To sync users and groups, the Workspace virtual appliance must connect to Active Directory.
- To sync with ThinApp, the Workspace virtual machine must join the Active Directory domain and connect to the ThinApp Repository share.

Table 2-3. Ports used by Workspace

<table>
<thead>
<tr>
<th>Port</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Load Balancer</td>
<td>Workspace-va</td>
<td>Hypertext Transport Protocol over SSL (HTTPS)</td>
</tr>
<tr>
<td>443</td>
<td>Workspace-va</td>
<td>Workspace-va 2, 3, etc.</td>
<td>Hypertext Transport Protocol over SSL (HTTPS)</td>
</tr>
</tbody>
</table>
Table 2-3. Ports used by Workspace (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Browsers</td>
<td>Workspace-va</td>
<td>Hypertext Transport Protocol over SSL (HTTPS)</td>
</tr>
<tr>
<td>8443</td>
<td>Browsers</td>
<td>Workspace-va</td>
<td>Administrator Port Hypertext Transport Protocol over SSL (HTTPS)</td>
</tr>
<tr>
<td>25</td>
<td>Workspace-va</td>
<td>SMTP</td>
<td>TCP port to relay outbound mail</td>
</tr>
<tr>
<td>389, 636, 3268, 3269</td>
<td>Workspace-va</td>
<td>Active Directory</td>
<td>Default values are shown. These ports are configurable.</td>
</tr>
<tr>
<td>5432</td>
<td>Workspace-va</td>
<td>Database</td>
<td>The PostgreSQL default port is 5432. The Oracle default port is 1521</td>
</tr>
<tr>
<td>389, 443</td>
<td>Workspace-va</td>
<td>View server</td>
<td>Access to View server</td>
</tr>
<tr>
<td>443</td>
<td>Workspace-va</td>
<td>VMware ThinApp repository</td>
<td>Access to ThinApp repository</td>
</tr>
<tr>
<td>5500</td>
<td>Workspace-va</td>
<td>RSA SecurID system</td>
<td>Default value is shown. This port is configurable.</td>
</tr>
<tr>
<td>53</td>
<td>Workspace-va</td>
<td>DNS server</td>
<td>TCP/UDP Every workspace-va must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22</td>
</tr>
<tr>
<td>88, 464, 135</td>
<td>Workspace-va</td>
<td>Domain controller</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>4666</td>
<td>Workspace-va</td>
<td>Workspace-va</td>
<td>Port and address is used by ehcache for peer discovery. The default address is 230.0.0.1.</td>
</tr>
<tr>
<td>40002, 40003</td>
<td>Workspace-va</td>
<td>Workspace-va</td>
<td>Ehcache RMI replication ports.</td>
</tr>
<tr>
<td>TCP: 9300-9400 UDP: 54328</td>
<td>Workspace-va</td>
<td>Workspace-va</td>
<td>Audit needs</td>
</tr>
</tbody>
</table>

Hardware Requirements for ESX Server

Ensure that the environment for the host and the vSphere instance that runs Workspace virtual appliance meets the minimum hardware requirements. Storage requirements vary per deployment based on the number of users.

**Note** You must turn on time sync at the ESX host level using an NTP server. Otherwise, a time drift will occur between the virtual appliances.

Table 2-4. Minimum 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>
Supported Web Browsers for Workspace

The Workspace administrator console is a Web-based application that is installed when you install Workspace. You can access and use the Workspace Admin Console from the following browsers.

- Internet Explorer 10 and 11 for Windows systems
- Google Chrome 34.0 or later for Windows and Mac systems
- Mozilla Firefox 28 or later for Windows and Mac systems
- Safari 6.1.3 and later for Mac systems

Preparing to Deploy Workspace

Before you deploy Workspace, you must prepare your environment. This preparation includes downloading the Workspace OVF file, creating DNS records and IP addresses.

Prerequisites

Before you begin to install Workspace complete the prerequisites tasks.

- One or more ESX servers to deploy Workspace virtual appliance.

  **NOTE** For information about supported vSphere and ESX server versions, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- VMware vSphere Client or vSphere Web Client is required to deploy the OVF file and access the deployed virtual appliance remotely to configure networking.

- Workspace OFV file from the VMware Web site.

- **Create DNS Records and IP Addresses** on page 11
  
  A DNS entry and a static IP address must be available for the Workspace appliance. Because each company administers their IP addresses and DNS records differently, before you begin your installation, request the DNS record and IP addresses to use.

- **Database Options with Workspace** on page 11
  
  Workspace can be set up with an internal or an external database. A vPostgres database is embedded in the Workspace appliance. The internal database is the default. You can select to connect to an external database when you configure the Workspace Setup wizard.

- **Connect to Active Directory** on page 12
  
  Workspace uses your existing Active Directory infrastructure for user authentication and management. To sync users and groups, the Workspace virtual appliance must connect to Active Directory.

- **Deployment Checklists** on page 12
  
  You can use Workspace deployment checklists to gather the necessary information to install Workspace.
Create DNS Records and IP Addresses

A DNS entry and a static IP address must be available for the Workspace appliance. Because each company administers their IP addresses and DNS records differently, before you begin your installation, request the DNS record and IP addresses to use.

(Optional) Reverse Lookup and IP Addresses

Configuring reverse lookup is optional in Workspace. When you implement reverse lookup, you must define a PTR record on the DNS server so the virtual appliance uses the correct network configuration.

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 2-5. 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-workspace-va.company.com</td>
<td>A</td>
<td>10.28.128.3</td>
</tr>
</tbody>
</table>

This example shows reverse DNS records and IP addresses.

Table 2-6. 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>128.28.10.in-addr.arpa.</td>
<td>IN</td>
<td>PTR my-workspace-va.company.com</td>
</tr>
</tbody>
</table>

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 the DNS name lookup.

Using a Unix/Linux-based DNS Server

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

Database Options with Workspace

Workspace can be set up with an internal or an external database. A vPostgres database is embedded in the Workspace appliance. The internal database is the default. You can select to connect to an external database when you configure the Workspace Setup wizard.

Using the embedded vPostgres database configuration is useful for small deployments and can be used by default. The internal database does not require any additional configuration outside of Workspace, but it is recommended that you configure your internal database for high availability. See KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1.

To use an external database, your database administrator must prepare an empty external database and schema before connecting to the external database. Licensed users can use an external vPostgres virtual appliance or Oracle database to set up a high availability external database environment. See “Connecting to an External Database,” on page 22.
**Connect to Active Directory**

Workspace uses your existing Active Directory infrastructure for user authentication and management. To sync users and groups, the Workspace virtual appliance must connect to Active Directory.

Your Active Directory must be accessible in the same LAN network as the Workspace virtual appliance. See “Establishing a Connection to Active Directory,” on page 32

**Deployment Checklists**

You can use Workspace deployment checklists to gather the necessary information to install Workspace.

Depending on your deployment, you might only need a portion of the network information for your virtual appliances when you create the static IP addresses in the DNS before the installation and during a Workspace installation.

**Information for Fully Qualified Domain Name**


**Table 2-7. 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>Workspace FQDN</td>
<td></td>
</tr>
</tbody>
</table>

**Network Information for Workspace Virtual Appliance**

**Table 2-8. Workspace 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 for this virtual appliance</td>
<td></td>
</tr>
<tr>
<td>Default Gateway address</td>
<td></td>
</tr>
<tr>
<td>Netmask or prefix</td>
<td></td>
</tr>
</tbody>
</table>

**Active Directory Domain Controller**

**Table 2-9. 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 (Must have privileges to join computers to the domain.)</td>
<td></td>
</tr>
</tbody>
</table>
### SSL Certificate (Optional)

**Table 2-10. 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 Workspace.

### Workspace License Key

**Table 2-11. Workspace License Key Information Checklist**

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>License key</td>
<td></td>
</tr>
</tbody>
</table>

*Note* The License key information is entered in the Workspace administration console in the Settings > Global Settings tab after the installation is complete.

### External Database

**Table 2-12. External Database Information Checklist**

<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>

### Workspace Passwords

**Table 2-13. Administration password used in Workspace**

<table>
<thead>
<tr>
<th>Information to Gather</th>
<th>List the Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace administrator account password</td>
<td></td>
</tr>
<tr>
<td>Virtual appliance root account password</td>
<td></td>
</tr>
<tr>
<td>Sshuser account password for remote log in</td>
<td></td>
</tr>
</tbody>
</table>
The tasks to deploy and set up Workspace using the vSphere Client or the vSphere Web Client includes deploying the OVF template, booting up the Workspace virtual appliance, and setting up Workspace.

After the Workspace virtual appliance is deployed, you use the Workspace Setup wizard to set up the Workspace environment.

Use your information in the deployment checklists to complete the installation. See “Deployment Checklists,” on page 12.

This chapter includes the following topics:

- “Install the Workspace OVF File,” on page 15
- “(Optional) Add IP Pools in Workspace,” on page 16
- “Configure Workspace Settings,” on page 17
- “Set Proxy Server Settings for Workspace,” on page 19
- “Workspace Administrative Services,” on page 20
- “Customer Experience Improvement Program,” on page 20

Install the Workspace OVF File

To start the Workspace installation, you must deploy the OVF file using the VMware vSphere Client or the vSphere Web Client. You can download and deploy the OVF file from a local file that is accessible to the vSphere Client or from a Web URL.

Prerequisites

- If using the vSphere Web Client, use either Firefox or Chrome browsers. Do not use Internet Explorer to deploy the OVF file.
- Download the Workspace OVF file.

Procedure

1. From the vSphere Client or the vSphere Web Client, select OVF template to deploy the Workspace OVF file.
2. In the Deploy OVF Template pages, enter the information specific to your deployment of Workspace.

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Browse to the OVF package location, or enter a specific URL.</td>
</tr>
<tr>
<td>OVF Template Details</td>
<td>Verify that you selected the correct version of Workspace.</td>
</tr>
</tbody>
</table>
### Page Description

**License**
Read the End User License Agreement and click Accept.

**Name and Location**
Enter the name to identify this Workspace virtual appliance. The name must be unique within the virtual machine folder. Names are case sensitive.

**Host / Cluster**
Select the host or cluster to run the deployed template.

**Resource Pool**
Select the resource pool.

**Storage**
Select the location to store the virtual machine files.

**Disk Format**
Select the disk format in which to store the Workspace files. For production environments, select the Thick Provision format. Use the Thin Provision format for evaluation and testing.

**Network Mapping**
Map the networks used in Workspace to networks in your inventory.

**Properties**

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>To deploy Workspace, leave the Application section check box unchecked.</td>
</tr>
<tr>
<td>In the Timezone setting field, select the correct time zone.</td>
</tr>
<tr>
<td>The Customer Experience Improvement Program is enabled by default. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements.</td>
</tr>
<tr>
<td>In the Host Name field, enter the host name to use. If this field is blank, reverse DNS is used to lookup the hostname.</td>
</tr>
<tr>
<td>To configure the static IP address for Workspace, enter the address for each of the following fields: Default Gateway, DNS, IP Address, and Netmask.</td>
</tr>
<tr>
<td>IMPORTANT</td>
</tr>
<tr>
<td>To configure DHCP, leave the address fields blank.</td>
</tr>
<tr>
<td>(Optional) After Workspace is installed, you can configure IP Pools. See &quot;(Optional) Add IP Pools in Workspace,&quot; on page 16.</td>
</tr>
</tbody>
</table>

**Ready to Complete**
Review the options you selected. If the information is correct, click Finish.

A progress bar displays. Depending on your network speed, this deployment can take several minutes.

3 When the deployment is complete, click Close in the progress bar.

4 Select the Workspace virtual appliance you just deployed and click Power on the virtual machine.

The Workspace virtual appliance is initialized. You can go to the Console tab to see the details. When the virtual appliance initialization is complete, the Console screen displays the Workspace version and URLs to log in to the Workspace Web interface and complete the set up of Workspace.

**What to do next**
Configure Workspace settings, including connecting to Active Directory and selecting users and groups to sync to Workspace.

**(Optional) Add IP Pools in Workspace**

Network configuration with IP Pool is optional in Workspace. You can manually add IP pools to Workspace after Workspace is installed. You edit the workspace-va virtual appliance networking properties to change the properties to dynamic properties and configure the netmask, gateway, and DNS settings.

IP Pools act like Dynamic Host Configuration Protocol (DHCP) servers to assign IP addresses from the pool to the workspace-va virtual appliance. To enable the Workspace appliance to use IP Pools, you need to edit appliance OVF properties.

**Prerequisites**
The workspace-va virtual appliance must be powered off to add the IP Pool settings.
Procedure

1. From the vSphere Client or the vSphere Web Client, right-click the virtual appliance that is being configured for IP Pools and select Edit Settings.

2. Click Properties in the Properties section of the page.

3. In the Advanced Property Configuration page, configure the following Key labels: vami.DNS.WorkspacePortal, vami.netmask0.WorkspacePortal, and vami.gateway.WorkspacePortal.
   a. On the Advanced Property Configuration page, select one of the Key labels and click Edit.
   b. On the Edit Property Settings page, next to the Type field, click Edit.
   c. On the Edit Property Type page, select Dynamic Property and select the appropriate value from the drop down menu for netmask, gateway and DNS Servers respectively.
   d. Click OK until all pages are closed.

4. Power on the virtual appliance.

The properties are configured to select from IP Pools.

Configure Workspace Settings

After the Workspace OVF is deployed and installed, you run the Workspace Setup wizard to configure the information to connect to your Active Directory; create an internal database or select an external database, if you are using one, and select users and groups to sync with Workspace.

Prerequisites

- Workspace virtual appliance powered on.
- List of passwords to use for the Workspace administrator, Workspace root account, and Workspace Sshuser account.
- If using an external database, the external database must be set up and the external database connection information available.
- Active Directory connection information.
- When multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the Workspace Directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members will be missing from the Domain Local group.
- List of the Active Directory user attributes you want to use as filters, and a list of the groups you want to add to Workspace.

Procedure

1. To configure Workspace after the OVF is deployed, go to the Workspace URL, https://workspacehostname.com.

   On the Welcome screen, click Continue.

2. On the Set Passwords page, create passwords for the following administrator accounts.
   - Appliance Administrator. Create the Workspace administrator password. The user name is admin and cannot be changed. This account was created during the initial installation of Workspace.
   - Root Account. A default VMware root password was used to set up Workspace. Create a new root password.
Sshuser Account. Create the password to use to remotely access the workspace-va virtual appliance.

Click Continue.

3 Select the database to use.

- If you are using an internal database, click Continue.
- If you are using an external database, select External Database and enter the external database connection information, user name, and password for the database server that you set up previously. To verify that Workspace can connect to the database, click Test the Connection.

Click Continue.

The connection to the database is configured and the database is initialized.

4 On the Directory page, enter your Active Directory information and click Verify.

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Type</td>
<td>Leave this as Active Directory.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this check box if you use SSL for your directory connection.</td>
</tr>
<tr>
<td>Use DNS Service Location</td>
<td>Select this check box if DNS service location is used for directory connection.</td>
</tr>
<tr>
<td>Server Host</td>
<td>Enter the Active Directory host address. Do not use non-ASCII characters when you enter the hostname.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the port number for the Active Directory host. For a single domain Active Directory, the default port is 389. When SSL is selected, the default port is 636.</td>
</tr>
<tr>
<td>Search Attribute</td>
<td>Enter the Active Directory account attribute that contains the user name. For most deployments, select sAMAccountName.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the DN that is the starting point for directory server searches. For example, OU-myunit,DC=mycompany,DC=com.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>Enter the bind DN, including common name (CN), of the Active Directory user account that has privileges to search for users. This user becomes an administrator for your Workspace deployment.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Enter the Active Directory password for the Bind DN account.</td>
</tr>
</tbody>
</table>

The Bind DN information is confirmed and the administrator's account is added as a user in Workspace.

Click Continue.

5 On the Map User Attributes page, select the attributes used in Active Directory that map to the Workspace Directory attributes.

If you plan to integrate with View, select Required next to the userPrincipal Name attribute. If you plan to integrate with Horizon DaaS, select Required next to the distinguishedName attribute. You can also do this later from the Connector Services Admin pages.

6 On the Select Users page, select user attributes from the drop-down menu to create filters to restrict the type of users that sync with Workspace. Click Continue.

7 Groups from Active Directory do not automatically sync to Workspace. On the Selected Groups page, click Add next to the group's DN description to add the group. Click Continue.

The Push to Workspace page displays information about the number of users and groups to sync to Workspace.

Click Push to Workspace to start the synchronization.
When the Setup is Complete page displays, click **Log in to Workspace** to log in to the admin console.

The Workspace sign in screen displays. Enter the Bind DN user name and password that you entered when you set up the connection to Active Directory. In the Workspace Admin Console, you can set up resources to use Workspace and assign users to those resources.

**NOTE** If a networking error occurs and the hostname cannot be uniquely resolved using reverse DNS, the configurator process stops. You must fix the networking problems and reboot the workspace-va virtual appliance. Then, you can continue the deployment process. The new network settings are not available until after you reboot the workspace-va virtual appliance.

**What to do next**

Log in to the Workspace admin console to customize a catalog of resources for your organization’s applications and enable user access to these resources.

Set up other resources, including View, ThinApp, Horizon DaaS, and Citrix-based applications. See the `Setting Up Resources in VMware Workspace Portal Guide`.

---

**Set Proxy Server Settings for Workspace**

The Workspace virtual appliance accesses the cloud application catalog and other Web services on the Internet. If your network configuration provides Internet access through an HTTP proxy, you must adjust your proxy settings on the Workspace appliance.

Enable your proxy to handle only Internet traffic. To ensure the proxy is set up correctly, set the parameter for internal traffic to `no-proxy` within the domain.

**Procedure**

1. From the vSphere Client, log in as the root user to the workspace-va virtual appliance.
2. Type `yast2`.
3. Select Network Services and select the Proxy page.
4. Enter the correct proxy URL in the HTTP field.
   
   `http://proxy.example.com:3128`

5. Enter the correct proxy URL in the HTTPS field.
   
   `https://proxy.example.com:3128`

6. Restart the Tomcat server on the workspace-va virtual machine to use the new proxy settings.
   
   `service horizon-workspace restart`

The cloud application catalog and other Web services are now available in Workspace.
Workspace Administrative Services

You manage Workspace users, groups, resources, authentication, sync setup, and the database connection from different Workspace administrative services.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Admin Console</td>
<td>In the Workspace Admin Console interface, you set up the resource catalog and administer your users and groups, entitlements, and reports. You log in as the administrator user role assigned from Active Directory. The URL to directly log in to the admin console is <a href="https://WorkspaceFQDN/SAAS/admin">https://WorkspaceFQDN/SAAS/admin</a>.</td>
</tr>
<tr>
<td>Connector Services Admin</td>
<td>In the Connector Services Admin pages, you configure the directory, set up your authentication adapters, and administer other enterprise integrations such as virtual desktops and remote apps. This includes setting up the integration to the View connection server, ThinApp repository, and Citrix published applications resources. From these pages you can also check directory sync status and alerts. You log in as the Workspace administrator, using the user name admin and the admin password you created when you set up Workspace. A link to the Connector Services Admin pages can be found at https://Workspace_FQDN.com:8443.</td>
</tr>
<tr>
<td>Appliance Configurator</td>
<td>In the Appliance Configurator pages, you can manage the Workspace database, update certificates, enable Syslog, change the Workspace and system passwords and manage other infrastructure functions. You log in as the Workspace administrator, using the user name admin and the admin password you created when you set up Workspace. A link to the Appliance Configurator pages can be found at https://Workspace_FQDN.com:8443. You can also access the Appliance Configurator pages from the Workspace Admin Console, Settings &gt; Virtual Appliance System Configuration page.</td>
</tr>
</tbody>
</table>

Customer Experience Improvement Program

When you install Workspace, you can choose to participate in VMware’s customer experience improvement program.

If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware’s response to user requirements. No data that identifies your organization is collected.

Before collecting the data, VMware makes anonymous all fields that contain information that is specific to your organization.

**Note** If your network configurations Internet access through HTTP proxy, in order to send this information, you must adjust your proxy settings on the workspace appliance. See “Set Proxy Server Settings for Workspace,” on page 19
Manage Workspace Appliance Configuration Settings

After you configure Workspace, you can go to the Appliance Configurator pages to update the current configuration and monitor system information for the virtual appliance.

You can update or change settings for your database, FQDN and SSL certificates, and more on the Appliance Configurator pages.

Table 4-1. Appliance Configurator Settings

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Setting Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Connection</td>
<td>The database connection setting, either Internal or External, is enabled. You can change the database type. When you select External Database, you enter</td>
</tr>
<tr>
<td></td>
<td>the external database URL, user name, and password. To set up an external database, see “Connecting to an External Database,” on page 22.</td>
</tr>
<tr>
<td>Install Certificate</td>
<td>On this page, you install a custom or self-signed certificate for Workspace and if Workspace is configured with a load balancer, you can install the load</td>
</tr>
<tr>
<td></td>
<td>balancer’s root certificate. The location of the Workspace root CA certificate is displayed on this page as well. See “Using SSL Certificates in Workspace,”</td>
</tr>
<tr>
<td></td>
<td>on page 26.</td>
</tr>
<tr>
<td>Workspace FQDN</td>
<td>The Workspace FQDN is displayed on this page. You can change it. Workspace FQDN is the URL that users use to access Workspace.</td>
</tr>
<tr>
<td>Configure Syslog</td>
<td>On this page, you can enable an external syslog server. Workspace logs are sent to this external server. See “Enable the Syslog Server,” on page 26.</td>
</tr>
<tr>
<td>Change Password</td>
<td>On this page, you can change the Workspace admin password.</td>
</tr>
<tr>
<td>System Security</td>
<td>On this page, you can change the root password for the Workspace appliance and the password used to log in remotely as an admin.</td>
</tr>
<tr>
<td>Log File Locations</td>
<td>A list of the Workspace log files and their directory locations is displayed on this page. You can bundle the log files into a tar zip file and download it</td>
</tr>
<tr>
<td></td>
<td>from this page. See “Log File Information,” on page 28.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Change Workspace Appliance Configuration Settings,” on page 22
- “Connecting to an External Database,” on page 22
- “Enable the Syslog Server,” on page 26
Change Workspace Appliance Configuration Settings

After you configure Workspace, you can go to the Appliance Configurator pages to update the current configuration and monitor system information for the virtual appliance.

Procedure

1. To access the appliance configurator pages, log on to the Workspace Admin Console.
2. Open the Settings tab and click **Virtual Appliance System Configuration**.
3. Log in to the Appliance Configurator with the Workspace administrator password.
4. Use the left navigation pane to select the page to view.

What to do next

Verify that the settings or updates you make are in effect.

Connecting to an External Database

An internal PostgreSQL database is embedded in the Workspace appliance. To use an external database with Workspace, your database administrator must prepare an empty, external, Oracle or PostgreSQL database and schema before connecting to the database in Workspace.

You can connect to the external database connection when you run the Workspace Setup wizard. You can also go to the Appliance Configurator Database Connection page to configure the connection to the external database.

Licensed users can use an external vPostgres virtual appliance or Oracle database to set up a high availability environment.

**NOTE** To configure your internal database for high availability, see KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1.

Configure an Oracle Database

During the Oracle installation, you must specify certain Oracle configurations for optimum performance with Workspace.

Prerequisites

Workspace requires Oracle quoted identifiers for the username and schema. Therefore, you must use double quotes when you create the Oracle `saas` username and schema.

Procedure

1. Specify the following settings when creating an Oracle database.
   a. Select the **General Purpose/Transaction Processing Database** configuration option.
   b. Click **Use Unicode > UTF8**.
   c. Use National Character Set.
2. Connect to the Oracle database after the installation is finished.
3. Log in to the Oracle database as the sys user.
4 Increase the process connections. Each additional workspace-va virtual machine requires a minimum of 300 process connections to function with Workspace. For example, if your environment has two workspace-va virtual machines, run the alter command as sys or system user.
   a Increase the process connections using the alter command.
      alter system set processes=600 scope=spfile
   b Restart the database.

5 Create a database trigger that all users can use.

Sample SQL to Create a Database Trigger

CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
  username VARCHAR2(30);
BEGIN
  username:=SYS_CONTEXT('USERENV','SESSION_USER');
  IF username = 'saas' THEN
    execute immediate 'alter session set NLS_SORT=BINARY_CI';
    execute immediate 'alter session set NLS_COMP=LINGUISTIC';
  END IF;
EXCEPTION
  WHEN OTHERS THEN
    NULL;
END;

6 Run the Oracle commands to create a new user schema.

Sample SQL to Create a New User

CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas";
GRANT CONNECT TO "saas";
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";

If you use a clustered Oracle database, see the VMware documentation regarding RAC set up.

Configure a PostgreSQL Database

During the PostgreSQL installation, you must specify certain PostgreSQL configurations for optimum performance with Workspace.

NOTE  Workspace does not currently support generic PostgreSQL.
Prerequisites

- Install and configure a supported version of VMware vFabric PostgreSQL as the external database server from one of the installation packages, such as OVA, OVF, or RPM, with the citext module installed. The citext module supports the CITEXT data type, a case insensitive text type. Verify that the VMware vFabric PostgreSQL version that you use is compatible with your version of Workspace. For information about supported VMware vFabric PostgreSQL versions, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- Install and configure the load balancing implementation.

- Verify that your environment meets these requirements:
  - The database server you use is PostgreSQL.
  - The database administrator username and password are available.
  - You must enter a username and password to create a user with authorization to the `saas` schema. This user is required when you connect a workspace-va virtual machine instance to the database.

  **Note** The workspace-va virtual machine uses the database name `saas`. During the initialization process, it drops and recreates any existing database named `saas`.

Procedure

1. Log in as the root user.
2. Edit the `postgresql.conf` file.
   
   For example, the VMware vFabric PostgreSQL database location is `/var/vmware/vpostgres/current/pgdata/`.
3. Increase the `max_connections` parameter. Each additional workspace-va virtual machine requires at least 300 connections to function properly with Workspace.
4. Set the `max_connections` parameter value to 600 for the two workspace-va virtual machines.
5. Restart the database.
6. Add a new line to the `postgresql.conf.auto` file that includes the `search_path='saas'` parameter.
7. Run the PostgreSQL commands to create a new PostgreSQL database schema.

**Table 4-2. Create a New Database Schema SQL**

<table>
<thead>
<tr>
<th>Sample SQL to Create a New Database Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATE ROLE horizon LOGIN</td>
</tr>
<tr>
<td>PASSWORD yourpassword</td>
</tr>
<tr>
<td>NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;</td>
</tr>
<tr>
<td>ALTER ROLE horizon</td>
</tr>
<tr>
<td>SET search_path = saas;</td>
</tr>
<tr>
<td>CREATE DATABASE saas</td>
</tr>
<tr>
<td>WITH OWNER = postgres</td>
</tr>
<tr>
<td>ENCODING = 'UTF8'</td>
</tr>
<tr>
<td>TABLESPACE = pg_default</td>
</tr>
<tr>
<td>CONNECTION LIMIT = -1;</td>
</tr>
<tr>
<td>GRANT CONNECT, TEMPORARY ON DATABASE saas TO public;</td>
</tr>
<tr>
<td>GRANT ALL ON DATABASE saas TO postgres;</td>
</tr>
<tr>
<td>GRANT ALL ON DATABASE saas TO horizon;</td>
</tr>
<tr>
<td>\connect saas;</td>
</tr>
<tr>
<td>CREATE SCHEMA saas AUTHORIZATION horizon;</td>
</tr>
<tr>
<td>CREATE EXTENSION citext SCHEMA saas;</td>
</tr>
</tbody>
</table>
Transfer Data from the Internal Database

If your deployment uses an internal database and you plan to switch to an external database, you can extract the existing data from the database and add it to a new external database.

Prerequisites

Prepare the external database server. See “Configure a PostgreSQL Database,” on page 23.

Procedure

1. Log in as the root user.
2. Go to the /opt/vmware/vpostgres/current/bin directory.
3. Run the ./pg_dump -U postgres -w --clean -f /tmp/db_dump.data saas command.
4. Copy the db_dump.data file to the newly prepared external database server.
   
   scp /tmp/db_dump.data

5. Log in as the root user on the external database server.
6. Go to the /opt/vmware/vpostgres/current/bin directory.
7. Run the db_dump.data command.
   
   ./psql -U postgres -w -d saas -f /tmp/db_dump.data

   You might see DROP and ALTER commands while the db_dump.data command runs.

Add an External Database to the Workspace Appliance

After you run the Workspace Setup wizard, you can configure Workspace to use a different database.

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

Prerequisites

- Install and configure VMware vFabric PostgreSQL or Oracle as the external database server. For information on configuring a PostgreSQL database for Workspace, see “Configure a PostgreSQL Database,” on page 23. For information about specific Oracle versions that are supported by Workspace, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- Transfer data from the internal database, if you had been using one.

Procedure

1. In the Workspace Admin Console click Settings and select VA Configuration.
2. Click Manage Configuration.
3. Log in to Appliance Configurator with the Workspace administrator password.
4. On the Database Connection Setup page, select External Database as the database type.
5 Enter information about the database connection.
   a Type the JDBC URL of the database server.
      PostgreSQL jdbc:postgresql://IP_address/saas?stringtype=unspecified
      Oracle jdbc:oracle:thin:@IP_address:port/sid
   b Type the name of the user with read and write privileges to the database.
      PostgreSQL horizon
      Oracle “saas”
   c Type the password for the user you created when you configured your Oracle or PostgreSQL database.
6 Click Test Connection to verify and save the information.

Enable the Syslog Server
Workspace exports application-level events to the external syslog server. Operating system events are not exported.

Since most companies do not have unlimited disk space, Workspace does not save the complete logging history for each virtual machine. If you want to save more history or create a centralized location for your logging history, you can set up an external syslog server.

If you do not configure a syslog server during the initial configuration, you can configure it later from the Syslog Configuration page in the Appliance Configurator.

Prerequisites
Set up an external syslog server. You can use any of the standard syslog servers available. Several syslog servers include advanced search capabilities.

Procedure
1 In the Workspace Admin Console, click Settings and select VA Configuration.
2 Click Manage Configuration.
3 Log in to the Appliance Configurator.
4 Click Configure Syslog in the left navigation pane.
5 Click Enable.
6 Enter the IP address or the FQDN of the server where you want to store the logs.
7 Click Save.
Workspace sends a copy of your logs to the syslog server.

Using SSL Certificates in Workspace
When the Workspace appliance is installed, a default SSL server certificate is automatically generated. You can use this self-signed certificate to test Workspace. VMware strongly recommends that you generate and install commercial SSL certificates when Workspace is used in a production environment.

A certificate of authority (CA) is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate.
If you deploy Workspace with the self-signed SSL certificate, the Workspace root CA certificate must be available as a trusted CA for any client who accesses Workspace. The clients can include end user machines, load balancers, proxies, and so on. You can download the Workspace root CA from https://workspacehostname.com/horizon_workspace_rootca.pem.

You can install the Workspace certificate of authority from the Appliance Configurator > Install Certificate page. You can also add the load balancer’s root CA certificate on this page as well. See “Apply Workspace Root Certificate to the Load Balancer,” on page 41.

**Apply Public Certificate Authority to Workspace**

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

You can add new certificates to Workspace.

**Note** If Workspace FQDN points to a load balancer, the SSL certificate is applied to the load balancer.

**Prerequisites**

Generate a Certificate Signing Request (CSR) and obtain a valid, signed certificate from a CA. If your organization provides SSL certificates that are signed by a CA, you can use these certificates.

**Procedure**

1. To apply the certificate to Workspace, in the Workspace Admin Console, click Settings and select VA Configuration.
2. Click Manage Configuration.
3. Log in to the Appliance Configurator with the Workspace administrator password.
4. Select Install Certificate.
5. In the Terminate SSL on Workspace appliance tab, paste the complete certificate chain and private key. Ensure that the certificate includes the Workspace FQDN hostname.
6. Save the SSL certificate.

**What to do next**

Verify that users can log in successfully.

**Workspace FQDN and SSL Certificates**

When you apply the certificate in the admin console Settings > VA Configuration > Manage Configuration page make sure that you include the entire certificate chain.

The SSL certificate works with Workspace only if you include the entire certificate chain. For each certificate copy everything between and including the lines that include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

You must copy the certificate chain order exactly, SSL Certificate, Intermediate CA Certificates, Root CA Certificate.

**Certificate Chain Example**

-----BEGIN CERTIFICATE-----

SSL Cert - Workspace SSL Cert

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
Certificate Chain Example

Intermediate/Issuing CA Cert

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

Root CA Cert

-----END CERTIFICATE-----

Log File Information

Workspace log files can help you debug and troubleshoot. The log files listed below are a common starting point. Additional logs can be found in the /opt/vmware/horizon/workspace/logs directory.

Table 4-3. Log File Information

<table>
<thead>
<tr>
<th>Component</th>
<th>Location of Log File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Service Logs</td>
<td>/opt/vmware/horizon/workspace/logs/horizon.log</td>
<td>Information about activity on the Workspace application, such as entitlements, users, and groups.</td>
</tr>
<tr>
<td>Configurator Logs</td>
<td>/opt/vmware/horizon/workspace/logs/configurator.log</td>
<td>Requests that the Configurator receives from the REST client and the Web interface.</td>
</tr>
<tr>
<td>Connector Logs</td>
<td>/opt/vmware/horizon/workspace/logs/connector.log</td>
<td>A record of each request received from the Web interface. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.</td>
</tr>
<tr>
<td>Update Logs</td>
<td>/opt/vmware/var/log/update.log /opt/vmware/var/log/vami</td>
<td>A record of output messages related to update requests during an upgrade of Workspace. The files in the /opt/vmware/var/log/vami directory are useful for troubleshooting. You can find these files on all virtual machines after an upgrade.</td>
</tr>
<tr>
<td>Apache Tomcat Logs</td>
<td>/opt/vmware/horizon/workspace/logs/catalina.log</td>
<td>Apache Tomcat records of messages that are not recorded in other log files.</td>
</tr>
</tbody>
</table>

Collect Log Information

During testing or troubleshooting, the logs can give feedback about the activity and performance of the virtual appliance as well as information about any problems that occur.

You collect the logs from each workspace-va appliance that is in your environment.

Procedure

1. Log in to the Appliance Configurator
2. Open the Log File Locations page and click Prepare log bundle.
   The information is collected into a tar.gz file that can be downloaded.
3. Download the prepared bundle.

What to do next

To collect all logs, do this on each workspace-va appliance.
After you configure Workspace, you can go to the Connector Services Admin pages to manage the Workspace directory, enable or disable authentication adapters, change Active Directory user attributes, manage Active Directory groups, manually sync the directory, and set up resources used in Workspace, including View pools, Citrix-based resources, and ThinApp packages.

Table 5-1. Settings Managed from Connector Services Admin Pages

<table>
<thead>
<tr>
<th>Page Name</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>About page displays general information about Workspace, including the version number.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configuration page is not applicable at this time for the Workspace appliance.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Enable Join Domain and complete the information on this page to use View or ThinApp resources in Workspace and to provide single sign-on to the Web interface using Kerberos Windows authentication. You must join the same Active Directory as the resource uses. The Active Directory information that you provide on this page is for the user who has permission to join machines to the Active Directory domain. See the appropriate chapters in the Setting Up Resources in VMware Workspace Portal Guide for information about configuring these resources.</td>
</tr>
<tr>
<td>Directory Authentication Method</td>
<td>Enable Windows Authentication to configure a multi-domain, single forest or a trusted multi-forest Active Directory environment with Workspace. See “Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory,” on page 34.</td>
</tr>
<tr>
<td>Identity Provider</td>
<td>Identity Provider page shows the identity provider instance that you use to authenticate users with Active Directory within the enterprise network.</td>
</tr>
<tr>
<td>Auth Adapters</td>
<td>Auth Adapters page shows the authentication methods available in Workspace, including password authentication, Kerberos authentication, and SecureID. You can enable and configure the authentication information. See Chapter 9, “Setting Up User Authentication,” on page 53.</td>
</tr>
<tr>
<td>Directory</td>
<td>View and manage the Active Directory connection information from this page. See “Establishing a Connection to Active Directory,” on page 32.</td>
</tr>
<tr>
<td>Map User Attributes</td>
<td>The mapping of Active Directory attributes to Workspace Directory attributes is displayed on this page. If you configure View resources, the userPrincipalName attribute must be checked on this page.</td>
</tr>
<tr>
<td>Directory Sync</td>
<td>Change the sync schedule. When Workspace was installed, the default schedule was set to sync the directories once a day at 11:55 PM. You can also edit the directory sync rules to select users and groups from Active Directory.</td>
</tr>
<tr>
<td>Page Name</td>
<td>Setting</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sync Safeguards</td>
<td>Set sync safeguards to prevent unintended changes to the users and groups that are added to Workspace as a result of a directory synchronization. For example, you can set a limit on the maximum percentage of users that can be deleted at once. If any of your trigger conditions are met, the directory synchronization does not take place, requiring you to manually intervene. Default conditions are enabled, but you can adjust them to be more or less protective. You can view the safeguard alerts from the Troubleshooting tab.</td>
</tr>
<tr>
<td>Horizon DaaS Resources</td>
<td>Enable and configure Horizon DaaS as a Resource. You must enable the distinguishedName attribute on the Map User Attributes page.</td>
</tr>
<tr>
<td>View Pools</td>
<td>Enable and configure View pools as a resource in Workspace. First, you must first configure the domain connection on the Join Domain page and enable the userPrincipalName attribute on the Map User Attributes page. See the appropriate chapters in the Setting Up Resources in VMware Workspace Portal Guide for information about configuring this resource.</td>
</tr>
<tr>
<td>Published App - Citrix</td>
<td>Enable and configure the Citrix-based applications as a resource in Workspace. See the appropriate chapters in the Setting Up Resources in VMware Workspace Portal Guide for information about configuring this resource.</td>
</tr>
<tr>
<td>Packaged Apps - ThinApp</td>
<td>Enable and configure ThinApp packages as a resource in Workspace. First, you must first configure the domain on the Join Domain connection page. See the appropriate chapters in the Setting Up Resources in VMware Workspace Portal Guide for information about configuring this resource.</td>
</tr>
</tbody>
</table>

**Procedure**

2. Log in to the Connector Services Admin with the Workspace admin password.
3. Use the left navigation pane to select the page to view.

**What to do next**

Verify that the new settings or updates are available.
The Active Directory environment can consist of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests. After you customize Active Directory, you update your configuration information in Workspace.

- **Integrating Workspace with Active Directory** on page 31
  You can integrate Workspace with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

- **Establishing a Connection to Active Directory** on page 32
  Workspace uses your existing Active Directory infrastructure for user authentication and management. You configure the Active Directory information when Workspace is installed and setup.

- **Establishing a Connection to Multi-Domains or Trusted Multi-Forest Domains in Active Directory** on page 34
  When Workspace is installed, a single Active Directory domain is configured and synchronized to Workspace. You must enable Windows Authentication to configure a multi-domain, single forest, or a trusted multi-forest Active Directory environment with Workspace.

### Integrating Workspace with Active Directory

You can integrate Workspace with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

When you install Workspace, connect Workspace to a single Active Directory domain. If you have multiple domains, you can integrate Workspace into your existing Active Directory environment from the Connector Services Admin pages after Workspace is installed.

### Single Active Directory Domain Environment

A single Active Directory deployment allows you to sync users and groups from a single Active Directory domain. To install Workspace in a Single Active Directory domain environment, see “Establishing a Connection to Active Directory,” on page 32.

### Multi-Domain, Single Forest Active Directory Environment

A multi-domain, single forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains within a single forest.

You enable Windows Authentication as a directory authentication method to configure a multi-domain, single forest Active Directory environment for Workspace.
To install Workspace in a multi-domain, single forest Active Directory environment, see “Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory,” on page 34.

Multi-Forest Active Directory Environment with Trust Relationships
A multi-forest Active Directory deployment with trust relationships allows you to sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains.

You enable Windows Authentication as a directory authentication method to configure a multi-forest Active Directory environment for Workspace.

To install Workspace in a trusted multi-forest Active Directory environment, see “Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory,” on page 34.

Multi-Forest Active Directory Environment Without Trust Relationships
A multi-forest Active Directory deployment without trust relationships allows you to sync users and groups from multiple Active Directory domains across forests without a trust relationship between the domains. This deployment requires use of Workspace User Store technology.

Contact VMware Professional Services to learn more about a multi-forest Active Directory deployment without trust relationships.

Establishing a Connection to Active Directory
Workspace uses your existing Active Directory infrastructure for user authentication and management. You configure the Active Directory information when Workspace is installed and setup.

Required Active Directory Information
Workspace uses the following Active Directory information to verify end user’s credentials when they sign in. You configure this information when you install Workspace.

<table>
<thead>
<tr>
<th>Server host</th>
<th>Active Directory host address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SSL</td>
<td>If you use SSL for your directory connection, configure this setting and add the certificate to the certificate field.</td>
</tr>
<tr>
<td>Use DNS Service Location</td>
<td>If you do not know the sever host name and port number, check Use DNS Service Location. Workspace uses DNS Service Location records to locate the Active Directory domain.</td>
</tr>
<tr>
<td>Server port</td>
<td>The port number of the Active Directory host. The default port for LDAP is 389. The default port for LDAP over SSL is 636.</td>
</tr>
<tr>
<td>Search attribute</td>
<td>The Active Directory account attribute that contains the user name. Most Active Directory Domain Service deployments use \texttt{samAccountName}.</td>
</tr>
<tr>
<td>Base distinguished name (DN)</td>
<td>The Base DN which is 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 add groups.</td>
</tr>
</tbody>
</table>
Bound DN

The Bind DN of the Active Directory user account that has privileges to search for users. 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 DN attribute defined in Active Directory. This user becomes the administrator for your Workspace deployment. You can promote other Active Directory users to the administrator role from the Workspace Admin Console.

Note: When multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the Workspace Directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members will be missing from the Domain Local group.

The following examples are best practices when selecting the Base DN and Bind DN:

- **Base DN:** `dc=example, dc=com`. 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.

Bind password

The Active Directory password for the Bind DN account.

### Selecting Active Directory Users and Groups to Sync to Workspace

When you configure the Active Directory connection in Workspace, you set up a base DN as the point from where to search for users. This search includes all users. To restrict the number of users that sync with Workspace, you can create user-attribute-based search filters to exclude specific types of users.

The base DN you set up is used to search for users. To include groups in your search, you can create filters to add specific types of groups to the Workspace directory.

Before creating filters and adding groups in the Workspace, work with your Active Directory administrator to understand the structure of your Active Directory to select the correct users and groups to synchronize.

### Using Filters to Add Users and Groups

You select the users and groups you want to sync to Workspace. The first sync occurs during the initial Workspace setup. You can make changes at any time from the Connector Services Admin pages.

**Procedure**

1. Log in to Connector Services Admin.
2. Select the Directory Sync page and click **Edit Directory Sync Rules**.
3. From the Select Users page, the base DN for Users text box displays the existing base DN. To add another base DN, click **Add another**.
4. From the **Apply Filters to Exclude Users** drop-down menu, to exclude certain user types, select the user attribute to filter by, select the query rule, and add the value.
5. Click **Add another** to add additional filters.
6. Click **Next** to add groups.
7. To find specific groups in the Selected Groups list, in the **Group Name Filter** text box, enter the group name you want to add.
8. Click **Add** next to the group names you want to include.
9. Click **Next**.

   The Push to Workspace page displays the number of users and groups you selected to add to Workspace.

10. Click **Save and Continue**.

   Active Directory is synchronized with Workspace.
Establishing a Connection to Multi-Domains or Trusted Multi-Forest Domains in Active Directory

When Workspace is installed, a single Active Directory domain is configured and synchronized to Workspace. You must enable Windows Authentication to configure a multi-domain, single forest, or a trusted multi-forest Active Directory environment with Workspace.

**Note** When you enable Windows Authentication, the Directory configuration is changed to enable the DNS Service Location field. If you want to override the built-in SRV lookup, see “Create a Domain Host Lookup File to Override DNS Service Location (SRV) Lookup,” on page 37.

To configure Workspace to provide user interactive Windows Authentication, you must join Workspace to the Active Directory domain, enable Windows Authentication in Workspace, and sync the users and groups with Workspace.

Configure Windows Authentication for Multi-Domains or Trusted Multi-Forest Active Directory

To configure Workspace to provide interactive Windows Authentication for multi-domains or trusted multi-forest Active Directory domains, you must join Workspace to the Active Directory domain, enable Windows authentication, and sync users and groups with Workspace.

**Procedure**

1. **Join Workspace to Active Directory Domain with Multi-Domains or Trusted Multi-Forest Domains** on page 35
   To configure a multi-domain, single forest, or a trusted multi-forest Active Directory using the interactive Windows authentication method, you must join the Workspace appliance to the Active Directory domain.

2. **Enable Access to Windows Authentication for a Trusted Multi-Forest Active Directory Domain** on page 35
   To configure Workspace to provide user interactive Windows authentication, after you join Workspace to the trusted multi-forest active directory domain, you must enable Windows authentication in Workspace.

3. **Select Users and Groups to Sync to Workspace** on page 36
   Before you sync users and groups from Active Directory domains to Workspace, restrict the type of users to add to Workspace and select the groups that should be added from the different domains.

4. **Add Multiple Domain Names to the Sign In Page** on page 37
   After Windows Authentication for multiple Active Directory domains is configured, you enable Password Adapter to add the domains to the user signin page. Users can select their domain from the drop-down list when signing in to Workspace.

5. **Create a Domain Host Lookup File to Override DNS Service Location (SRV) Lookup** on page 37
   When you enable Windows Authentication, the Directory configuration is changed to enable the DNS Service Location field. To override the built-in SRV lookup, you can create a file called domain krb.properties and add the domain to host values that take precedence over SRV lookup.
Join Workspace to Active Directory Domain with Multi-Domains or Trusted Multi-Forest Domains

To configure a multi-domain, single forest, or a trusted multi-forest Active Directory using the interactive Windows authentication method, you must join the Workspace appliance to the Active Directory domain.

Prerequisites

- Verify that you have the Active Directory domain name, username, and password of an account in that Active Directory that has the rights to join the domain.

Procedure

1. Log in to Connector Services Admin.
2. Select the Join Domain page.
3. In the AD Domain text box, enter the fully qualified domain name of the Active Directory.
4. In the AD Username text box, enter the user name of an account in the Active Directory that has permissions to join systems to that Active Directory domain.
5. In the AD Password text box, enter the password associated with the AD Username. This password is not stored by Workspace.
6. Click Join Domain.

The Join Domain page is refreshed and displays a message that you are currently joined to the domain.

What to do next

Enable Windows Authentication to access the multi-domain, single forest, or a trusted multi-forest Active Directory domain.

Enable Access to Windows Authentication for a Trusted Multi-Forest Active Directory Domain

To configure Workspace to provide user interactive Windows authentication, after you join Workspace to the trusted multi-forest active directory domain, you must enable Windows authentication in Workspace.

Prerequisites

Make sure that you joined Workspace to the Active Directory domain.

Procedure

1. Log in to Connector Services Admin.
3. Click Enable Windows Authentication.
4. Click Save.

The Windows authentication method is enabled. Workspace updates the Directory page and the Auth-Adapters, PasswordIdpAdapter page to add a check mark to the Use DNS Service Location field and to change the Bind DN account format to sAMAccountName.

After Active Directory syncs the domains with Workspace, a list of domains are added to the Directory Authentication Method page. When Password Adapter authentication is enabled in the Auth Adapters, PasswordIdpAdapter page, the domain names are added to the user sign-in page.
What to do next

If multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the Workspace Directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members will be missing from the Domain Local group.

Select users and groups from the Active Directory domains and sync Active Directory to Workspace.

Select Users and Groups to Sync to Workspace

Before you sync users and groups from Active Directory domains to Workspace, restrict the type of users to add to Workspace and select the groups that should be added from the different domains.

Prerequisites

Create a list of the Active Directory user attributes you want to use as filters and create a list of groups you want to add to Workspace.

Procedure

1. Log in to Connector Services Admin.
3. In the Select Users page, the base DN for Users text boxes display the existing base DN configuration. To add another base DN, click Add another.
4. In the Apply Filters to Exclude Users drop-down menu, to exclude certain user types, select the user attribute to filter by, select the query rule, and add the value.
5. Click Add another, to add additional filters.
6. Click Next to add groups.
7. Groups that are created in your Active Directory are listed on the Selected Groups page. To find specific groups, in the Group Name Filter text field enter the group name you want to add.
8. Click Add next to the group names you want to include.
9. Click Next.
10. Click Save and Continue.

The users and groups in the Active Directory domains are synchronized with Workspace. The domain names are added to the Directory Authentication Method page as they are synchronized to Workspace.

What to do next

Enable the password adapter feature so that the Active Directory domain names are added to the user signin page. Users select their domain when they sign in.
Add Multiple Domain Names to the Sign In Page

After Windows Authentication for multiple Active Directory domains is configured, you enable Password Adapter to add the domains to the user signin page. Users can select their domain from the drop-down list when signing in to Workspace.

Prerequisites

The Windows authentication method must be enabled in Workspace to establish the connection to multi-domains or trusted multi-forest domains.

The Active Directory domains are synchronized to Workspace.

Procedure

1. Log in to Connector Services Admin.
2. Open the Auth Adapters page and in the PassswordldpAdapter row, click Edit.
3. Select Enable Password Adapter.
4. Click Save.

The domain names are added to a drop-down list on the user signin page.

Create a Domain Host Lookup File to Override DNS Service Location (SRV) Lookup

When you enable Windows Authentication, the Directory configuration is changed to enable the DNS Service Location field. To override the built-in SRV lookup, you can create a file called domain_krb.properties and add the domain to host values that take precedence over SRV lookup.

Procedure

1. From the workspace-va command line, log in as the user with root privileges.
2. Change directories to /usr/local/horizon/conf and create a file called domain_krb.properties.
3. Edit the domain_krb.properties file to add the list of the domain to host values. Add the information as <AD Domain>=<host:port>, <host2:port2>, <host2:port2>.
   For example, enter the list as example.com=examplehost.com:636, examplehost2.example.com:389
4. Change the owner of the domain_krb.properties file to horizon and group to www. Enter chown horizon:www /usr/local/horizon/conf/domain_krb.properties.
5. Restart Workspace. Enter service horizon-workspace restart.
Advanced Configuration for VMware Workspace Portal Appliance

After you complete the basic Workspace installation, you might need to complete other configuration tasks such as configuring a load balancer to enable external access to Workspace.

The Workspace architecture diagram demonstrates what you can build within the Workspace environment. See Chapter 2, “Preparing to Install VMware Workspace Portal,” on page 7 for a typical deployment.

Using a Load Balancer to Enable External Access to Workspace

During deployment, Workspace is set up inside the internal network. If you want to provide access to Workspace for users connecting from outside networks, you must install a load balancer, such as Apache, nginx, F5, and so on, in the DMZ.

If you do not use a load balancer, you cannot expand the number of Workspace virtual machines in the future. You might need to add more Workspace virtual machines to provide redundancy and load balancing. The following diagram shows the basic deployment architecture you can use to enable external access.
Specify Workspace FQDN during Deployment

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

The Workspace virtual machine 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.

Settings on the Load Balancer to Configure for Workspace

Load Balancer settings to configure for Workspace include enabling X-Forwarded-For headers, setting the Load Balancer timeout correctly, and enabling sticky sessions. In addition, the SSL Trust must be configured between Workspace and the Load Balancer.

- X-Forwarded-For Headers. You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.
- Load Balancer Timeout. For Workspace to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see this error, “502 error: The service is currently unavailable.”
Enabling Sticky Session on the Load Balancer to the Workspace. Ensure that you enable sticky session on the load balancer to the workspace-va servers if your deployment uses multiple workspace servers. Sticky session improves Web interface performance. If sticky session is not enabled, some functions might fail.

**Apply Workspace Root Certificate to the Load Balancer**

When Workspace is configured with a load balancer, you must establish SSL trust between the load balancer and Workspace. The Workspace root certificate must be copied to the load balancer. The certificate can be downloaded from the Appliance Configurator, Install Certificate page.

If 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 Workspace virtual machine, you must copy the Workspace root CA certificate to the load balancer as a trusted root certificate.

**Procedure**

1. In the Workspace Admin Console, click **Settings** and select **VA Configuration**.
2. Click **Manage Configuration**.
3. Log in to the Appliance Configurator with the Workspace administrator password.
4. Select **Install Certificate**.
5. Select the Terminate SSL on a Load Balance tab and in the Appliance Root CA Certificate field, click the link `https://workspacehostname/horizon_workspace_rootca.pem`.
   
   The Workspace root certificate displays.
6. Copy and paste the root certificate into the correct location on each of your load balancers. Refer to the documentation provided by your load balancer vendor.

**What to do next**

Copy and paste the Load Balancer root certificate into the Workspace Appliance Configurator Install Certificate, Terminate SSL on a Load Balancer page.
Configuring Redundancy

You can set up the connector virtual appliance for failover and redundancy by adding multiple connector virtual appliances in a cluster. If one of the virtual appliances becomes unavailable for any reason, Workspace is still available.

This chapter includes the following topics:

- “Configuring Redundancy/Failover for Workspace Appliance in the Same Data Center,” on page 43
- “Deploying Workspace in Secondary Data Center with Active-Active Read-Only Capability,” on page 46

Configuring Redundancy/Failover for Workspace Appliance in the Same Data Center

Enterprises achieve failover and redundancy in Workspace by adding multiple workspace-va virtual appliances in the Workspace cluster in a data center. If one of the virtual appliances shuts down for any reason, Workspace is still available.

To set up failover in Workspace cluster, you clone the workspace-va appliance. Cloning the appliance creates a duplicate of the appliance with the same configuration as the original. You can customize the cloned appliance to change the appliance name, network settings, and other properties as required.

The cloned Workspace appliance IP address must follow the same guidelines as the IP address of the original virtual appliance. The IP address must resolve to a valid hostname using forward and reverse DNS.

All nodes in the cluster are identical and nearly stateless copies of each other. Syncing to Active Directory and to resources that are configured in Workspace, such as View or ThinApp, is disabled on the cloned virtual appliance.

Create Multiple Workspace Virtual Appliances

For failover, your enterprise can clone the workspace-va virtual appliance to create multiple virtual appliances of the same type to distribute traffic and eliminate potential downtime.

Using multiple workspace-va virtual appliance improves availability, load balances requests to Workspace, and decreases response times to the end user.

Prerequisites

- The virtual appliance must be configured behind a load balancer. Make sure that the load balancer port is 443. Do not use 8443 as this port number is the Workspace administrative port and is unique to each virtual appliance.
Either an external database configured as described in “Connecting to an External Database,” on page 22 or an internal database configured as described in VMware KB 2094258, Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1, must be set up in order to add additional workspace-va virtual appliances.

VMware vSphere Client or vSphere Web Client is required to clone the virtual appliance and to access the cloned virtual appliance to configure networking.

Add an IP Address to Cloned Virtual Appliance Properties on page 45
You must assign a new IP address before you power on a cloned virtual appliance. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

Enable SecurID Authentication on page 45
In many cases, enterprises enable RSA SecurID-based authentication for their end users who connect from external networks. After you cloned the workspace-va virtual appliance, if you use RSA SecureID authentication, you must add the cloned Workspace host name and IP address to the RSA server and create a new agent on the cloned virtual appliance.

Enable Kerberos Authentication on page 45
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 Workspace without typing a username and password. After you clone the Connector appliance, if you use Kerberos Authentication, you must re-enable join the domain and Kerberos authentication on the cloned virtual machine.

Procedure
1. Power off the workspace-va virtual appliance that is being cloned.
2. Right-click the virtual appliance that is being cloned, and click Next.
3. Enter the name you want to use to identify this cloned virtual appliance. The name must be unique within the virtual machine folder or data center.
4. Select the host or cluster on which to run the cloned virtual appliance.
5. Select the resource pool in which to run the virtual appliance and click Next.
6. Select the datastore location where you want to store the virtual appliance files.
7. Select the format for the virtual appliance’s disks. This should be the same format as the source. Click Next.
8. Select Do not customize as the guest operating system option.
9. Review the options you selected. If the information is correct, click Finish.

The cloned virtual appliance is deployed. You cannot use or edit the virtual appliance until the cloning is complete.

What to do next
Assign an IP address to the cloned workspace-va before you power up the machine and add the new virtual appliance to the load balancer.
Add an IP Address to Cloned Virtual Appliance Properties

You must assign a new IP address before you power on a cloned virtual appliance. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

Procedure

1. From the vSphere Client or the vSphere Web Client, select the virtual appliance that was cloned.
2. Select Summary > Commands, click Edit.
3. Select Options and in the Options Settings list, select Properties.
4. Change the IP address in the IP Address field.
5. If the IP address is not in the reverse DNS, add the host name in the HostName text box.
6. Click OK.
7. Power on the cloned machine.

What to do next

Enable the authentication methods configured for Workspace on each of the cloned virtual appliances.

Enable SecurID Authentication

In many cases, enterprises enable RSA SecurID-based authentication for their end users who connect from external networks. After you cloned the workspace-va virtual appliance, if you use RSA SecureID authentication, you must add the cloned Workspace host name and IP address to the RSA server and create a new agent on the cloned virtual appliance.

Prerequisites

Create a new RSA Server authentication agent with the cloned Workspace appliance host name and IP address. See “Prepare the RSA SecurID Server for the Connector Services Admin,” on page 54.

Procedure

1. Log in to Connector Services Admin.
2. Click Auth Adapters.
3. In the Secure ID row, click Edit.

Enable 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 Workspace without typing a username and password. After you clone the Connector appliance, if you use Kerberos Authentication, you must re-enable join the domain and Kerberos authentication on the cloned virtual machine.

Procedure

1. Log in to Connector Services Admin.
2. In the Join Domain page, enable Join Domain.
   a. In the AD Password text box, enter the password of the user in Active Directory that has rights to join the domain.
   b. Click Join Domain.
c Click Auth Adapters.

d Select KerberosIdAdapter and on the page that opens, select Enable Windows Authentication.

e Click Save.

3 On the Connector Services Admin page, select Auth Adapters and click Edit in the KerberosIdpAdapter row.

a The Name field shows KerberosIdpAdapter as the name. You can change this.

b In the Directory UID Attribute text box, enter the account attribute that contains the user name.

c Check Enable Windows Authentication to extend authentication interactions between users’ browsers and Workspace.

d Check Enable NTLM to enable NT LAN Manager (NTLM) protocol-based authentication.

e Check Enable Redirect if round-robin DNS and load balancers do not have Kerberos support. Authentication requests are redirected to Redirect Host Name. If this is checked, enter the redirect host name in Redirect Host Name text box.

f Click Save.

Deploying Workspace in Secondary Data Center with Active-Active Read-Only Capability

Deploy Workspace in a secondary data center to provide failover capabilities if the primary Workspace data center becomes unavailable.

Beginning with Workspace 2.1.1, two options to provide failover capabilities to a secondary data center are available. The existing method of active - hot standby allows continuity of the entire Workspace service with minimal downtime as the secondary data center is made primary. The method available beginning with Workspace 2.1.1 enables a secondary data center to be powered on and active with read-only access, which eliminates any downtime during the fail-over. The read-only capability allows end users to view and launch their applications. This section documents how to set up a secondary data center in read-only mode.

**NOTE** If your enterprise environment requires second data center failover with full read/write capability, other deployment options are also available. See KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1.
The scenario for Figure 1 is as follows:

- The primary data center includes WS1 as the master Workspace server configured with an internal database. WS2 is cloned from WS1 and the database is configured as a slave to the master database in WS1.

- The secondary data center is a manual replication of the primary data center. The master Workspace (WS1) configuration is imported to WS3 and WS4. The database is configured as slaves of WS1, with read-only access.

- Each data center is configured with a load balancer.

- The View Pods and Citrix-based Xen App Farm resources in the primary data center are setup in the secondary data center to mirror the configuration in the primary data center. When XenApp applications are configured, set up two Integration Brokers, one in each datacenter. Use a load balancer or a DNS record to control traffic flow to either the primary data center or to secondary data centers when the primary data center becomes unavailable. The ThinApp repository is set up in a Distributed File System (DFS) for high availability.

- The Workspace FQDN should be served by a load balancer or a DNS entry which forwards all the traffic either to the load balancer in the primary data center or to the load balancer in the secondary data center.
Setting Up a Secondary Data Center

The secondary data center is typically managed by a different vCenter server. When you set up the secondary data center you can configure and implement the following based on your requirements:

- Workspace servers in the secondary data center from the imported OVA file
- Load balancer for the secondary data center
- Duplicate View and Citrix-based desktops and applications and entitlements
- (Optional) pgpool-II for database redundancy to provide redundancy within a single datacenter
- Load balancer or DNS entry across the primary and secondary data centers for failover

Add Workspace Appliances by Importing Workspace OVA

To set up Workspace in a second data center for redundancy, you export an OVA file of the primary Workspace appliance and use the OVA file to deploy Workspace appliances in a secondary data center.

Prerequisites

- Workspace OVA file that was exported from the master Workspace in the primary data center
- IP Address and DNS record of secondary data center

Procedure

1. From the vSphere Client of the vSphere Web Client, select OVF template to deploy the Workspace OVA file that was exported.

2. To install Workspace appliances, see “Install the Workspace OVF File,” on page 15.

3. After the Workspace appliances are powered on, update the Workspace appliance configuration for each.

   The Workspace appliances in the secondary data center are identical copies of the master Workspace in the primary data center. Syncing to Active Directory and to resources that are configured in the primary data center is disabled.

What to do next

Go to the Connector Services Admin pages and configure the following:

- Enable Join Domain as configured in the master Workspace appliance in the primary data center.
- In the Auth Adapters page, add the authentication methods that are configured in the primary data center. See Chapter 9, “Setting Up User Authentication,” on page 53.
- In the Directory Authentication Method page, enable Windows Authentication, if configured in the primary data center.

Go to the Appliance Configurator Install Certificate page to add certificate authority signed certificates, duplicating the certificates in the Workspace appliances in the primary data center. See “Using SSL Certificates in Workspace,” on page 26.

Edit Runtime-config.properties File in Secondary Data Center

You must edit the runtime-config.properties files for the Workspace appliances in the secondary data center to change the JDBC URL to point to the database in the secondary data center and to configure the appliance for read-only access.

Procedure

1. Using a ssh client, log in to the Workspace appliance as the root user.
2 Open the runtime-config.properties file at /usr/local/horizon/conf/runtime-config.properties.

3 Change the JDBC URL to point to the database for the secondary data center.
See “Add an External Database to the Workspace Appliance,” on page 25.

4 Configure the Workspace appliance to have read-only access.
Type read.only.service=true.

5 Restart the Tomcat server on the workspace-va appliance.
  service horizon-workspace restart

What to do next
Repeat these steps on each Workspace appliance in the secondary data center.

Manage Resources Usage in Multiple Workspace Data Centers
You must configure the failover order of resources in both the primary and secondary data centers to make
the appropriate resources available from any data center.

You use the hznAdminTool command to create a database table with the failover order for resources in your
organization per service instance. The configured failover order is followed when a resource is launched.
You run the hznAdminTool failoverConfiguration in both data centers to set up the failover order.

Prerequisites
When Workspace is deployed in multiple data centers, the same resources are also set up in each data
center. Each application or desktop pools in the View Pods or Citrix-based XenFarms is considered as a
different resource in the Worksapce catalog. To prevent duplication of the resource in the catalog, make sure
that you enabled Do not sync duplicate applications in the View Pools or Published Apps - Citrix pages in
the Connector Services Admin page.

Procedure
1 Using a ssh client, log in to the Workspace appliance as the root user.

2 To view a list of the server instances, type hznAdminTool serviceInstances.
A list of the service instances with the ID number assigned displays, as in this example.

"id":103,"hostname"":"ws4.domain.com","ipaddress":"10.142.28.92"{"id":
154,"hostname"":"ws3.domain.com","ipaddress":"10.142.28.91"{"id":
1,"hostname"":"ws1.domain.com","ipaddress":"10.143.104.176"{"id":
52,"hostname"":"ws2.domain.com","ipaddress":"10.143.104.177"}

3 For each service instance in your organization, configure the failover order for View and Citrix-based
resources, type hznAdminTool failoverConfiguration -configType <configType> -configuration
<configuration> -serviceInstanceId <serviceInstanceId> [-orgId <orgId>]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-configType</td>
<td>Type the resource type being configured for failover. Values are either VIEW or XENAPP.</td>
</tr>
<tr>
<td>-configuration</td>
<td>Type the failover order. For VIEW config type, type as a comma separated list of the primary View Connector Server host names that are listed in the View Pools page from the Connector Services Admin page. For XENAPP config type, type as a comma separated list of XenFarm names. XenFarm names are not displayed in the Workspace Connector Services Admin pages. Contact your XenApp administrator for the list of names.</td>
</tr>
</tbody>
</table>
### Configure Database for Failover

For Workspace, database replication is configured so that data remains consistent across database servers within the primary data center and across to the secondary data center.

Whether you are using the vPostgres internal database or configure an external database to work with Workspace, you must configure your database for high availability. Configure a master and slave database architecture, with the slave is an exact replica of the master.

To set up your external database for high availability, refer to your external database documentation.

To set up the internal Workspace database as a master and slave configuration for high availability, see KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1.

### Using a DNS Record to Control Which Data Center is Active

If you use a Domain Name System (DNS) record to route user traffic in your data centers, the DNS record should point to a load balancer in the primary data center under normal operating situations.

If the primary data center becomes unavailable, the DNS record should be updated to point to the load balancer in the secondary data center.

When the primary data center becomes available again, the DNS record should be updated to point to the load balancer in primary data center.
Setting Time To Live in DNS Record

The time to live (TTL) setting determines how long before DNS related information is refreshed in the cache. For a seamless failover of View desktops and applications, make sure that the time to live (TTL) setting on the DNS records is short. If the TTL setting is set too long, users might not be able to access their View desktops and applications immediately after failover. To enable quick refresh of the DNS, set the DNS TTL to 30 seconds.

Workspace Activities Not Available in Read-Only Mode

Using Workspace in read-only mode is designed for high availability to allow end users access to the resources in their My Apps portal. Some activities in the Workspace admin console and other admin services pages might not be available when Workspace is in read-only mode. Below is a partial list of common activities that are not available.

When Workspace is running in read-only mode, activities related to changes in Active Directory or the database cannot be made and syncing to the Workspace database does not work.

Administrative functions that require writing to the database are not available during this time. You must wait until Workspace returns to read and write mode.

Workspace Administration Console Read-Only Mode

The following are some of the limitations in the Workspace admin console in read-only mode.

- Adding, deleting, editing users and groups in the Users & Groups tab
- Adding, deleting, editing applications in the Catalog tab
- Adding, deleting, editing application entitlements
- Changing branding information

Connector Services Admin Pages Read-Only Mode

The following are some of the limitations in the Connector Service Admin pages in read-only mode.

- Directory Sync to add, edit, delete users and groups
- Editing information about resources, including View, XenApp and other resources
- Editing the Authentication Methods page

Appliance Configurator Pages Read-Only Mode

The following are some of the limitations in the Appliance Configurator pages in read-only mode

- Testing the database connection setup
- Changing the Workspace admin password in the Change Password page

End User My Apps Portal Read-Only Mode

When Workspace is in read-only mode, users can sign in to their Workspace portal and access their resources. The following functionality in the end user Workspace portal is not available when Workspace is in read-only mode.

- Mark a resource as Favorite or unmark a resource as Favorite
- Drag and drop resources on the user's My Apps page to rearrange them
- Add resources from the App Center or remove resources from the user's My Apps page
- The label New is not removed from an application when it is launched
Workspace Windows Client Read-Only Mode

When Workspace is in read-only mode, users cannot setup new Windows clients. Existing Windows clients continue to work.
Setting Up User Authentication

Workspace supports the following authentication methods: Active Directory password, Kerberos, and RSA SecureID.

<table>
<thead>
<tr>
<th>Workspace Authentication Types Supported by Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Without any configuration, Workspace supports Active Directory password authentication. This method authenticates users directly against Active Directory.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Kerberos authentication provides domain users with single sign-on access to Workspace, eliminating the requirement for domain users to log in to Workspace after they log in to the enterprise network. The identity provider instance 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 Workspace from outside the enterprise network.</td>
</tr>
</tbody>
</table>

For more information about configuring Workspace user authentication, see the Workspace Administrator’s Guide.

This chapter includes the following topics:

- “Configuring SecurID for Workspace,” on page 53
- “Configuring Kerberos for Workspace,” on page 55

Configuring SecurID for Workspace

When you configure RSA SecurID server, you must add the Workspace appliance information as the authentication agent on the RSA SecurID server and configure the RSA SecureID server information on Workspace.

After you deploy Workspace, you can configure SecurID to provide additional security. You must ensure your network is properly configured for your 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 Workspace Setup wizard, you have the information necessary to prepare the RSA SecurID server. After you prepare the RSA SecurID server for the Workspace appliance, go to the Workspace Connector Services Admin Auth Adapters page to enable SecurID.

- Prepare the RSA SecurID Server for the Connector Services Admin on page 54

The RSA SecurID server must be configured with information about the Workspace appliance as the authentication agent. The information required is the hostname and the IP addresses for network interfaces.
Prepare the RSA SecurID Server for the Connector Services Admin

The RSA SecurID server must be configured with information about the Workspace appliance as the authentication agent. The information required is the hostname and the IP addresses for network interfaces.

Prerequisites

Workspace

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network to allow communication with the Connector Services Admin: RSA AM 6.1.2, 7.1 SP2 and above, and 8.0 and above. 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.

Procedure

1. On a supported version of the RSA SecurID server, add the Workspace appliance as an authentication agent. Enter the following information.

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

2. Download the compressed configuration file and extract the sdconf.rec file.

   Be prepared to upload this file later when you configure RSA SecurID in Workspace.

What to do next

Go to the Connector Services Admin Advanced tab and in the Auth Adapters page configure SecurID.

Configure RSA SecurID Authentication in Workspace

After the Workspace appliance is configured as the authentication agent in the RSA SecurID server, you must add the RSA SecureID configuration information to Workspace.

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.

Procedure

1. Go to the Connector Services Admin Auth Adapters page and in the SecurIDldpAdapter row, click Edit.
2. Click the Enable SecurID check box.
Configure the SecurID Authentication Adapter page.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name is required. The default name is SecurIDldpAdapter. You can change this at any time.</td>
</tr>
<tr>
<td>Enable SecurID</td>
<td>Check this box to enable securID authentication.</td>
</tr>
<tr>
<td>Number of authentication</td>
<td>The maximum number of failed login attempts using the RSA SecurID token. The default is five attempts.</td>
</tr>
<tr>
<td>attempts allowed</td>
<td></td>
</tr>
<tr>
<td>Connector Address</td>
<td>Enter the Workspace local host name or IP address. The value you enter must match the value you used when you added the Workspace appliance as an authentication agent to the RSA SecurID server. If your RSA SecurID server has a value assigned to the Alternate IP address prompt, enter that value as the Workspace IP address. If no alternate IP address is assigned, enter the value assigned to the IP address prompt.</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 RSA SecureID server configuration file. First, you must download the compressed file from the RSA SecurID 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 field 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. Ensure that the node secret file on the RSA SecurID server and on the Workspace appliance 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 Workspace appliance as well.</td>
</tr>
</tbody>
</table>

4. Save your SecurID settings.

**Configuring Kerberos for Workspace**

Kerberos authentication provides users with single sign-on access to Workspace. You enable Windows authentication to allow the Kerberos protocol to secure interactions between users' browsers and Workspace. You do not need to directly configure Active Directory to make Kerberos function with your Workspace deployment.

You go to the Connector Services Admin pages to enable Kerberos authentication. You must join the domain on the Connector Services Admin Join Domain page and enable Kerberos in the Auth Adapters page.

**Kerberos Authentication Operating System Support**

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

**Configuring your Browser**

The following Web browsers can be configured to send your Kerberos credentials to Workspace on computers running Windows: Firefox, Internet Explorer, and Chrome. All the browsers require additional configuration.

When Kerberos is enabled, you need to configure the Web browsers to send your Kerberos credentials to Workspace when users sign in.
Configure Kerberos on Workspace on page 56
To configure Workspace to provide Kerberos authentication, you must join to the domain and enable Kerberos authentication on Workspace.

Configure Internet Explorer to Access the Web Interface on page 57
You must configure the Internet Explorer browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using Internet Explorer.

Configure Firefox to Access the Web Interface on page 58
You must configure the Firefox browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using Firefox.

Configure the Chrome Browser to Access the Web Interface on page 58
You must configure the Chrome browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using the Chrome browser.

Configure Kerberos on Workspace
To configure Workspace to provide Kerberos authentication, you must join to the domain and enable Kerberos authentication on Workspace.

Procedure
1. Go to Connector Services Admin and select Join Domain.
2. On the Join Domain page, enter the information for the Active Directory domain.
   a. In the AD Domain text box, enter the fully qualified domain name of the Active Directory. The domain name you enter must be the same Windows domain where the Workspace appliance resides.
   b. In the AD Username text box, enter the user name of an account in the Active Directory that has permissions to join systems to that Active Directory domain.
   c. In the AD Password text box, enter the password associated with the AD Username. This password is not stored by Workspace.
   d. Click Join Domain.
      The Join Domain page is refreshed and displays a message that you are currently joined to the domain.
3. On the Connector Services Admin page, select Auth Adapters and click Edit in the KerberosldpAdapter row.
   a. The Name field shows KerberosldpAdapter as the name. You can change this.
   b. In the Directory UID Attribute text box, enter the account attribute that contains the user name.
   c. Check Enable Windows Authentication to extend authentication interactions between users’ browsers and Workspace.
   d. Check Enable NTLM to enable NT LAN Manager (NTLM) protocol-based authentication.
   e. Check Enable Redirect if round-robin DNS and load balancers do not have Kerberos support. Authentication requests are redirected to Redirect Host Name. If this is checked, enter the redirect host name in Redirect Host Name text box.
   f. Click Save.
Configure Internet Explorer to Access the Web Interface

You must configure the Internet Explorer browser if Kerberos is configured for your Workspace deployment and if you want to grant users access to the Web interface using Internet Explorer. Kerberos authentication works in conjunction with 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 into 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 Workspace appliance is part of the local intranet zone.
   a. Use Internet Explorer to access the Workspace login URL at https://workspaceHostname.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 Workspace 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 Workspace 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 Workspace URL in the Add this Web site to the zone text box.
      https://workspaceHostname.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.
      This option takes effect only after you restart Internet Explorer.
   c. Click OK.
Log in to the Workspace Web interface at https://workspaceHostname.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 Workspace. Now, users can use single sign-on access to Workspace.

Configure Firefox to Access the Web Interface

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

Kerberos authentication works in conjunction with 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 Workspace URL in the text box.
   
   https://workspaceHostname

5. Click OK.
7. Type your Workspace URL in the text box.
   
   https://workspaceHostname

8. Click OK.
9. Test Kerberos functionality by using the Firefox browser to log in to Workspace at https://workspaceHostname.
   
   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 Workspace. Now, users can use single sign-on access to Workspace.

Configure the Chrome Browser to Access the Web Interface

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

Kerberos authentication works in conjunction with 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 Google documentation for information about how to configure Chrome for Kerberos authentication.

Procedure

1. Test Kerberos functionality by using the Chrome browser.
2. Log in to the Workspace at \textit{https://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 Workspace. Users can use single sign-on access to Workspace.
The embedded OpenLDAP service is typically used for demonstration or test configurations. When you use 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 accessible locally only from the Linux console on the workspace-va virtual appliance. You can use standard LDAP commands to perform operations in the embedded OpenLDAP server. The required binaries (ldapadd, ldapsearch, ldapdelete, and ldapmodify) are installed on the virtual appliance.

You must use certain parameters when you configure OpenLDAP in the Appliance Configurator and Connector Services Admin pages.

### Table 10-1. OpenLDAP Configuration Information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ConnectorFullyQualifiedDomainName or localhost</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>

The Demo User Store includes ten sample users and one group for demonstration purposes.

Specific sample data is included with the Demo User Store. During deployment, this data is loaded into the sample database.

To add users or groups, create files and name them ldapusers.ldif and ldapgroups.ldif. Use the original files, users.ldif and groups.ldif, as templates. See “Add a User to the Demo User Store,” on page 62 and “Add Groups and Assign Users to Groups in the Demo User Store,” on page 64.

### Table 10-2. Sample Information included in the Demo User Store

<table>
<thead>
<tr>
<th>Sample Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample files</td>
<td>users.ldif</td>
</tr>
<tr>
<td></td>
<td>groups.ldif</td>
</tr>
<tr>
<td>Directory path</td>
<td>/etc/openldap</td>
</tr>
<tr>
<td>Sample usernames</td>
<td>testuser1 – testuser10</td>
</tr>
</tbody>
</table>
Table 10-2. Sample Information included in the Demo User Store (Continued)

<table>
<thead>
<tr>
<th>Sample Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password for all users</td>
<td>password</td>
</tr>
<tr>
<td>Sample group</td>
<td>testgroup1</td>
</tr>
<tr>
<td>The sample group, testgroup1, contains ten sample users.</td>
<td></td>
</tr>
</tbody>
</table>

- **Add a User to the Demo User Store** on page 62
  
  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 your tests produce results that are relevant to your production environment.

- **Add Groups and Assign Users to Groups in the Demo User Store** on page 64
  
  When you set up your Demo User Store, determine the number of groups and users to add based on the size of your production environment. Add enough groups and users to create an environment that closely resembles your production environment.

**Add 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 your tests produce 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 workspace-va virtual machine.

**Prerequisites**

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

**Procedure**

1. Replace the `value` tag in the `ldapusers.ldif` file with your information. See the Sample `ldapusers.ldif` table.

2. Copy the `ldif` file to the workspace-va virtual machine.

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

   ```
   /usr/bin/ldapadd -h 127.0.0.1 -D cn=Manager,dc=test,dc=example,dc=com -w H0rizon! -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

Table 10-3. Sample ldapusers.ldif File

---

Sample ldapusers.ldif

Use a unique value for each parameter.

dn: cn=value,ou=users,dc=test,dc=example,dc=com
objectClass: user
objectCategory: person
cn: value
sn: value
sAMAccountName: value
canonicalName: value
mail: value
givenName: value
distinguishedName: cn=value,ou=users,dc=test,dc=example,dc=com
objectGUID: value (For example, cd0ff02b-f9d6-4fac-a5bc-6380d1867999.)
userPassword: value (For example, {SSHA}WbipwJh13Jdy2tHppdxFMzzNVSfksZ.)

---

What to do next

Generate an encrypted password for use by your Demo User Store users. See “Generate an SSHA Encrypted Password,” on page 63.

Generate 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, encrypt each password one at a time.

Prerequisites


Procedure

1 Open the workspace-va virtual appliance.
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.
Add Groups and Assign Users to Groups in the Demo User Store

When you set up your Demo User Store, determine the number of groups and users to add based on the size of your production environment. 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 workspace-va 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 workspace-va virtual machine.

3. Run the `ldapadd` command to add a group to the Demo User Store.
   
   ```bash
   /usr/bin/ldapadd -h 127.0.0.1 -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 10-4. Example of the `ldapgroups.ldif` File**

<table>
<thead>
<tr>
<th>Sample Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a unique <code>value</code> for each parameter.</td>
</tr>
</tbody>
</table>

- `dn`: `cn=value,ou=users,dc=test,dc=example,dc=com`  
- `objectClass`: `group`  
- `objectCategory`: `group`  
- `sAMAccountName`: `value`  
- `canonicalName`: `value`  
- `mail`: `value`  
- `distinguishedName`: `cn=value,ou=users,dc=test,dc=example,dc=com`  
- `objectGUID`: (e.g. cd0f02b-f9d6-4fac-a5bc-6380d1867899)  
- `member`: `User DN1` (e.g. `cn=user1,ou=users,dc=test,dc=example,dc=com`)  
- `member`: `User DN2`  
- `member`: `User DN3`  
- `member`: `User DN4`  

**What to do next**

Use the Demo User Store for testing until you are ready to move Workspace in production.
Index

A
Active Directory, users 29, 32
Active Directory domains
   sync 36
   Windows authentication 34
Active Directory domain, add to sign in page 37
add domains to end user sign in page 37
add groups from Active Directory Domains 36
add user, Demo User Store 62
admin console 17, 20
admin console limitations in read only mode 51
administrator web sites 20
appliance configuration 21
appliance configurator, settings 22
appliance configurator limitations in read-only mode 51
authentication 29, 45

C
certificate chain 27
checklist
   Active Directory Domain Controller 12
   network information, IP Pools 12
Chrome 58
Citrix resource, configure 29
cloned machines, adding IP address 45
collect logs 28
configuration settings, appliance 21
configure
   logging 28
   virtual machines 39
connector services admin limitations in read-only mode 51
connector services admin 20
connector-va 43

D
data, transfer 25
database 11
database failover 50
demo user store 61
deployment
   checklists 12
   preparation 10
DNS, TTL Setting 50
DNS server redirect 50
DNS service location look-up 37

E
external database, Configurator 25
external access 39

F
failover 43, 46
failover order for resources 49
failover, configure database for 50
filter 33
filters 33
Firefox 58
forward DNS 11
FQDN 27

G
gateway-va 43
groups
   assign groups 64
   assign users 64

H
hardware
   ESX 8
   requirements 8
hznAdminTool, resource failover 49

I
identity provider 29
importing OVA 48
install Workspace 17
internal database 17
Internet Explorer 57
IP Address on cloned machines 45
IP Pools 16

J
JDBC, change on secondary data center 48
join domain
   kerberos 56
   multi-domain Active Directory 35
   trust multi-forest Active Directory 35

K
Kerberos, configure 56
L
limitations in read-only mode 51
Linux
SUSE 5
system administrator 5
log bundle 28
logging 28
M
Microsoft Windows Preview 12
multi-data center, DNS redirect 50
multi-domain Active Directory windows authentication 35
multi-domain Active Directory configuration 34
multi-domain names, add to sign in page 37
multiple virtual appliance 43
multiple virtual machines 43
multiple data centers 46
N
network configuration, requirements 8
O
oracle database 22
OVA file
deploy 15
install 15
overview, install 7
P
password adapter 37
passwords 17
PostgreSQL database 23
primary data center 46
proxy server settings 19
Q
query 33
R
read-only mode 46
read-only mode, set up 48
read-only mode limitations 51
read-only mode, end user functionality 51
redundancy 43
resources, configure 29
reverse lookup 11
reverse DNS 11
RSA SecurID server 54
runtime-config.properties file 48
S
safeguard alerts 29
secondary data center 46
SecurID, configure 54
self-signed certificate 26
server components 5
service-va 43
set up secondary data center 48
setup, admin setup 17
SMTP Server 12
SRV 37
SSHA encrypted password 63
SSL certificate, major certificate authority 41
SUSE Linux 5
sync directory 29
sync Active Directory domains 36
syslog server 26
system and functional administrator
Linux 5
Windows 5
T
ThinApps, configure 29
trusted multi-forest configuration 34
trusted multi-forest Active Directory domain windows authentication 35
TTL Settings for DNS 50
U
user authentication 5, 53
V
vCenter, credentials 12
version 29
version of Workspace 29
View, configure 29
virtual appliance, requirements 8
W
windows authentication 35
Windows authentication 37
Windows, system administrator 5
Windows authentication for Active Directory Domains 34
Workspace administrators 20
Workspace FQDN 21
Workspace
deploy 15
install 15
license key 12
VMware, Inc.